Communauté
UNIVERSITÉ Grenoble Alpes

MANCHESTER 1824
The University of Manchester

THÈSE

Pour obtenir le grade de

DOCTEUR DE LA COMMUNAUTE UNIVERSITE GRENOBLE ALPES

préparée dans le cadre d'une cotutelle *entre la Communauté Université Grenoble Alpes* et *The University of Manchester*

Spécialité : **Droit International**

Arrêté ministériel : le 6 janvier 2005 – 25 mai 2016

Présentée par

Thibault Moulin

Thèse dirigée par **Théodore CHRISTAKIS** et **Jean D'ASPREMONT**
codirigée par **Iain SCOBBIE**

préparée au sein du ***Centre d'Etudes sur la Sécurité Internationale et les Coopérations Européennes*** et du ***Manchester International Law Centre***

dans **l'Ecole Doctorale Sciences Juridiques** et **School of Law**

Le Cyber-Espionnage en Droit International

Thèse soutenue publiquement le **04 octobre 2018**,
devant le jury composé de :

M Toby SEDDON
Professeur, The University of Manchester, Président du Jury
M Duncan HOLLIS
Professeur, Temple Law School, Rapporteur du Jury
M Nicholas TSAGOURIAS
Professeur, The University of Sheffield, Rapporteur du Jury
Mme Karine BANNELIER-CHRISTAKIS
Maître de Conférences, Université Grenoble Alpes, Membre du Jury
M Michael GALANIS
Professeur Associé, The University of Manchester, Membre du Jury

CYBER-ESPIONAGE IN INTERNATIONAL LAW

A thesis submitted to the University of Manchester for the degree of Doctor of Philosophy in the Faculty of Humanities, and to the *Communauté Université Grenoble Alpes* for the degree of *Docteur en Droit International.*

2018

Thibault MOULIN
School of Law / Faculté de Droit

TABLE OF CONTENTS

94.922 words

TABLE OF CASES

I. INTERNATIONAL

Arbitral Tribunals

Award in the Arbitration regarding the Iron Rhine ("Ijzeren Rijn") Railway (Belgium/Netherlands) (2005) 27 RIAA 35

Case concerning the audit of accounts between the Netherlands and France pursuant to the Additional Protocol of 25 September 1991 to the Convention on the Protection of the Rhine against Pollution by Chlorides of 3 December 1976 (France/Netherlands) (2004) 25 RIAA 267

Island of Palmas case (Netherlands/USA) (1928) 2 RIAA 831

European Court of Human Rights

Banković and ors v Belgium and ors (2001) 44 EHRR SE5

Bosphorus Hava Yollari Turizm Ve Ticaret Anonim Sirketi v Ireland (2005) 42 EHRR 1

Golder v the UK (1975) 1 EHRR 524

Luedicke, Belkacem and Koç v Germany (1978) 2 EHRR 149

Tyrer v the UK (1978) 2 EHRR 1

Weber and Saravia v Germany ECHR 2006-XI 309

European Court of Justice

Commission of the European Communities v Council of the European Communities (22/70) [1971] ECR 263

Draft agreement between the Community, on the one hand, and the countries of the European Free Trade Association, on the other, relating to the creation of the European Economic Area (1/91) [1991] ECR I-6079

Van Gend en Loos v Nederlandse Administratie der Belastingen (26/62) [1963] ECR 1

Inter-American Court of Human Rights

Case of the Mapiripán Massacre v Colombia (Merits, Reparation and Costs) IACHR Series C No 134 (15.09.2005)

International Court of Justice

Aegean Sea Continental Shelf (Greece v Turkey) (Judgment) [1978] ICJ Rep 3

Ahmadou Sadio Diallo (Guinea v DRC) (Preliminary Objections) [2007] ICJ Rep 582

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-and-Herzegovina v Serbia-and-Montenegro) (Judgment) [2007] ICJ Rep 43

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v Serbia) (Judgment) [2015] ICJ Rep 3

Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of All Forms of Racial Discrimination (Ukraine v Russian Federation) (Order of 19.04.2017) <www.icj-cij.org/files/case-related/166/19395.pdf>

Arbitral Award of 31 July 1989 (Guinea-Bissau v Senegal) (Judgment) [1991] ICJ Rep 53

Armed Activities on the Territory of the Congo (DRC v Uganda) (Judgment) [2005] ICJ Rep 168

Armed Activities on the Territory of the Congo (New Application: 2002) (DRC v Rwanda) (Admissibility) [2006] ICJ Rep 6

Arrest Warrant of 11 April 2000 (DRC v Belgium) (Judgment) [2002] ICJ Rep 3

Avena and Other Mexican Nationals (Mexico v USA) (Judgment) [2004] ICJ Rep 12

Barcelona Traction, Light and Power Company, Limited (Belgium v Spain) (Judgment) [1970] ICJ Rep 3

Case concerning Right of Passage over Indian Territory (Portugal v India) (Judgment) [1960] ICJ Rep 6

Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica) (Judgment) [2015] ICJ Rep 665

Certain Expenses of the United Nations (Article 17, Paragraph 2, of the Charter) (Advisory Opinion) [1962] ICJ Rep 151

Certain Questions of Mutual Assistance in Criminal Matters (Djibouti v France) (Judgment) [2008] ICJ Rep 177

Colombian-Peruvian asylum case (Colombia/Peru) (Judgment) [1950] ICJ Rep 266

Competence of the General Assembly for the Admission of a State to the United Nations (Advisory Opinion) [1950] ICJ Rep 4

Constitution of the Maritime Safety Committee of the Inter-Governmental Maritime Consultative Organization (Advisory Opinion) [1960] ICJ Rep 150

Continental Shelf (Libya/Malta) (Judgment) [1985] ICJ Rep 13

Corfu Channel (UK v Albania) [1949] ICJ Rep 4

Corfu Channel (UK v Albania) (Contre-Mémoire soumis par le Gouvernement de la République Populaire d'Albanie) [15.06.1948] <www.icj-cij.org/files/case-related/1/1492.pdf>

Corfu Channel Case (UK v Albania) (Duplique présentée par le Gouvernement de la République Populaire d'Albanie conformément à l'Ordonnance rendue le 28 mars 1948 par la Cour Internationale de Justice) [20.09.1948] <www.icj-cij.org/files/case-related/1/10896.pdf>

Corfu Channel (UK v Albania) (Reply submitted, under the Order of the Court of 26th March, 1948, by the Government of the UK) [30.07.1948] <www.icj-cij.org/files/case-related/1/10895.pdf>

Delimitation of the Maritime Boundary in the Gulf of Maine Area (Canada/USA) (Judgment) [1984] ICJ Rep 246

Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights (Advisory Opinion) [1999] ICJ Rep 62

Dispute regarding Navigational and related Rights (Costa Rica v Nicaragua) (Judgment) [2009] ICJ Rep 213

Effect of Awards of Compensation Made by the UN Administrative Tribunal (Advisory Opinion) [1954] ICJ Rep 47

Fisheries Jurisdiction (UK v Iceland) (Judgment) [1974] ICJ Rep 3

Frontier Dispute (Burkina-Faso/Mali) (Judgment) [1986] ICJ Rep 554

Gabcikovo-Nagymaros Project (Hungary/Slovakia) (Judgment) [1997] ICJ Rep 7

Interhandel Case (Switzerland v USA) (Preliminary Objections) [1959] ICJ Rep 6

Jurisdictional Immunities of the State (Germany v Italy: Greece intervening) (Judgment) [2012] ICJ Rep 99

Kasikili/Sedudu Island (Botswana/Namibia) (Judgment) [1999] ICJ Rep 1045

LaGrand (Germany v USA) (Judgment) [2001] ICJ Rep 466

Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970) (Advisory Opinion) [1971] ICJ Rep 16

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226

Legality of the Use by a State of Nuclear Weapons in Armed Conflict (Advisory Opinion) [1996] ICJ Rep 66

Legality of Use of Force (Serbia-and-Montenegro v Belgium) (Preliminary Objections) [2004] ICJ Rep 279

Maritime Delimitation and Territorial Questions between Qatar and Bahrain (Qatar v Bahrain) (Judgment) [2001] ICJ Rep 40

Maritime Dispute (Peru v Chile) (Judgment) [2014] ICJ Rep 3

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA) (Judgment) [1986] ICJ Rep 14

North Sea Continental Shelf (Germany/Denmark; Germany/Netherlands) (Judgment) [1969] ICJ Rep 3

Nottebohm Case (second phase) (Liechtenstein v Guatemala) (Judgment) [1955] ICJ Rep 4

Obligations concerning Negotiations relating to Cessation of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Islands v UK) (Preliminary Objections) [2016] ICJ Rep 833

Oil Platforms (Iran v USA) (Preliminary Objection) [1996] ICJ Rep 803

Oil Platforms (Iran v USA) (Judgment) [2003] ICJ Rep 161

Pulp Mills on the River Uruguay (Argentina v Uruguay) (Judgment) [2010] ICJ Rep 14

Questions relating to the Obligation to Prosecute or Extradite (Belgium v Senegal) (Judgment) [2012] ICJ Rep 422

Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia) (Memorial of Timor-Leste) [2014] <www.icj-cij.org/files/case-related/156/18699.pdf>

Reparation for Injuries suffered in the Service of the United Nations (Advisory Opinion) [1949] ICJ Rep 174

Request for Interpretation of the Judgment of 15 June 1962 in the Case concerning the Temple of Preah Vihear (Cambodia v Thailand) (Cambodia v Thailand) (Judgment) [2013] ICJ Rep 281

Reservations to the Convention on Genocide (Advisory Opinion) [1951] ICJ Rep 15

Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia/Malaysia) (Judgment) [2002] ICJ Rep 625

Territorial Dispute (Libya/Chad) (Judgment) [1990] ICJ Rep 6

United States Diplomatic and Consular Staff in Tehran (USA v Iran) (Judgment) [1980] ICJ Rep 3

Whaling in the Antarctic (Australia v Japan: New Zealand intervening) (Judgment) [2014] ICJ Rep 226

Permanent Court of International Justice

Article 3, Paragraph 2, of the Treaty of Lausanne (Advisory Opinion) [1925] PCIJ Rep Series B No 12

Case concerning the Factory at Chorzów (Germany v Poland) (Claim for Indemnity, Jurisdiction) [1927] PCIJ Rep Series A No 9

Case of the S.S. "Lotus" (France v Turkey) (Judgment) (1927) PCIJ Rep Series A No 10

Case of the SS "Wimbledon" (UK, France, Italy and Japan v Germany) (Judgment) (1923) PCIJ Rep Series A No 1

Competence of the International Labour Organization to Regulate, incidentally, the Personal Work of the Employer (Advisory Opinion) (1926) PCIJ Rep Series B No 13

Interpretation of the Convention of 1919 concerning the employment of Women during the Night (Advisory Opinion) (1932) PCIJ Rep Series A/B No 50

Nationality Decrees Issued in Tunis and Morocco on Nov. 8th, 1921 (Advisory Opinion) (1923) PCIJ Rep Series B No 4

Polish Postal Service in Danzig (Advisory Opinion) (1925) PCIJ Rep Series B No 11

WTO Panels and Appellate Body

Australia–Certain Measures Concerning Trademarks and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging ('Australia–Tobacco Plain Packaging (Ukraine)') (15.03.2012) WT/DS434/1

Australia–Certain Measures Concerning Trademarks, Geographical Indications and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging ('Australia–Tobacco Plain Packaging (Honduras)') (10.04.2012) WT/DS435/1

Australia–Certain Measures Concerning Trademarks, Geographical Indications and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging ('Australia–Tobacco Plain Packaging (Dominican Republic)') (23.07.2012) WT/DS441/1

Australia–Certain Measures Concerning Trademarks, Geographical Indications and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging ('Australia–Tobacco Plain Packaging (Cuba)') (07.05.2013) WT/DS458/1

Australia–Certain Measures Concerning Trademarks, Geographical Indications and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging ('Australia–Tobacco Plain Packaging (Indonesia)') (20.09.2013) WT/DS467/1

Bahrain–Measures Relating to Trade in Goods and Services, and Trade-Related Aspects of Intellectual Property Right (04.08.2017) WT/DS527/1

Canada–Continued Suspension of Obligations in the EC–Hormones Dispute (31.03.2008) WT/DS321/R

China–Measures Affecting the Protection and Enforcement of Intellectual Property Rights ('China–Intellectual Property Rights') (20.09.2013) WT/DS467/1

European Communities–Protection of Trademarks and Geographical Indications for Agricultural Products and Foodstuffs ('EC–Trademarks and Geographical Indications') (10.04.2003) WT/DS174/1/Add.1

Indonesia–Certain Measures Affecting the Automobile Industry ('Indonesia–Autos') (15.10.1996) WT/DS59/1

Japan–Measures concerning Sound Recordings (04.06.1996) WT/DS42/1

Saudi Arabia–Measures Relating to Trade in Goods and Services, and Trade-Related Aspects of Intellectual Property Right (01.08.2017) WT/DS528/1

United Arab Emirates–Measures Relating to Trade in Goods and Services, and Trade-Related Aspects of Intellectual Property Rights (12.10.2017) WT/DS526/2

United States–Continued Suspension of Obligations in the EC–Hormones Dispute (31.03.2008) WT/DS320/R

United States–Section 211 Omnibus Appropriations Act of 1998 ('US–Section 211 Appropriations Act') (15.07.1999) WT/DS176/1

United States–Section 337 of the Tariff Act of 1930 and Amendments Thereto (18.01.2000) WT/DS186/1

United States–Standards for Reformulated and Conventional Gasoline ('US–Gasoline') (20.05.1996) WT/DS2/9

II. NATIONAL

Australia

ACT Supreme Court, *R v Lappas* (2003) 139 A Crim R 77

Federal Court of Australia, *Minister of Foreign Affairs and Trade; the Commissioner of the Australian Federal Police and the Commonwealth of Australia v Geraldo Magno and Ines Almeida, Re* (1992) FCA 566

Canada

Federal Court, *Canadian Security Intelligence Service Act, Re* (2007) 2008 FC 301

Federal Court, *Security Intelligence Service Act, Re* (2009) 2009 FC 1058

France

Cour de Cassation (1984) Bull crim 1984 No 310

Cour de Cassation (1987) Bull crim 1987 No 78

Cour de cassation (1988) No 87-84.360

Cour de Cassation, *Von Berenberg-Gossler* (1969) 52 ILR 492

Germany

Bundesgerichtshof (04.04.1990) 3 StB 5/90

United Kingdom

Court of Appeal, *R v Bingham (Maureen Grace)* (1973) 57 Cr App R 439

Court of Appeal, *R v Blake (George)* (1961) 45 Cr App R 292

United States of America

California Northern District Court, *United States v Liew et al* (2014) Case No 3:11-cr-00573

SDNY District Court, *United States v Coplon* (1949) 84 F.Supp 472

US Court of Appeals for the Second Circuit, *United States v Rosenberg et al* (1952) 195 F 2d 583

US District Court, Massachusetts, *United States v Zehe* (1985) 601 F Supp 196

US Supreme Court, *Ex Parte Quirin* (1942) 317 US 1

US Supreme Court, *Johnson v Eisentrager* (1950) 339 US 763

TABLE OF STATUTES

I. INTERNATIONAL / BILATERAL

Arms Trade Treaty (adopted 02.04.2013)

Charter of the Association of Southeast Asian Nations (adopted 20.11.2007–EIF 15.12.2008) 2624 UNTS 223

Charter of the Organization of American States (adopted 30.04.1948–EIF 13.12.1951) 119 UNTS 3

Charter of the United Nations and Statutes of the International Court of Justice (adopted 26.06.1945–EIF 24.10.1945)

Convention on International Civil Aviation (Adopted 07.12.1944–EIF 04.04.1947)

Constitutive Act of the African Union (adopted 11.07.2000–EIF 26.05.2001) 2158 UNTS I-37733

Convention (II) with Respect to the Laws and Customs of War on Land ('Hague II') (adopted 29.07.1899–EIF 04.09.1900)

Convention (IV) respecting the Laws and Customs of War on Land ('Hague IV') (adopted 18.10.1907–EIF 26.01.1910)

Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land ('Hague V') (adopted 18.10.1907–EIF 26.01.1910)

Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War ('Hague XIII') (adopted 18.10.1907–EIF 26.01.1910)

Convention for the Protection of Human Rights and Fundamental Freedoms ('European Convention of Human Rights'/'ECHR') (adopted 04.11.1950–EIF 03.09.1953) 213 UNTS 22

Convention on Cybercrime (adopted 23.11.2001–EIF 01.07.2004) ETS 185

Constitution and Convention of the International Telecommunication Union (adopted 12.08.1992–EIF 01.07.1994) 1825 UNTS 331

General Agreement on Trade-Related Aspects of Intellectual Property ('TRIPS') (Annex 1C of Marrakesh Agreement Establishing the World Trade Organization) 1869 UNTS 299

Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War ('Geneva Convention IV') (adopted 12.08.1949–EIF 21.10.1950) 7 UNTS 287

Pact of the League of Arab States (adopted 22.03.1945–EIF 11.05.1945) 70 UNTS 237

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts ('Additional Protocol I') (adopted 08.06.1977–EIF 07.12.1978) 1125 UNTS 3

Rome Statute of the International Criminal Court (Adopted 17.07.1998–EIF 01.07.2002) 2187 UNTS 3

The Hague Rules of Air Warfare ('The Hague Air Rules') (adopted 19.02.1923)

Understanding on the Rules and Procedures Governing the Settlement of Disputes (Annex 2 of Marrakesh Agreement Establishing the World Trade Organization) 1869 UNTS 401

United Kingdom–United States of America Agreement ('UKUSA/Five Eyes/FVEY') (signed on 05.03.1946)

United Nations Convention on the Law of the Sea ('UNCLOS') (adopted 10.12.1982–EIF 16.11.1994) 1833 UNTS 397

Vienna Convention on Consular Relations ('VCCR') (adopted 24.04.1963–EIF 19.03.1967) 596 UNTS 261

Vienna Convention on Diplomatic Relations ('VCDR') (adopted 18.04.1961–EIF 24.04.1964) 500 UNTS 95

Vienna Convention on the Law of Treaties ('VCLT') (adopted 23.05.1969–EIF 27.01.1980) 1155 UNTS 331

II. ECOWAS, EU

Commission Delegated Regulation of 12 October 2015 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Directive C/DIR. 1/08/11 On Fighting Cyber Crime Within ECOWAS (19.08.2011)

III. NATIONAL

Algeria

Code pénal

Argentina

Código Penal

Australia

Australian Security Intelligence Organisation Act 1979

Criminal Code Act 1995

Intelligence Services Act 2001

Austria

Strafgesetzbuch

Azerbaijan

Criminal code

Belgium

Loi Organique des Services de Renseignement et de Sécurité ('L.R&S') (30.11.1998) MB 30.01.1999, 2827

Code pénal

Bolivia

Código Penal

Bosnia-and-Herzegovina

Criminal code

Law on the Intelligence and Security Agency (2004)

Burkina Faso

Code pénal

Burundi

Code pénal

Cameroon

Code pénal

Canada

Canadian Security Intelligence Service Act ('CSIS Act') RSC 1985 c C-23

Central African Republic

Code pénal

Chad

Code pénal

Chile

Código Penal

Ley Sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia ('Ley 19974') (02.10.2004) No 19974

China

Criminal Law of the People's Republic of China

Colombia

Código Penal

Comoros

Code pénal

Croatia

Act on the Security Intelligence System of the Republic of Croatia (30.06.2006)

Criminal code

Czech Republic

Act on Cyber Security and Change of Related Acts ('Act on Cyber Security') (23.07.2014) No 181

Act on Intelligence Services of the Czech Republic ('BIS Act') (07.07.1994) No 153/1994

Criminal Code

Democratic Republic of Congo

Code pénal

Ecuador

Código Penal

Eritrea

Criminal code

Estonia

Penal Code

Ethiopia

Criminal Code

Computer Crime Proclamation (07.07.2016) No 958-2016, FNG No 83, 9104

France

Code de Sécurité intérieure

Code pénal

Georgia

Law of Georgia on the Georgian Intelligence Service (27.04.2010) No 2984-RS

Germany

Strafgesetzbuch

Gesetz über den Bundesnachrichtendienst ('BND-Gesetz BNDG') (20.12.1990) BGBl I S2954, 2979

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ('Artikel 10-Gesetz–G 10') (26.06.2001) BGBl. I S1254, 229

Ghana

The Security and Intelligence Agencies Act (1996) No 256

Greece

Law on National Intelligence Service and other provisions (03.03.2008) No 3649, FEK 132 A 39/3.03.2008

Hungary

Criminal code

India

Official Secrets Act 1923

Israel

Israel Penal Law 5937/1977

Italy

Law on Intelligence System for the Security of the Republic and new Provisions governing Secrecy ('Law 124/2007') (03.08.2007) No 124, OJ No 187 of 13.08.2007

Kazakhstan

Penal Code

The Law of the Republic of Kazakhstan On Foreign Intelligence ('Law 277-IV') (22.05.2010) No 277-IV

Kenya

Kenya Defence Forces Act 2012

National Intelligence Service Act 2012

Latvia

Criminal code

Luxembourg

Loi portant réorganisation du Service de renseignement de l'État ('Loi SRE') (05.07.2016) A129

Malaysia

Penal code

Mexico

Código Penal

Ley de Seguridad Nacional (2005) DOF 31-01-2005

Moldova

Criminal code

Montenegro

Criminal code

Law on the National Security Agency (2015) No 08/15

Morocco

Code pénal

Netherlands

Intelligence and Security Services Act 2002

Wetboek van Strafrecht

New Zealand

Crimes Act 1961

Intelligence and Security Act 2017

Nigeria

Computer Security and Critical Information Infrastructure Protection Bill 2005

National Security Agencies Act 1986

Official Secrets Act 1962

Norway

Act relating to the Norwegian Intelligence Service (20.03.1998)

Instructions for the Intelligence Service (31.08.2001)

Papua New Guinea

National Intelligence Organization Act 1984 ('NIO Act')

Paraguay

Código Penal

Ley Que crea el Sistema Nacional de Inteligencia (20.08.2014) No 5241

Peru

Código Penal

Ley del Sistema de Inteligencia Nacional–SINA y de la Dirección Nacional de Inteligencia–DINI (14.12.2005) No 26664, NL 04.01.2006, 309260

Philippines

Cybercrime Prevention Act of 2012

Penal Code

Republic of Korea

Criminal Act

Unfair Competition Prevention and Trade Secret Protection Act 1961

The Act on Promotion of Information and Communications Network Utilization and Data Protection, Etc. (16.01.2001) No 6360

Russia

Criminal Code

Federal Law On Foreign Intelligence (08.12.1995) No 5

Serbia

Criminal code

Singapore

Computer Misuse and Cybersecurity Act 1993

Slovakia

The Act of the National Council of the Slovak Republic on the Slovak Information Service ('Act on the Slovak Information Service') (21.01.1993) No 46/1993

Slovenia

Resolution on the National Security Strategy of the Republic of Slovenia (02.04.2010) ULRS 27/2010

South Africa

Cybercrimes and Cybersecurity Bill 2015

Spain

Código Penal

Ley reguladora del Centro Nacional de Inteligencia ('Ley 11/2002') (06.05.2002) No 11/2002, BOE-A-2002-8628

Real Decreto por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa (25.06.2004) No 1551/2004, BOE No 154 of 26.06.2004

Switzerland

Code pénal

Loi fédérale sur le Renseignement (LRens) (25.09.2017) RO 2017, 4095ss

Tajikistan

Criminal code

Thailand

Penal code

Trade Secrets Act 2015 (No 2) BE 2558

Computer Crime Act 2017 (No 2) BE 2560

Tunisia

Code pénal

Turkey

Criminal Code

The Law on the State Intelligence Services and the National Intelligence Organization ('Law 2937') (01.11.1983) No 2937

Uruguay

Código Penal

UK

Investigatory Powers Act 2016 ('IPA')

Official Secrets Act 1989 ('OSA 1989')

Regulation of Investigatory Powers Act 2000 ('RIPA')

USA

An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigative tools, and for other purposes ('Patriot Act') (2001) Pub L 107–56, 115 STAT 272

Executive Order 12.333, 'United States intelligence activities' ('EO 12333') (04.12.1981) 56 FR59941

Venezuela

Ley Especial contra los Delitos Informaticos (30.10.2001) GO 37.313

LIST OF ABBREVIATIONS AND ACRONYMS

I. DOMESTIC ENTITIES

AGO	Attorney General's Office (UK)
AIV	Adviesraad Internationale Vraagstukken (Advisory Council of International Affairs, the Netherlands)
AIVD/GISS	Algemene Inlichtingen- en Veiligheidsdienst (General Intelligence and Security Services, the Netherlands)
AN	Assemblée nationale (National Assembly, France)
ANI	Agencia Nacional de Inteligencia (National Intelligence Agency, Chile)
ASD	Australian Signals Directorate
BKA	Bundeskanzleramt (Federal Chancellery, Austria)
BMI	Bundesministeriums des Innern (Federal Ministry of the Interior, Germany)
BND	Bundesnachrichtendienst (Federal Intelligence Service, Germany)
CA	Cour d'Appel / Court of Appeal
CAF	Canadian Armed Forces
CAVV	Commissie van Advies inzake Volkenrechtelijke Vraagstukken (The Advisory Committee on Issues of Public International Law, the Netherlands)
CFCS	Center for Cybersikkerhed (Centre for Cybersecurity, Denmark)
CISEN	Centro de Investigación y Seguridad Nacíonal (Centre for Investigation and National Security, Mexico)
CNI	Centro Nacional de Inteligencia (National Intelligence Centre, Spain)
Comité R	Comité permanent de contrôle des services de renseignements et de sécurité (Permanent Oversight Committee on the Intelligence and Security Services, Belgium)
CONPES	Consejo Nacional de Política Económica y Social (National Council on Economic and Social Policy, Colombia)

CSE/CSEC	Communications Security Establishment (Canada)
DEFMIN	Minister of Defence (Finland)
DoD	Department of Defense (USA)
DoJ	Department of Justice (USA)
DPMC	Department of the Prime Minister and Cabinet (New Zealand)
EOS Committee	Norwegian Parliamentary Intelligence Oversight Committee
FCA	Federal Court of Australia
FCO	Foreign and Commonwealth Office (UK)
FISC/FISA Court	United States Foreign Intelligence Surveillance Court
FMPRC	Ministry of Foreign Affairs of the People's Republic of China
GAO	Government Accountability Office (USA)
GCSB	Government Communications Security Bureau (New Zealand)
GPO	US Government Publishing Office
ICANN	Internet Corporation for Assigned Names and Numbers
ISC	Intelligence and Security Committee of Parliament (UK)
ISPC	Information Security Policy Council (Japan)
MAC	Ministerstwo Administracji i Cyfryzacji (Ministry of Administration and Digitisation, Poland)
MCDMS	Ministry for Competitiveness and Digital Maritime and Services Economy (Malta)
MCIT	Ministry of Communication and Information Technology (Afghanistan, Saudi Arabia, Egypt)
MEITY	Ministry of Electronics and Information Technology (India)
MFA	Ministry of Foreign Affairs (generic term)
MI	Military Intelligence
MICT	Ministry of Information and Communications Technology (Jordan)
MID	Ministry of Foreign Affairs of the Russian Federation
MITEC	Ministry of Information Technology & Communications (Rwanda)

MIVD/DISS	Militaire Inlichtingen- en Veiligheidsdienst (Military Intelligence and Security Service, the Netherlands)
MoD	Ministry of Defence (UK)
MOD	Ministry of Defence (generic term)
MOPA	Ministry of Public Administration (Bangladesh)
MOTC	Ministry of Transport and Communications (Qatar)
MP/MPs	Member of Parliament/Members of Parliament
MSC	Ministry of Security and Justice (the Netherlands)
NCSC	National Cyber Security Centrum (The Netherlands)
NITA	National Information Technology Authority (Uganda)
NZSIS	New Zealand Security Intelligence Service
OGC	Office of General Counsel (USA)
OLC	Office of Legal Counsel (USA)
PCM	Presidenza del Consiglio dei Ministri (Presidency of the Council of Ministers, Italy)
PM	Prime Minister
PM&C	Department of the Prime Minister and Cabinet (Australia)
Presidencia	Oficina de la Presidencia de la República (Office of the President of the Republic, Mexico)
RCAF	Royal Canadian Air Force
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale (Secretariat-General for National Defence and Security, France)
SGRS	Service Général du Renseignement et de la Sécurité (General Intelligence and Security Service, Belgium)
SIS/MI6	Secret Intelligence Service (UK)
SRC	Service de Renseignement de la Confédération (Federal Intelligence Service, Switzerland)
SUPO	Suojelupoliisi (Security Intelligence Service, Finland)

TJAGLCS	The Judge Advocate General's Legal Center and School (USA)
UDHB	Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (Ministry of Transport, Maritime and Communication, Turkey)
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (Federal Department of Defence, Civil Protection and Sport, Switzerland)

II. INTERNATIONAL ORGANISATIONS, ORGANS, AND CONFERENCES

ASEAN	Association of Southeast Asian Nations
DSB	Dispute Settlement Body (WTO)
DSU	Dispute Settlement Understanding (WTO)
EC	European Community
ECJ	European Court of Justice
ECtHR	European Court of Human Rights
EU	European Union
HRC	Human Rights Committee
IACtHR	Inter-American Court of Human Rights
ICJ	International Court of Justice
ICTY	International Criminal Tribunal for the former Yugoslavia
ILC	International Law Commission
ITU	International Telecommunication Union
MERCOSUR	Mercado Común del Sur
OAS	Organization of American States
PCIJ	Permanent Court of International Justice
UN	United Nations
UNASUR	Unión de Naciones Suramericanas
UNDP	United Nations Development Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNGA	United Nations General Assembly
UNGGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
UNSC	United Nations Security Council

WSIS	World Summit on the Information Society (ITU)
WTDC	World Telecommunication Development Conference (ITU)
WTO	World Trade Organization
WTSA	World Telecommunication Standardization Assembly (ITU)

III. MISCELLANEOUS TERMS

CC	Criminal Code
CIS	Computer Information Systems
CP	Code Pénal / Código Penal
DNS	Domain Name System
DO	Dissenting Opinion
EW	Electronic Warfare
HR	Human Rights
IHL	International Humanitarian Law
IO	International Organization
IW	Information Warfare
HPCR	Program on Humanitarian Policy and Conflict Research at Harvard University
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
Info Actys	Information Activities (Australia)
LOAC	Law of Armed Conflicts
PC	Penal Code
PNG	*Persona Non Grata*
POW	Prisoner Of War
PRC/China	People's Republic of China
ROE	Rules Of Engagement
SO	Separate Opinion
UK	United Kingdom
USA	United States of America
WMD	Weapons of Mass Destruction
WvS	Wetboek van Strafrecht

IV. ACADEMIC SOURCES

Reviews

A.F.D.I.	Annuaire Français de Droit International
A.F.L.R.	Air Force Law Review
A.J.I.L.	American Journal of International Law
Am.U.Int'l.L.Rev.	American University International Law Review
Ariz.St.L.J.	Arizona State Law Journal
Austl.Int'l.L.J.	Australian International Law Journal
Australian Y.B.I.L.	Australian Yearbook of International Law
B.Y.B.I.L.	Baltic Yearbook of International Law
Berk.J.Int'l.L.	Berkeley Journal of International Law
Bond L.R.	Bond Law Review
British Y.B.I.L.	British Journal of International Law
Brook.J.Int'l.L.	Brooklyn Journal of International Law
Canadian Y.B.I.L.	Canadian Yearbook of International Law
Cardozo J.Int'l.&Comp.L.	Cardozo Journal of International and Comparative Law
Chi.J.Int'l.L.	Chicago Journal of International Law
C.I.L.J.	Cambridge International Law Journal
C.J.I.C.L.	Cambridge Journal of International and Comparative Law
Col.J.T.L.	Columbia Journal of Transnational Law
Colum.L.Rev.	Columbia Law Review
Conn.L.R.	Connecticut Law Review
Denv.J.Int'l.L.&Pol'y	Denver Journal of International Law and Policy
Duke J.Comp.&Int'l.L.	Duke Journal of Comparative and Comparative Law
E.J.I.L.	European Journal of International Law
Eur.J.Legal.Stud.	European Journal of Legal Studies
Fed.Comm.L.J.	Federal Communication Law Journal
Ford.L.R.	Fordham Law Review
G.C.Y.I.L.J.	Global Community: Yearbook of International Law and Jurisprudence

Geo.J.Int'l.L.	Georgetown Journal of International Law
Geo.Wash.Int'l.L.Rev.	George Washington International Law Review
German Y.B.I.L.	German Yearbook of International Law
Harv.L.Rev.	Harvard Law Review
Harv.Nat'l.Sec.J.	Harvard National Security Journal
Hous.J.Int'l.L.	Houston Journal of International Law
I.C.L.Q.	International and Comparative Law Quarterly
I.D.E.A.	IDEA–The Journal of Law and Technology
I.J.L.I.	International Journal of Legal Information
I.L.S.	International Law Studies (US Naval War College)
Irish Y.B.I.L.	Irish Yearbook of International Law
I.R.R.C.	International Review of the Red Cross
Int.Lawyer	International Lawyer
I.O.L.R.	International Organizations Law Review
Is.L.R.	Israel Law Review
JAG L.Rev.	Jag Law Review
J.A.I.L.	Japanese Annual of International Law
J. Air L.	The Journal of Air Law and Commerce
Japanese Y.B.I.L.	Japanese Yearbook of International Law
J.Conflict&Sec.L.	Journal of Conflict and Security Law
J.I.L.P.	New York University Journal of International Law and Politics
J.L.&Cyber Warfare	Journal of Law & Cyber Warfare
J.Nat'l.Sec.L.&Pol'y	Journal of National Security Law & Policy
J.S.Afr.L.	Journal of South African Law
Keesings	Keesing's Contemporary Archives (1931-1988) / Keesing's Record of World Events (1988-present)
Lewis&Clark L.Rev.	Lewis & Clark Law Review
L.J.I.L.	Leiden Journal of International Law
McG.L.J.	McGill Law Journal

Melb.J.Int'l.L.	Melbourne Journal of International Law
Mich.J.Intl.L.	Michigan Journal of International Law
Mich.Telecomm.&Tech.L.Rev.	Michigan Telecommunications and Technology Law Review
Mil.L.Rev.	Military Law Review
Minn.J.Int'l.L.	Minnesota Journal of International Law
Minn.J.L.Sci.&Tech.	Minnesota Journal of Law, Science & Technology
M.L.R.	Modern Law Review
M.P.E.P.I.L.	Max Planck Encyclopedia of Public International Law
M.P.Y.U.N.L.	Max Planck Yearbook of United Nations Law
Nat'l. Security L.&Pol'y	National Security Law & Policy
Naval L.Rev.	Naval Law Review
N.C.J.Int'l.L.&Com.Reg.	North Carolina Journal of International Law and Commercial Regulation
Netherlands Y.B.I.L.	Netherlands Yearbook of International Law
N.I.L.R.	Netherlands International Law Review
N.Ky.L.Rev.	Northern Kentucky Law Review
N.S.L.B.	National Security Law Brief
N.Y.L.Sch.J.Int'l.&Comp.	New York Law School Journal of International and Comparative Law
Or.Rev.Int'l.L.	Oregon Review of International Law
Pace Int'l.L.Rev.	Pace International Law Review
P.I.L.R.	Loyola Public Interest Law Reporter
Q.R.J.	Qualitative Research Journal
R.B.D.I.	Revue Belge de Droit International
Recueil des Cours	Recueil des Cours de l'Académie de Droit International / Collected Courses of the Hague Academy of International Law
R.G.D.I.P.	Revue Générale de Droit International Public
R.S.D.I.E.	Revue Suisse de Droit International et Européen / Schweizerische Zeitschrift für internationales und europäisches

	Recht / Swiss Review of International and European Law
Spanish Y.B.I.L.	Spanish Yearbook of International Law
Stan.J.Int'l.L.	Stanford Journal of International Law
Stan.L.Rev.	Stanford Law Review
Syd.L.R.	Sydney Law Review
Syracuse J.O.S.T.	Syracuse Journal of Science & Technology Law
Temple L.Q.	Temple Law Quarterly
Tex.Int'l.L.J.	Texas International Law Journal
Tex.L.Rev.	Texas Law Review
Tul.J.Tech.&Intell.Prop.	Tulane Journal of Technology and Intellectual Property
U.Chi.L.Rev.	University of Chicago Law Review
U.Det. Mercy L.Rev.	University of Detroit Mercy Law Review
Utrecht J.Int'l.&Eur.L.	Utrecht Journal of International and European Law
Va.J.Int'l.L.	Virginia Journal of International Law
Vanderbilt J.Transnatl.L.	Vanderbilt Journal of Transnational Law
Vill.L.Rev.	Villanova Law Review
Y.B.I.H.L.	Yearbook of International Humanitarian Law
Z.a.ö.R.V.	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht

Publishers

Blackstone	Blackstone Press
C.A.P.	Carolina Academic Press
C.U.P.	Cambridge University Press
E.E.	Edward Elgar Publishing
E.U.P.	Edinburgh University Press
Falmer Press	Falmer Press Publishers
H.U.P.	Harvard University Press
L.G.D.J.	Librairie Générale de Droit et de Jurisprudence
M.N.P.	Martinus Nijhoff Publishers
N.A.P.	National Academies Press

Prace W.T.N.	Prace Wrocławskiego Towarzystwa Naukowego
O.U.P.	Oxford University Press
O.S.U. Press	Ohio State University Press
U.G.A. Press	University of Georgia Press
Y.U.P.	Yale University Press

Dictionaries

Black's	Black's Law Dictionary
O.E.D.	Oxford English Dictionary

ABSTRACT

States have spied on each other for centuries, raising tensions. Yet, express regulation may only be found in the law of war. While spies may be caught and punished, it is paradoxically admitted that sending them does not breach international law. As to peacetime espionage, no similar convention exists, and it has never been expressly prohibited or authorized. An indirect regulation may nevertheless be found in the rule of territorial sovereignty, as–lacking its consent–sending an agent on the soil of another state would be illegal. This echoes states' ambivalent position on the international stage. They have indeed always sent spies to foreign territories. When those agents were caught, the targeted states punished them in accordance with their domestic law, protested or exchanged them. However, the applicability of this framework is challenged by the emergence of cyber-espionage, as a physical intrusion by an agent is not required anymore. Thus, this thesis' leading question is whether the dematerialization and de-territorialisation of spying prevents the application of international rules to cyber-espionage.

Facing this lack of express regulation and changes, doctrine has tried to fill this loophole. Authors usually propose to apply existing treaties, examine the legality of cyber-spying in the light of sovereignty and non-intervention, or try to identify new customary rules. However, this thesis finds numerous problems in these approaches, as only sparse reference to the rules of treaty interpretation contained in the Vienna Convention on the Law of Treaties (VCLT), the draft conclusions of the International Law Commission (ILC) on the 'Identification of customary international law', and even state practice may be found. Then, many analogies rely on the false assumption that cyberspace and land are similar.

Seven instruments are under review in this thesis. To determine what they have to say about cyber-spying, this research proposes to resort to the VCLT rules of interpretation, the ILC draft conclusions, and to systematically incorporate the maximal amount of state practice. This thesis finally concludes that sovereignty, the Charter of the United Nations, and the Agreement on Trade-Related Aspects of Intellectual Property Rights are silent regarding cyber-espionage. Then, it finds that cyber-espionage *per se* does not violate the rule of non-intervention. It also finds that most of wartime rules are inapplicable, while cyber-spying is neither authorized, nor forbidden by customary international law. The sole surveillance of electronic archives, documents and correspondence goes against the Vienna Convention on Diplomatic Relations.

DECLARATION

This thesis has also been submitted to the *Communauté Université Grenoble Alpes* in line with a Joint-PhD agreement with the University of Manchester.

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning

COPYRIGHT STATEMENT

DEDICATION

This work is dedicated to my parents, Christophe and Anne, and to my grand-parents, Bernard and Marie-Jo. For their love and caring.

ACKNOWLEDGEMENT

It is the twilight of the academic year in Manchester, and such is at present the case for my journey throughout this PhD. In some days, I will leave my adopted city, now empty of students, and fly back to a small village somewhere in the French Alps–*home*. And, in some months, I hope to reap the rewards of this effort: 'my' PhD degree. It is the end of an era, and–hopefully–the beginning of new adventures!

The last few years have been a highly instructive and unforgettable moment., and it is now time to thank those who have contributed to it.

First and foremost, I would like to express my gratitude to my supervisors–Professors Iain Scobbie, Jean d'Aspremont and Théodore Christakis–for their dedication, benevolence and continual advice. Approaching international law with a critical eye, perpetual questioning, and integrity in research will remain their most precious legacy.

Then, I would like to thank my examiners–Professors Duncan Hollis, Nicholas Tsagourias, Tobby Seddon, Dr Karine Bannelier-Christakis and Dr Michael Galanis–for their presence at my viva and their useful comments.

This work would not have been possible without the support of the *COMUE Grenoble-Alpes*, which have allowed me–through a doctoral contract and various research fundings (*IDEX*, *Initiatives d'Excellence,* the *Projet SHS*)–to fully dedicate myself to my research.

I then feel very privileged to have met so many great fellows in Manchester: Ajmal, Antal, David(s), Elena, Kriton, Mariela, Masha and Martin, Max, Ruben, Sean... By your side, I have experienced unforgettable moments, both within Williamson Building–and outside: doing tourism on the shores of Volga river, attending a wedding in an authentic steam train moving through the English countryside, or simply having exciting discussions in the pubs of Manchester. I would also like to thank my old friends (Andrea, Camila, Emmanuel, Ivan, Mirko and Michael) for these refreshing moments throughout Europe. Köszönöm; спасибо; ευχαριστώ; gracias; grazie; merci – Thank you! Thanks, also, to the members of the administrative staff.

My PhD–and life experience–would have been very different without my cousins and confidants, Jeanne-Marie and Pierre-Marc. Thank you for your presence and your attentive ear, at any time!

I would like to express very special thanks to my grand-parents, Bernard and Marie-Jo. They have attentively followed my progression since my childhood, expressing an unwavering faith in my success. I am also thinking to the other members of my family (Béatrice and André, Bertrand and Vanina, Thierry and Françoise, my cousins…)

Last but not least, I would like to thank my parents, Christophe and Anne. They formed me into the man I am today. Thanks also to my sisters, Coralie and Ludmilla, for standing on my sides.

Manchester, 30 June 2018 / Jerusalem, 18 November 2019.

INTRODUCTION

On the occasion of an interview in 2010, Julian Assange stated that '[i]ntelligence agencies keep things secret because they often violate the rule of law or of good behavior'.[1] Further clarification should nevertheless be added. First, intelligence agencies exist to preserve the common welfare–whether economic or security–of the population they are supposed to serve. Second–and in carrying out this mission, including through spying or cyber-espionage–they may actually violate the domestic laws of other states. However, they usually operate within a legal framework, i.e. the law of their state of allegiance. As highlighted by the former director of French foreign intelligence services, Bernard Bajolet, 'the NSA [National Security Agency] has to comply with American law, as the DGSE [French General Directorate for External Security] has to comply with French law'.[2] As a consequence, espionage is not a legal vacuum, but rather–and at least–a mesh of antagonistic domestic laws. The motto of the Australian Signals Directorate (ASD) is self-explanatory: 'Reveal Their Secrets–Protect Our Own'. The role of international law is a different question, and will lengthily be tackled all throughout the thesis. As of now, two main challenges may be introduced. While an express reference to espionage may only be found in conventional wartime law, cyber-espionage has no basis in any treaty. Then, the existence of most international rules precedes the emergence of the Internet. Upon signing the Patriot Act,[3] George W. Bush underlined that '[e]xisting law was written in the era of rotary telephones […] This new law […] will allow surveillance of all communications used by terrorists, including e-mails, the Internet and cell phones […] As of today, we'll be able to better meet the technological challenges posed by this proliferation of communications technology'.[4] While a major part

---

[1] Andy Greenberg, 'An Interview With WikiLeaks' Julian Assange', *Forbes* (29.11.2010) <www.forbes.com/sites/andygreenberg/2010/11/29/an-interview-with-wikileaks-julian-assange/8/#1e3eb8747153> accessed:03.05.2018.

[2] Assemblée nationale (AN), 'Avis fait au nom de la Commission de la défense nationale et des forces armées sur le projet de loi (no 2669) relatif au renseignement', No.2691 (31.03.2015) 79 <www.assemblee-nationale.fr/14/pdf/rapports/r2691.pdf> accessed:03.05.2018.

[3] An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigative tools, and for other purposes ('Patriot Act') (2001) Pub L 107–56, 115 STAT 272.

[4] 'Text: Bush Signs Anti-Terrorism Legislation', *WP* (25.10.2001)

of international law was actually 'written in the era of rotary telephones', adopting 'new law' has proved to be difficult in the digital age. According to Jolley, '[t]he international legal framework has been slow to adapt to the changes brought by the Internet and the "information society" that has evolved in the Internet's wake [...] States and scholars have: (1) ignored the Internet, (2) attempted to regulate the Internet through analogy to older technologies such as the telephone, telegraph, and wire services; and (3) attempted to legislate the Internet via domestic and international legislation'.[5] Barrie synthetizes the doctrinal method as follows: 'one is forced to make assumptions and deductions from modern international law instruments'.[6] The methods used by doctrine are actually a bit richer. They include the direct application of existing treaty provisions to cyber-espionage, as well as the resort to meta-principles of interpretation (analogical, consequentialist and target-based approaches) and the quest for international customary rules. However, this thesis finds numerous problems in these typical approaches. First, the direct application of treaties and meta-principles of interpretation is carried out at the expense of the official rules of interpretation contained in the Vienna Convention on the Law of Treaties (VCLT).[7] Second, many instances of analogical reasoning rely on the wrong assumption that cyberspace and land are similar. Third, the quest for CIL rarely follows the draft conclusions of the International Law Commission (ILC) on the 'Identification of customary international law'. Fourth, a sufficiently representative sample of state practice is a notable absentee in most academic work. Yet, this element is an essential one, whether in terms of treaty interpretation, assessment of customary international law (CIL), or application of sovereignty and non-intervention with respect to cyber-espionage. What is proposed in this thesis is to resort to the VCLT rules of interpretation, the draft conclusions of the ILC and to systematically incorporate the maximal amount

<www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushtext_102601.html> accessed:03.05.2018.

[5] Jason Jolley, 'Attribution, state responsibility, and the duty to prevent malicious cyber-attacks in international law' (PhD thesis, University of Glasgow, 2017) 2.

[6] George Barrie, 'Spying–an international law perspective' (2008) 2 J.S.Afr.L. 238, 238.

[7] Vienna Convention on the Law of Treaties ('VCLT') (adopted:23.05.1969-EIF:27.01.1980) 1155 UNTS 331.

of state practice. In this introductory note, the structure and main methodological choices are first explained (1). Then, the main assumption of this thesis is developed–i.e., the relevance of international law in cyberspace (2). A definition of the main concepts is moreover provided (3). Finally, the conceptual framework is developed (4).

1. Structure and main methodological choices

The research question, objectives and methods (1.1), as well as the structure of the dissertation (1.2) have to be introduced.

1.1. Research question, objectives and methods

As this thesis further demonstrates, cyberspace cannot be assimilated to land, sea, airspace, or outer-space.[8] It is indeed a new and de-territorialized 'fifth domain'. In such conditions, espionage activities go through a radical change: they are dematerialized, i.e. they do not require a physical intrusion–the sending of an agent on the territory of a foreign state–and are carried out remotely. Yet, many international rules were conceived when the Internet was non-existent, and in relation to a physical paradigm. Thus, the question at issue is whether the dematerialization and de-territorialisation of spying prevents the application of international rules to cyber-espionage. To proceed, this thesis establishes five objectives:

A. To identify patterns of reasoning in doctrinal works;
B. To apply the VCLT rules of interpretation to existing treaties, and contribute to establishing the status of cyber-espionage law;
C. To apply the ILC draft conclusions in the quest for CIL, and contribute to establishing the status of cyber-espionage law;

[8] See Ch.I-IV.

D. To determine whether the rules of territorial sovereignty and non-intervention are applicable to cyber-espionage, and contribute to establishing the status of cyber-espionage law;
E. To compare the status of doctrine and the status of law, thus revealing the gaps in the former.

To fulfil each of these objectives, original research methods have been resorted to and need to be explained.

A. Objective 1: The identification of reasoning patterns in doctrine

To identify patterns in doctrinal reasoning, it was first necessary to read the maximal number of doctrinal works related to espionage, cyber-espionage, and interception of telecommunications.

First, this phase identified the legal instruments used by doctrine. Many of them were related to wartime espionage, including rules of land warfare: Lieber Code, Declaration of Brussels, Oxford Manual, The Hague Conventions of 1899 (Hague II)[9] and 1907 (Hague IV),[10] and Additional Protocol I to the Geneva Conventions.[11] However, some references to draft conventions on naval[12] and air warfare[13] were also identified. As to peacetime traditional espionage, references to the following elements were found: peaceful cooperation, territorial integrity, the United Nations Convention on the Law of the Sea (UNCLOS),[14] unlawful intervention, reciprocity, CIL, human rights law (HR),

[9] Convention (II) with Respect to the Laws and Customs of War on Land ('Hague II') (Adopted:29.07.1899–EIF:04.09.1900).

[10] Convention (IV) respecting the Laws and Customs of War on Land ('Hague IV') (Adopted:18.10.1907–EIF:26.01.1910)

[11] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts ('Additional Protocol I') (adopted:08.06.1977–EIF:07.12.1978) 1125 UNTS 3.

[12] Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War ('Hague XIII') (adopted:18.10.1907–EIF:26.01.1910).

[13] The Hague Rules of Air Warfare ('The Hague Air Rules') (adopted:19.02.1923).

[14] United Nations Convention on the Law of the Sea ('UNCLOS') (Adopted:10.12.1982–EIF:16.11.1994) 1833 UNTS 397

international crime, unfriendly acts, the Vienna Convention on Diplomatic Relations (VCDR),[15] arms control, and domestic law. When it came to cyber-espionage, references were usually made to both *jus in bello*–including rules related to the duties of neutral powers–and *jus ad bellum* (the Charter of the United Nations),[16] territorial integrity, non-interference, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS),[17] and CIL. The VCDR, non-intervention, unfriendly acts, sovereignty, HR law, good faith, the Constitution of the International Telecommunication Union (ITU),[18] and CIL were invoked for the interceptions of communications.

Second, their reasoning and arguments were mapped, and to determine patterns. The analogy between espionage and cyber-espionage proves to be a recurrent mode of reasoning in the application of sovereignty, *jus ad bellum* (JAB) and *jus in bello* (JIB). However, resort to consequentialist and target-based approaches is also common in the application of JAB. Doctrine also tends to directly apply the rules of non-intervention (demonstrating the existence of coercion and/or exclusive domestic jurisdiction), the VCDR (articles 3, 41(1), 22, 24, 27(2)), TRIPS (articles 3, 39, 73).

Sparse references to state practice may be found in doctrinal works, with the exception of some examples in the application of the VCDR and CIL. In the first situation, some authors consider that diplomatic espionage is so widespread that it is now legal. In the second situation, state practice is associated with *opinio juris* in the quest for customary rules.

The collection of secondary sources is part of doctrinal research. In this framework, '[t]he researcher seeks to collect and then analyse a body of case-law, together with any relevant legislation (so-called primary sources) [...] This

---

[15] Vienna Convention on Diplomatic Relations ('VCDR') (adopted:18.04.1961–EIF:24.04.1964) 500 UNTS 95

[16] Charter of the United Nations and Statutes of the International Court of Justice ('UN Charter') (Adopted:26.06.1945–EIF:24.10.1945).

[17] General Agreement on Trade-Related Aspects of Intellectual Property ('TRIPS') (Annex 1C of Marrakesh Agreement Establishing the World Trade Organization) 1869 UNTS 299.

[18] Constitution and Convention of the International Telecommunication Union (Adopted:22.12.1992–EIF:01.01.1994) 1825 UNTS 331.

[...] may also include secondary sources such as journal articles or other written commentaries on the case law and legislation'.[19] This phase of research is also of descriptive inspiration. 'Descriptive research involves gathering data that describe events and then organizing, tabulating, depicting, and describing the data collection'.[20] This methodology may be used 'as a tool to organize data into patterns that emerge during analysis'.[21]

B. *Objective 2: Treaty interpretation*

Among the instruments identified in doctrinal works, the UN Charter (JAB), The Hague Convention II (1899), IV and V (1907), as well as the Additional Protocol I (1977) (JIB), the VCDR, TRIPS, were analysed, while HR, the ITU Constitution, bilateral and regional treaties were left out.

To exploit these conventions, it was necessary to set up a theoretical framework on treaty interpretation. It started with reading theory, through which the main debates and case-law surrounding treaty interpretation were identified. While articles 31 to 33 of the VCLT are quite clear regarding the textual method to be applied, they do not expressly tackle some aspects of interpretation: evolutionary interpretation, strict and extensive interpretation, the interpretation of the constitutive treaties of international organisations (IO/IO's). To tackle these issues, an investigation of case-law from the Permanent Court of International Justice (PCIJ), the International Court of Justice (ICJ), the European Court of Justice (ECJ), the European Court of Human Rights (ECtHR) and the Inter-American Court of Human Rights (IACtHR) was carried out, with a subsequent mapping of any provision of interest. It revealed that their interpretation had to be done in accordance with parties' intentions, as reflected in the text. The customary nature of the VCLT rules was also revealed.

---

[19] Ian Dobinson and Francis Johns, 'Qualitative Legal Research' in Mike McConville (ed), *Research Methods for Law* (E.U.P. 2007) 18-19.

[20] AECT, 'The Handbook of Research for Educational Communications and Technology' (*aect,* 03.08.2001)
<www.aect.org/edtech/ed1/41/41-01.html> accessed:31.12.2017.

[21] Ibid.

This method was then applied to the treaties of interest. First, the terms of the provisions were defined using dictionaries. The dictionaries chosen are those used by the ICJ and the ECtHR: The *Oxford English Dictionary*,[22] *Black's Law Dictionary*, [23] *Encyclopaedia Britannica*, [24] and *Merriam-Webster* for the English language;[25] *Larousse* for the French language.[26] Other dictionaries referred to by case-law, but not used in this thesis includes the *Shorter Oxford Dictionary*,[27] and *Webster* for the English language;[28] *Littré*,[29] *Hatzfeld et Darmesteter*,[30] the *Dictionnaire de la terminologie du droit international*,[31] and *Robert* for the French language.[32] Second, the context of the provisions, as well as the object and purpose of the treaties were ascertained. Third, significant attention was paid to subsequent agreement, practice and rules of international law, which may be taken into account 'together with the context'. They were established using the resolutions of the United Nations General Assembly (UNGA), states' communications with the UNGA, national military, security and cyber strategies, parliamentary debates, WTO case-law, and the archives from Keesing's World News.

---

[22] *Oil Platforms (Iran v USA)* (Preliminary Objection, Judgment) [1996] ICJ Rep 803, 818; *Separate Opinion* (SO) *Cançado Trindade* in *Request for Interpretation of the Judgment of 15 June 1962 in the Case concerning the Temple of Preah Vihear (Cambodia v Thailand) (Cambodia v Thailand)* (Judgment) [2013] ICJ Rep 281, 328; SO *Owada* in *Application of the International Convention for the Suppression of the Financing of Terrorism and of the International Convention on the Elimination of All Forms of Racial Discrimination (Ukraine v Russian Federation)* (Order of 19.04.2017) 4 <www.icj-cij.org/files/case-related/166/19395.pdf> accessed:07.04.2018.

[23] *Oil Platforms* (n.22) 818; *SO Bandhari* in *Obligations concerning Negotiations relating to Cessation of the Nuclear Arms Race and to Nuclear Disarmament (Marshall Islands v UK)* (Preliminary Objections) [2016] ICJ Rep 833, [4]; *SO Cançado Trindade* (n.22) 328.

[24] *SO Abi-Saab* in *Frontier Dispute (Burkina-Faso/Mali)* (Judgment) [1986] ICJ Rep 554, 662.

[25] *SO Owada* (n.22) 4.

[26] *SO Abi-Saab* (n.24) 662; *Luedicke, Belkacem and Koç v Germany* (1978) 2 EHRR 149, [40]; *SO Owada* (n.22) 4; *SO Cançado Trindade* (n.22) 51.

[27] *Luedicke, Belkacem and Koç* (n.26) [40].

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] *Oil Platforms* (n.22) [45]; *Luedicke, Belkacem and Koç* (n.26) [40]; *Golder v The UK* (1975) 1 EHRR 524, [32].

[32] *Luedicke, Belkacem and Koç v Germany* (n.26) 40; *Golder* (n.31) [32]; *SO Cançado Trindade* (n.22) 51.

This aspect of research is essentially doctrinal, which is a 'type of research' that 'focuses on the legal rules themselves, to work out what the law says on a particular issue and why it says it'.[33] This 'traditional view of law' consists of regarding 'law as a set of legal rules derived from cases and statutes, which are applied by a judge who acts as a neutral and impartial referee seeking to resolve a dispute'.[34] 'On this view [...] legal reasoning is simply a matter of looking up the rule of law (in statutes and case-books), applying them to the facts of the problem […] and by this process arriving at the "right" result'.[35] Doctrinal research has sometimes been described as 'applying the relevant legal rules to the particular facts of the situation under consideration'.[36] Moreover, '[t]he main technique of doctrinal research is [...] interpretation'.[37]

C. Objective 3: Ascertaining customary international law

The first phase of research highlighted a certain doctrinal interest in CIL, but high divergences in their final conclusions on the legality of cyber-espionage and insufficient consideration of state practice. This research thus proceeded to its own quest for customary rules.

As previously done for treaty interpretation, setting up a theoretical framework was necessary. Reading the 'official' rules on the identification of CIL was a starting point, with the *North Sea Continental Shelf*, *Nicaragua* and *Gulf of Maine* cases, as well as Michael Wood's reports, and the subsequent draft conclusions of the ILC. While additional readings and the mapping of every ICJ case-law

---

[33] Graham Virgo, 'doctrinal legal research' in Peter Cane and Joanne Conaghan (eds), *The New Oxford Companion to Law* (O.U.P. 2008) 339.

[34] Marie Fox and Christine Bell, *Learning Legal Skills* (3rd edn, Blackstone 1999) 9.

[35] Ibid 239.

[36] Paul Chynoweth, 'Legal Research' in Andrew Knight and Les Ruddock (eds), *Advanced Research Methods in the Built Environment* (Blackwell 2008) 29.

[37] Maria Smirnova, 'Is the Right to Education a New "Jus Cogens" of Our Times? Methodology of Research' (2013) 7
<https://ssrn.com/abstract=3088502> accessed:31.12.2017.

connected to CIL revealed some issues with its identification, the ILC draft conclusions remain the reference point in identifying potential customary rules related to cyber-espionage. The documents used to ascertain practice and *opinio juris* were usually collected on the Internet–including the websites of the respective intelligence agencies–and yearbooks of international law. Some remarks should nevertheless be made with respect to these materials. First, most of these yearbooks are of Western origin, and the content of the most recent years is still not available online. Then, very few African countries add their legislation online, while Asian laws are rarely translated into English, French, German or Spanish. As a consequence, practice from Europe, Oceania, North and South America is more represented than Asia and Africa. It also happens that translations are available, but not up-to-date.[38] In such situations, the materials were handled with care, with the date of the version mentioned in the text.

This method is a hybrid one, and could be qualified as document analysis, but empirically-inspired. The materials used are documents in essence. '[A] document is a written text',[39] while '[d]ocument analysis is a systematic procedure for reviewing or evaluating documents–both printed and electronic (computer-based and Internet-transmitted) material'.[40] The different types of documents include '[o]fficial data and records', '[o]rganizational communication, documents and records' (including 'websites' and 'press releases'), '[p]ersonal communication, documents, and records', '[t]he media/contemporary entertainment', '[t]he Arts', and '[s]ocial artefacts'.[41] However, their mode of collection is inspired by quantitative empirical research. 'What makes research empirical is that it is based on observations of the world, in other words, data, which is just a term for facts about the world. These facts may be historical or

[38] For some texts in Chinese, Greek, Turkish, and Russian, I resorted to unofficial translations before having the meaning confirmed by a native speaker.

[39] Monageng Mogalakwe, 'The Use of Documentary Research Methods in Social Research' (2006) 10(1) African Sociological Review 221, 222.

[40] Glenn Bowen, 'Document analysis as a Qualitative Research Method' (2009) 9(2) Q.R.J. 27, 27.

[41] Zina O'Leary, *The Essential Guide to doing your Research Project* (2nd edn, Sage 2010) 219-20.

contemporary, or based on legislation or case law, or the outcomes of secondary archival research or primary data collection [...] As long as the facts have something to do with the world, they are data, and as long as research involves data that is observed or desired, it is empirical'.[42] Then, '[a]s a general rule, researchers should collect as much data as resources and time allow because basing inferences on more data rather than less is almost always preferable […]'.[43] As required by the ICJ and Wood's reports, this method allows an inductive process.

D. Objective 4: The evaluation of territorial sovereignty and non-intervention

The assessment of territorial sovereignty and non-intervention have a common feature: they essentially rely on a large investigation of state practice. This need for a tailor-made method is justified by various elements. The respect for territorial sovereignty and non-intervention stems from the principle of sovereignty, which itself stems from the treaty of Westphalia (1648). However, the binding character of both rules cannot be connected to any treaty or source in particular. Respect for territorial sovereignty has been incorporated in several conventions,[44] and violations are regularly denounced by states and condemned by tribunals, giving rise to reparations.[45] The same happened with non-intervention, even if ICJ's contribution was decisive: it defined the elements of a prohibited intervention and ruled that non-intervention 'is part and parcel of customary international law'.[46] Admittedly, the ICJ accepted to adapt the VCLT

---

[42] Lee Epstein and Gary King, 'The Rule of Inference' (2002) 69(1) U.Chi.L.Rev. 1, 2-3.

[43] Lee Epstein and Andrew Martin, 'Quantitative Approaches to Empirical Legal Research', in Peter Cane and Herbert Kritzer (eds), *The Oxford Handbook of Empirical Legal Research* (O.U.P. 2010) 910.

[44] Convention on International Civil Aviation (Adopted:07.12.1944–EIF:04.04.1947) art.1; UNCLOS, art.2; UN Charter, art.2(4).

[45] See Chapter I-I.

[46] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA)* (Judgment) [1986] ICJ Rep 14, [202].

rules for the purpose of interpreting resolutions of the Security Council[47] and declarations recognizing the jurisdiction of the Court as compulsory.[48] But no evidence of the right way exists for territorial sovereignty and non-intervention.

To assess sovereignty, it was resorted to document analysis, quantitative and qualitative research (which 'is used to gain an understanding of underlying reasons, opinions, and motivations').[49] To determine whether states considered cyber-espionage as a violation of sovereignty–and explaining the motivations underlying their positions–a maximal amount of state practice was collected in military doctrines, secret service and government documents, parliamentary practice, UNGA resolutions and its communications with states, press articles, and positions expressed in the IOs. A similar approach was taken for both elements of non-intervention. A more literal approach was however taken to define 'coercion', which is vital to determine whether an intervention is prohibited or not.

E. Objective 5: The comparison of the 'status of doctrine' and the 'status of law'

A literature review 'allows the author to critically evaluate the quality of existing scholarly writings and to identify best research techniques and practices'.[50] Moreover, it 'can help to put this thesis in context by identifying how it will differ from that of other scholars, making it an original contribution to the subject area'.[51] This is actually what mapping and establishing patterns of doctrinal reasoning made possible in this thesis. Doctrinal gaps were mentioned

---

[47] *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo (Advisory Opinion)* [2010] ICJ Rep 403, [94].

[48] *Fisheries Jurisdiction Case (Spain v Canada)* (Jurisdiction) [2008] ICJ Rep 432, [46].

[49] Susan DeFranzo, 'What's the difference between qualitative and quantitative research?' (*snapsurveys*, 16.09.2011) <www.snapsurveys.com/blog/qualitative-vs-quantitative-research/> accessed:01.01.2018.

[50] Lachmi Singh, 'The United Nations Convention on Contracts for the International Sale of Goods 1980 (CISG): an examination of the buyer's remedy of avoidance under the CISG' (PhD thesis, University of the West of England, 2015) 28.

[51] Ibid.

in the introduction: 1) the insufficient resort to the VCLT rules of interpretation; 2) analogies relying on the wrong assumption that land and cyberspace are similar; 3) the lack of reference to the ILC draft conclusions; 4) an insufficient investigation of state practice. By intending to compensate for these gaps, this thesis makes an original contribution to the subject area. It resorts to a systematic and unique inclusion of state practice, the rigorous reliance on both the VCLT's cannons of treaty interpretation and the ILC draft conclusions on CIL.

Some details should be added about the Tallinn Manuals. The first edition ('Tallinn Manual 1.0') focused on the law applicable to 'cyber warfare'[52]–a scope extended in the second version ('Tallinn Manual 2.0'), dedicated to 'cyber operations'.[53] The latter postulates that the 'lack of cyber-specific international law does not mean […] that cyber operations exist in a normative void', and considers that 'existing international law applies to cyber operations'.[54] It 'is intended as an objective restatement of the *lex lata'*, and its rules are supposed to 'reflect customary international law […] as applied in the cyber context'.[55] Allegedly, '[t]o the extent the rules accurately articulate customary international law, they are binding on all States, subject to the possible existence of an exception for persistent objectors'.[56] However, Tallinn Manuals have not been adopted by states or IO's, and do 'not represent the views of the NATO CCDCOE, its sponsoring nations, or NATO'.[57] Rather, they result from the work of an 'independent group of experts' convened by the CCDCOE, a NATO 'research and training institution'.[58] Admittedly, the Manuals have received considerable attention: more than fifty states took part in the 'Hague Process', when Dutch MFA Koenders 'convened States to unofficially comment on the

[52] Michael Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (C.U.P. 2013).

[53] Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (C.U.P. 2017).

[54] Ibid 3.

[55] Ibid 3-4.

[56] Ibid 4.

[57] Schmitt, *Tallinn Manual 1.0* (n.52) 11; Schmitt, *Tallinn Manual 2.0* (n.53) 2.

[58] Schmitt, *Tallinn Manual 2.0* (n.53) 1.

working drafts of the Manual […]'.[59] But in parallel, states distanced themselves from the Manual. The closing speech of Minister Koenders is enlightening: '[t]he Tallinn Manual does not provide the answers to all the questions. It is not an official document, and the Netherlands does not necessarily agree with everything in it […] the conversation must continue'.[60] Brian Egan had a similar approach: '[t]he United States has unequivocally been in accord with the underlying premise of this project, which is that existing international law applies to State behavior in cyberspace. In this respect, the Tallinn Manuals will make a valuable contribution to underscoring and demonstrating this point across a number of bodies of international law, even if we do not necessarily agree with every aspect of the Manuals'.[61] Efrony and Shany further note that 'certain key Rules in the Tallinn Manuals' have received 'only limited support', and that 'several' states 'have a limited interest in promoting legal certainty regarding the regulation of cyberspace'.[62] The thesis thus considers Tallinn Manuals as an academic exercise and a valuable doctrinal application of existing international law to cyberspace. While many norms invoked in the Manual are customary and thus, *de lege lata*, this thesis considers that their interpretation and application to cyber-activities are *de lege ferenda.* Lacking any official state endorsement, it is thus tackled in the 'status of doctrine'.

The research question, objectives and methods have been explained. Their influence on the structure of the thesis is now considered.

---

[59] Ibid 6.

[60] Bert Koenders, 'Speech Tallinn Manual 2.0' (2017) <www.rijksoverheid.nl/binaries/rijksoverheid/documenten/toespraken/2017/02/13/toespraak-minister-koenders-bij-presentatie-tallinn-manual-2.0/Speech+TALLINN+MANUAL+2.0.pdf> accessed:26.10.2018.

[61] Brian Egan, 'Remarks on International Law and Stability in Cyberspace' (10.11.2016) <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm> accessed:30.11.2017.

[62] Dan Efrony and Yuval Shany, 'A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice' (2018) 112(4) A.J.I.L. 583, 585.

1.2. Structure of the thesis

First, this thesis' main divisions are evoked, with the duality between 'the rules connected to territorial integrity' and 'the rules disconnected from territorial integrity', as well as the investigation of 'a special customary law on cyber-espionage' (A). Then, this thesis' chapters share a common division: the 'status of doctrine' and the 'status of law'. This construction is thus justified (B). The scope of this thesis and the exclusion of HR, bilateral and regional treaties are finally evoked (C).

A. Main divisions of this research: 'the rules connected to territorial integrity', 'the rules disconnected from territorial integrity', 'a special customary law on cyber-espionage'

The rules of sovereignty, non-intervention, JAB, and JIB share a common goal: regulating states' behaviours towards foreign territories, and preserving territorial integrity.[63] Such is not the case for the VCDR and TRIPS. Under the VCDR, diplomats have to comply with the receiving state's domestic law, while the latter must ensure the inviolability of diplomatic premises and correspondence. TRIPS does not contain any extraterritorial obligations. Yet–and as explained previously–the effects of espionage dematerialization and de-territorialisation on the applicability of international law is central to this thesis. The first two main parts of this doctoral thesis reflect this divergence, with the study of the rules connected to territorial integrity on the one hand (first part), and the rules disconnected from territorial integrity on the other hand (second part). It is interesting to see how these two bodies of rules may adapt. Finally, the references to new and special customary rules prohibiting or authorizing cyber-espionage *per se* are more and more frequent in literature. As this phenomenon is not related to the transposition of existing rules, this thesis proposes to study it in a third part. This plan is didactic, functional, and increases readability.

[63] A potential caveat is nevertheless acknowledged for non-intervention, as a prohibited intervention is not systematically at odd with territorial integrity.

As comparing the status of doctrine and the status of law are among the objectives of this thesis, a recurrent duality may be found in each chapter of this thesis.

B. Common divisions of the chapters: the 'status of doctrine', the 'status of law'

Each chapter of this doctoral dissertation is subdivided the same way, i.e. the 'status of doctrine' and the 'status of law'. They represent the two goals of this thesis: to ascertain both the status of doctrine and the status of law with respect to cyber-espionage. The status of doctrine corresponds to a classification of authors' and experts' arguments, introduced in a neutral fashion. The goal is to map, not to discuss them. While authors reach various conclusions, their reasoning presents patterns that are highlighted thanks to this classification. This work is decisive in realizing that references to the VCLT and state practice are insufficient in many doctrinal works. This thesis intends to correct these flaws and develop its own vision of law in the sub-chapter entitled 'status of law'.

While establishing the status of conventional law on cyber-espionage is an objective of this thesis, some instruments had to be excluded, and the scope of this research, determined.

C. Scope of this thesis and exclusion of human rights, regional, bilateral treaties, the ITU Constitution and general principles of law

HR treaties are potentially relevant to cyber-espionage activities, as they quasi-systematically involve a data breach. However, much has been written on mass surveillance,[64] and this thesis' goal is to focus on an aspect that received less

[64] See: Ilina Georgieva, 'The Right to Privacy under Fire–Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31 Utrecht J.Int'l.&Eur.L. 104; Courtney Giles, 'Balancing the Breach: Data Privacy Laws in the Wake of the NSA Revelations' (2015) 37(2) Hous.J.Int'l.L. 543; Daniel Joyce, 'Privacy in the Digital Era: Human Rights Online?' (2015) 16 Melb.J.Int'l.L. 270; Peter Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism' (2014) 82(5) Ford.L.R. 2137; Jordan Paust, 'Can You Hear Me Now?: Private Communication, National Security, and the Human Rights Disconnect' (2014-2015) 15 U.Chi.L.Rev. 612. Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015)

attention: economic, politic, military and diplomatic cyber-espionage.[65] As to the ITU, it has recently developed an interest in cyberspace. An analysis of its Constitution was originally present in this thesis, but had to be removed due to space constraints. It however fails to prohibit cyber-espionage, and doctrine is unanimous on this aspect.[66] Applying domestic law indeed prevails over the secrecy of international correspondence,[67] while its prevention of harmful interferences only applies to the jamming of radio services.[68] The task of studying regional treaties and bilateral agreements is unfortunately too large to be included in a doctoral thesis. Doctrine is also rare with respect to them, and would have allowed less debate.[69] The latter point only partially explains why general principles of law are not tackled. To the extent that states adopt a common approach to espionage in their domestic law–by prohibiting others to spy on them, but authorizing themselves to spy on the others–studying general principles of law might appear as relevant. Exceptionally, some substantial rights were qualified as such: *uti possidetis juris*,[70] the unlawfulness of genocide and the need to combat it[71]–perhaps, also, the right to self-determination.[72] However,

---

56 Harv.Int'l.L.J. 81. Marko Milanovic, 'Blockbuster Strasbourg Judgment on Surveillance in Russia' (*EJIL:Talk!,* 07.12.2015) <www.ejiltalk.org/blockbuster-strasbourg-judgment-on-surveillance-in-russia/> accessed:14.05.2018

65 These forms of espionage respectively aim at economic, politic, military and diplomatic secrets. They may nevertheless be intertwined, for instance during the development of a new weapon.

66 Craig Forcese, 'Spies without borders: international law and intelligence collection' (2011) 5 Nat'l Security L.&Pol'y 179, 209; John Kish and David Turns, *International Law and Espionage* (M.N.P. 1995) 49; Fabien Lafouasse, *L'Espionnage dans le Droit International* (Nouveau Monde 2012) 161.

67 ITU Constitution, art.37.

68 Ibid art.45.

69 Among the rare doctrinal works on the topic, see: Robert Van Arnam, 'Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection' (2001) 27 N.C.J.Int'l.L.&Com.Reg. 95; Giliam de Valk, 'Mind the gap: economic espionage within the EU' (*Leiden Safety and Security Blog*, 20.11.2017) <www.leidensafetyandsecurityblog.nl/articles/mind-the-gap-economic-espionage-within-the-eu> accessed:22.02.2018.

70 *Frontier Dispute* (n.24) [20].

71 *Reservations to the Convention on Genocide* (Advisory Opinion) [1951] ICJ Rep 15, 12.

72 *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)* (Advisory Opinion) [1971] ICJ Rep 16, [52].

the PCIJ and the ICJ have traditionally consecrated processual principles: *nemo auditur*,[73] reparation following the breach of an engagement,[74] respect of vested rights,[75] *res judicata*,[76] 'no one can be judge in his own suit',[77] indirect evidence,[78] the binding character of orders for provisional measures,[79] the fact that 'questions of immunity are [...] preliminary issues which must be expeditiously decided *in limine litis'*.[80] However, espionage hardly fits in this trend, and its regulation by general principles is thus hardly conceivable. In addition, the method of the ICJ is often criticized. As underlined by Hernandez, '[t]he Court and its predecessor have never conducted a survey of municipal law to support their conclusion as to the existence of a general principle', and 'has rarely made reference' to it 'when seeking properly to discern what general principles might exist even when that information has been made available by parties'.[81] Moreover, 'it can be argued that references to general principles by the ICJ, in particular, often manifest a reliance of the Court on customary international law'.[82] Finally, whether the absence of law on espionage is a *lacuna* may be discussed: states may have deliberately avoided to adopt rules on the topic.

---

[73] *Case concerning the Factory at Chorzów (Germany v Poland)* (Claim for Indemnity, Jurisdiction) [1927] PCIJ Rep Series A No.9, 31.

[74] Ibid 21.

[75] Ibid 28.

[76] *Effect of Awards of Compensation Made by the UN Administrative Tribunal (Advisory Opinion)* [1954] ICJ Rep 47, 53.

[77] *Article 3, Paragraph 2, of the Treaty of Lausanne (Advisory Opinion)* [1925] PCIJ Rep Series B No.12, 32.

[78] *Corfu Channel Case (UK v Albania)* (Judgment) [1949] ICJ Rep 4, 18.

[79] *LaGrand (Germany v USA)* (Judgment) [2001] ICJ Rep 466, [103].

[80] *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights* (Advisory Opinion) [1999] ICJ Rep 62, [63].

[81] Gleider Hernandez, *The International Court of Justice and the Judicial Function* (O.U.P. 2014) 261.

[82] Jean d'Aspremont, 'What Was Not Meant to Be: General Principles of Law As a Source of International Law' (2017) 11 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3053158> accessed:01.11.2018.

By investigating what international law has to say about cyber-espionage, this thesis actually relies on a main assumption: that this international law is relevant in cyberspace.

2. Main assumption: the relevance of international law

As this thesis further demonstrates, cyberspace is a new and unphysical domain. In such circumstances, the relevance of international law is not self-evident. Its general applicability is thus ascertained in the first instance (2.1). To the extent that '[m]ost of […] if not all institutions and principles of international law rely, directly or indirectly, on State sovereignty',[83] the specific applicability of this sovereignty is then assessed (2.2).

.

2.1. The general applicability of international law in cyberspace

The USA has tried to apply international law to information operations since the 90's, and considers that '[t]he development of norms for state conduct in cyberspace does not […] render existing international norms obsolete'.[84] Many states currently recognize that existing international law is applicable in cyberspace Russia proposes to strengthen 'cyberspace security', 'in accordance with [...] norms of the international law'.[85] The British government underlines '[t]he need for governments to act proportionately in cyberspace and in accordance with national and international law',[86] and the fact that 'these

---

[83] Samantha Besson, 'Sovereignty' (2011) M.P.E.P.I.L., [2].

[84] The White House, 'International Strategy for Cyberspace–Prosperity, Security, and Openness in a Networked World' (2011) 9 <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> accessed:02.10.2016.

[85] Russian MOD, 'Russian Federation Armed Forces' Information Space Activities Concept' (2000) [3.1] <http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle> accessed:22.08.2016.

[86] Cabinet Office, 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world' (2011) 22 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> accessed:14.11.2016.

principles apply with equal force to cyberspace'.[87] 'It is the UK's view that when states and individuals engage in hostile cyber operations, they are governed by law just like activities in any other domain [...] The question is not whether or not international law applies, but rather how it applies and whether our current understanding is sufficient'. [88] British parliamentaries are sometimes more moderate. According to Lord Browne of Ladyton, '[i]nternationally, in the absence of sufficient treaty law or UN statutes dealing explicitly with cyber actions, urgently we need to define the role that international law should play in covering either offensive or defensive cyber actions'.[89] According to Japan, 'it is important that existing international laws continue to be applied to acts using cyberspace' to maintain 'a degree of order'.[90] This applicability has also been recognized by Canada,[91] Georgia,[92] Poland,[93] the UK,[94] and Australia[95] in their answers to the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). The Swedish Defence

---

[87] UNGA, 'Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General' (16.07.2013) UN-Doc A/68/156, 18.

[88] Attorney General's Office (AGO), 'Cyber and International Law in the 21st Century' (2018) <www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed:24.05.2018.

[89] HL Deb 14 October 2010, vol 721, col 688

[90] Information Security Policy Council (ISPC), 'Cybersecurity Strategy' (2013) 49 <www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf> accessed:23.08.2016.

[91] Canada, 'Developments in the Field of Information and Telecommunications in the Context of International Security' (2015) 3 <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/08/CanadaISinfull.pdf> accessed:25.06.2018.

[92] Georgia, 'UN General Assembly Resolution 68/243' (2014) 7 <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/07/Georgia.pdf> accessed:26.08.2016.

[93] UNGA, 'Developments in the field of information and telecommunications in the context of international security' (19.07.2016) UN-Doc A/71/172, 16.

[94] UK, 'Response to General Assembly resolution 68/243 "Developments in the field of information and telecommunications in the context of international security"' (2014) 5 <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/07/UK.pdf> accessed:26.08.2016.

[95] UNGA, 'Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General' (30.06.2014) UN-Doc A/69/112, 2.

Commission[96] and the European Commission are of the same opinion.[97] Other states acknowledging such a broad applicability include Mexico,[98] New Zealand,[99] and India.[100] Chile acknowledges that 'there are practically no specific regulation instruments' for cyberspace, but affirms that 'it is actually regulated both by the existing national laws and by the general applicable international regulations'.[101] Consequently, 'the challenge lies particularly on being able to identify and interpret the relevant regulations of the applicable international law'.[102] Moreover, 'the respect of public international law' is deemed applicable 'in cyberspace'.[103] According to France, 'there is a consensus on some aspects of international law in cyberspace, but some questions of implementation are more complex', such as 'the definition of interstate hostile acts'.[104] Then, '[i]n 2013, the States acknowledged that far from being a space without rules, cyberspace

---

[96] Sweden, 'Submission by Sweden to UNGA resolution 68/243 entitled "Developments in the field of information and telecommunications in the context of international security"' (12.09.2014) 2 <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/10/Sweden.pdf> accessed:29.06.2018.

[97] European Commission, 'Cybersecurity strategy of the European Union–An Open, Safe and Secure Cyberspace' (2013) 16. <https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf> accessed:03.10.2016.

[98] Presidencia, 'CLAN 2016 Seguridad y Defensa' (2016) <www.gob.mx/presidencia/documentos/clan2016-seguridad-y-defensa> accessed:31.10.2017.

[99] UK government, 'New Zealand–United Kingdom Joint Statement on Cyber Security' (15.01.2013) <www.gov.uk/government/news/new-zealand-united-kingdom-joint-statement-on-cyber-security--2> accessed:23.09.2017.

[100] 'Joint statement by Prime Minister Stefan Löfven and Prime Minister Narendra Modi' (2016) [22] <www.government.se/statements/2016/02/joint-statement-by-prime-minister-stefan-lofven-and-prime-minister-narendra-modi/> accessed:09.11.2017.

[101] Chilean Government, 'National Cybersecurity Policy' (2017) 22 <http://ciberseguridad.interior.gob.cl/media/2017/04/NCSP-ENG.pdf> accessed:16.09.2017.

[102] Ibid.

[103] Chilean Ministry of National Defence (MND), 'Aprueba Politica de Ciberdefensa' (2018) DO 42.003, 1-2 <www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf> accessed:21.06.2018.

[104] AN, 'Rapport d'information' (07.10.2014) No.2249, 83 <www.assemblee-nationale.fr/14/pdf/rap-info/i2249.pdf> accessed:02.11.2017.

was governed by existing international law. Despite this, the international normative framework is still being debated'.[105]

In contrast, some states confess that the applicable legal framework is unclear and/or call for further discussion (Finland,[106] Italy,[107] New Zealand,[108] and the Netherlands)[109] or insist on the need to develop new norms in cyberspace (Austria,[110] Switzerland).[111] When explaining the rules it finds applicable in cyberspace, Colombia expressly refers to regional instruments, the ITU's 'Consensus on cybersecurity' and UNGA resolution 64/25, but fails to refer to general international law.[112]

---

[105] French Prime Minister (PM), 'French National Digital Security Strategy' (2015) 38 <www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf> accessed:01.07.2018.

[106] Ministry of Defence (DEFMIN), 'Finland's Cyber Security Strategy' (2013) 33 <www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf> accessed:02.10.2016.

[107] Presidency of the Council of Ministers (PCM), 'Italian National Strategic Framework for Cyberspace Security' (2013) 22 <www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf> accessed:24.09.2016.

[108] Department of the Prime Minister and Cabinet (DPMC), 'New Zealand's Cyber Security Strategy' (2015) 10 <www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-action-plan-december-2015.pdf> accessed:03.10.2016.

[109] Kingdom of the Netherlands, 'Developments in the field of information and telecommunications in the context of international security' (2015) 4 <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/08/NetherlandsISinfull.pdf> accessed:26.06.2018.

[110] Federal Chancellery (BKA), 'National ICT Security Strategy Austria' (2012) 12 <www.digitales.oesterreich.gv.at/documents/22124/30428/National_ICT_Security_Strategy_Austria_2012_print.pdf> accessed:02.10.2016.

[111] Federal Department of Defence, Civil Protection and Sport (VBS), 'National Strategy for Switzerland's Protection against Cyber Risks' (2012) 30 <www.isb.admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/Strategie%20zum%20Schutz%20der%20Schweiz%20vor%20Cyber-Risiken.pdf.download.pdf/Strategie_zum_Schutz_der_Schweiz_vor_Cyber-Risiken_k-ENGL.pdf> accessed:08.11.2017.

[112] National Council on Economic and Social Policy (CONPES), 'Policy Guidelines on Cybersecurity and Cyberdefense' (2011) 10-12 <www.sites.oas.org/cyber/Documents/Colombia%20-%20National%20Cybersecurity%20and%20Cyberdefense%20Policy.pdf> accessed:16.09.2017.

Most states acknowledge the general applicability of existing international law in cyberspace, while qualifying it as a different space. The military quasi-systematic approach qualifies cyberspace as a 'fifth environment', which exists next to land, sea, airspace and outer-space.[113] Cyberspace has even been defined as 'global commons' by Finland,[114] Japan,[115] Canada[116] and Hungary.[117] On the contrary, China affirms that '[i]nformation space is no "global domain"'.[118] The lack of border in cyberspace is highlighted by many states, including France,[119] the UK,[120] Germany,[121] Latvia,[122] Saudi Arabia,[123] and Bangladesh.[124] Only a few–

[113] See Chapter I-IV.

[114] Prime Minister's Office, 'Finnish Security and Defence Policy 2012' (2013) 23 <www.bbn.gov.pl/ftp/dok/07/FIN_Finnish_Security_Defence_Policy_2012_Government_Report.pdf> accessed:29.10.2017.

[115] Japanese MOD, 'Defence of Japan 2015' (2015) 154 <www.mod.go.jp/e/publ/w_paper/pdf/2015/DOJ2015_2-2-1_web.pdf> accessed:15.05.2017.

[116] Department of National Defence (DND), *The Future Security Environment 2013-2040* (National Defence 2014) 114.

[117] Hungarian MOD, 'Hungary's National Military Strategy' (2012) 10 <www.files.ethz.ch/isn/167317/Hungary%202012%20national_military_strategy.pdf> accessed:14.05.2017.

[118] PRC Permanent Mission to the UN (PMUN), 'Statement by Ms. Liu Ying of the Chinese Delegation at the Thematic Debate on Information and Cyber Security at the First Committee of the 68th Session of the UNGA' (30.10.2013) <www.china-un.org/eng/hyyfy/t1094491.htm> accessed:04.10.2016.

[119] Commission du livre blanc, *Défense et Sécurité nationale: le Livre blanc* (Odile Jacob, 2008) 53.

[120] Cabinet Office, 'The UK Cyber Security Strategy' (n.86) 16.

[121] Federal Ministry of the Interior (BMI), 'Cyber Security Strategy for Germany' (2011) 3 <www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile> accessed:24.09.2016.

[122] Latvian Government, 'Cyber Security Strategy of Latvia 2014-2018' (2014) 20 <www.unodc.org/res/cld/lessons-learned/lva/cyber_security_strategy_of_latvia_2014-2018_html/Cyber_Security_Strategy_of_Latvia.pdf> accessed:29.09.2016.

[123] Saudi Ministry of Communication and Information Technology (MCIT), 'Developing National Information Security Strategy for the Kingdom of Saudi Arabia' (2013) 11, 76 <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-of-saudi-arabia/view/++widget++form.widgets.file/@@download/NCSS_Saudi+Arabia_draft_EN.pdf> accessed:03.10.2016.

[124] Ministry of Public Administration (MOPA), 'National Cybersecurity Strategy' (2014) 3 <www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf> accessed:03.10.2016.

Afghanistan[125] and Turkey[126]–define a 'national cyberspace', which consists of 'public organizations, natural and legal persons' information systems. In the same fashion, Malta refers to its 'cyberspace territory'.[127]

While many states seem to agree on the applicability of general international law in cyberspace, it is necessary to determine whether it goes the same way for one of its specific and key aspect: sovereignty.

2.2. The specific applicability of sovereignty in cyberspace

It is common to claim that international law is articulated around a so-called principle of sovereignty. This principle was defined by Max Huber in the *Las Palmas* award as follows: '[s]overeignty in the relations between States signifies independence […] Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State'.[128] As two sides of the same coin, sovereignty has actually an internal and an external manifestation. The former 'refers to the international rights and duties of a State that pertain to its ultimate authority and competence over all people and all things within its territory, and in particular to the correlated principles of territorial and personal jurisdiction and integrity, and of non-intervention'.[129] Consequently–and failing the existence of a permissive rule to the contrary'–a state 'may not exercise its power in any form in the territory of another State'.[130]

---

[125] Afghan MCIT, 'National Cyber Security of Afghanistan' (2014) 14 <http://mcit.gov.af/Content/files/National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf> accessed:20.09.2017.

[126] Ministry of Transport, Maritime Affairs and Communication (UDHB), '2016-2019 National Cyber Security Strategy' (2016) 8 <www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf> accessed:21.06.2018.

[127] Ministry for Competitiveness and Digital Maritime and Services Economy (MCDMS), 'Malta Cyber Security Strategy' (2016) 21 <https://mita.gov.mt/en/maltacybersecuritystrategy/Documents/Mita%20_Malta%20Cyber%20Security%20Strategy%20-%20Book.pdf> accessed:12.10.2016.

[128] *Island of Palmas case (Netherlands/USA)* (1928) 2 RIAA 831, [838].

[129] Besson, 'Sovereignty' (n.83) [70].

[130] *The Case of the S.S. "Lotus"* (*France v Turkey*) (Judgment) [1927] Series A No.10, 18.

However, nothing 'prohibits a State from exercising jurisdiction in its own territory'.[131] The latter refers to the sovereign equality of states, and is enshrined in article 2(1) of the UN Charter: '[t]he Organization is based on the principle of the sovereign equality of all its Members'. PCIJ case-law is of importance in the development of this concept. The *Wimbledon* case qualified 'the right of entering into international engagements' as 'an attribute of State sovereignty',[132] while the *Lotus* case highlighted that '[i]nternational law governs relations between independent States'.[133] Therefore, '[t]he rules of law binding' them 'emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law', and '[r]estrictions upon the independence of States cannot […] be presumed'.[134] Sovereignty may thus be understood as an 'umbrella' principle, giving birth to different rules: the respect for territorial integrity, non-intervention, and non-aggression. As synthetized by Spector, this approach claims that sovereignty is only 'a background principle rather than a primary rule–and that it binds states only inasmuch as it informs other rules of international law, most prominently those prohibiting the threat or use of force or intervention in the internal affairs of other states'.[135] This is actually how practice may be read, as violations of sovereignty are usually assessed on the basis of a territorial intrusion, non-intervention or use of force.[136]

It is necessary to determine whether sovereignty applies in cyberspace. As underlined by Brian Egan, '[a]lthough many States, including the United States, generally believe that the existing international legal framework is sufficient to

---

131 Ibid.

132 *Case of the SS "Wimbledon" (UK, France, Italy and Japan v Germany)* (Judgment) (1923) PCIJ Rep Series A No.1, [35].

133 Lotus (n.130) 18.

134 Ibid.

135 Phil Spector, 'In Defense of Sovereignty, in the Wake of Tallinn 2.0' (2017-2018) 111 A.J.I.L. Unbound 219, 219. See also: Gary Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017-2018) 111 A.J.I.L. Unbound 207, 210; Roman Kwiecien, 'Armed Intervention and Violation of State Sovereignty in International Law' (2004) 13 Pol.Q.Int'l Affairs 73; Dan Svantesson, 'Lagom Jurisdiction–What Viking Drinking Etiquette Can Teach Us about Internet Jurisdiction and Google France' (2018) Masaryk U.J.L.&Tech. 29, 45.

136 For a famous example: *Nicaragua* (n.46) [202]-[213]. See also: Chapter I-I.

regulate State behavior in cyberspace, States likely have divergent views on specific issues'.[137]

Many states already acknowledge the applicability of sovereignty in cyberspace. According to Sweden, '[t]he antagonistic use of cyber capabilities, such as computer and network attacks, can effectively restrict the room for manoeuvre of the target and be a threat to national security and ultimately state sovereignty'.[138] China affirms that 'the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded'.[139] Consequently, '[n]o country should pursue cyber-hegemony, interfere in other countries' internal affairs, or engage in, condone or support cyber-activities that undermine other countries' national security', while '[n]ational governments are entitled to administer cyberspace in accordance with law'.[140]

Australia thinks that 'the principle of sovereign equality of States […] may be applicable',[141] and in Russia, armed forces 'are guided' by the 'respect for the state sovereignty' in 'the global information space'.[142] In their code of conduct, China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan pledge 'to comply with […] universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States'.[143] Colombia thinks that national sovereignty

---

137 Egan (n.61).

138 Sweden, 'Submission by Sweden to UNGA resolution 68/243' (n.96) 6.

139 UNGA, Developments in the field of information and telecommunications in the context of international security (02.07.2007) UN-Doc A/62/98, 7.

140 Ministry of Foreign Affairs of the People's Republic of China (FMPRC), 'International Strategy of Cooperation on Cyberspace' (2017) <http://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml> accessed:27.04.2018.

141 UNGA, 'Developments in the field of information and telecommunications in the context of international security' (15.07.2011) UN-Doc A/66/152, 6.

142 Russian MOD (n.85) [2.1].

143 UNGA, 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (13.01.2015) UN-Doc A/69/723, 4.

should be strengthened in the digital environment.[144] Chile finds 'the respect of sovereignty' and 'territorial integrity' applicable.[145]

The general connection between cyber-operations and a potential breach of sovereignty has been made by some States. According to Harold Koh, '[t]he physical infrastructure that supports the Internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial state […] operations targeting networked information infrastructures in one country may create effects in another country. Whenever a state contemplates conducting activities in cyberspace, the sovereignty of other states needs to be considered'.[146] Portugal affirms that the use of information technologies 'may negatively affect the national integrity of States'.[147] 'Cyberdefence' is defined by Colombia as 'the resort to military capacities in the face of cybernetic attacks or hostile acts of cybernetic nature that affect society, national sovereignty, independence, territorial integrity the constitutional order and national interests'. [148] Similar appeals to sovereignty were made following concrete instances of cyber-attacks. Following the theft of information about credit cards and their publication online, Israel affirmed that it 'will respond to cyber-attacks in the same way it responds to violent "terrorist"' and called it 'a breach of sovereignty comparable to a terrorist operation', that 'must be treated as such'.[149] Estonia called the 2007 cyber-attacks a 'possible infringement upon national sovereignty'.[150]

---

144 CONPES, 'Política Nacional de Seguridad Digital' (2016) 60 <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf> accessed:29.10.2017.

145 Chilean MND, 'Aprueba' (n.103) 2.

146 Harold Hongju Koh, 'International Law in Cyberspace', USCYBERCOM Inter-Agency Legal Conference in Fort Meade (18.09.2012) answer 9 <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers > accessed:14.07.2016.

147 UNGA, 'Developments' (30.06.2014) (n.95) 12.

148 CONPES, 'Política Nacional' (n.144) 88.

149 Ori Lewis, 'Israel warns against computer-hacker vigilantism', *Reuters* (12.01.2012) <www.reuters.com/article/us-israel-hackers/israel-warns-against-computer-hacker-vigilantism-idUSTRE80B23420120112> accessed:14.06.2018.

Finland and Spain think that the concept of sovereignty has been subject to evolution, and propose a form of *due diligence* in cyberspace. According to Spain, 'States should [...] cooperate effectively in order to prevent harmful practices in cyberspace, and not knowingly allow their territory to be used to commit internationally wrongful acts using such technologies'. [151] 'Internationally wrongful acts' thus allegedly exist in cyberspace. Finland affirms that '[s]overeignty also includes responsibility. A state must see to it that its area will not be used in an attack against another state. It must, therefore, also try to prevent attacks beyond its national borders perpetrated by private entities'.[152]

According to the Attorney General of England and Wales Jeremy Wright, '[s]overeignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention'.[153] As a consequence, '[t]he UK Government's position is therefore that there is no such rule as a matter of current international law'.[154]

Both Australia and Ukraine highlighted the legal uncertainties linked to the development of cyberspace. Australia asked 'for further work to develop understandings on how key concepts such as sovereignty and jurisdiction apply in cyberspace, taking into account our common interest in preserving the global nature of the Internet'.[155] Ukraine suggested the adoption of new international legal instruments, an aspect of which would be 'to determine the international legal status of cyberspace and to enshrine […] States' jurisdictions with regard

---

[150] Rene Vark, 'Republic of Estonia Materials on International Law 2009' (2010) 10 B.Y.B.I.L. 203, 255.

[151] UNGA, 'Developments' (19.07.2016) (n.93) 19.

[152] DEFMIN (n.106) 33.

[153] AGO (n.88).

[154] Ibid.

[155] UNGA, 'Developments' (19.07.2016) (n.93) 4-5.

to the national components of this space (comparable to States' air space and territorial waters)'.[156]

In spite of some ambiguities or uncertainties, many states consider that both international law and sovereignty are applicable in 'cyberspace'. Yet, it remains necessary to define what is 'cyberspace', as well as 'cyber-espionage'.

3. Definitions of main concepts

'Cyberspace' (3.1), and 'cyber-espionage' (3.2) are the main concepts used throughout this thesis, and need to be defined.

3.1. 'Cyberspace'

Defining 'what' is cyberspace has been a major concern of Western doctrine.[157] The definition provided by the American military–that is, 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'[158]–seems to be favoured by authors, and is now commonplace in academic articles.[159] However, it must be underlined that this definition is not universally accepted.

---

156 UNGA, 'Developments' (16.07.2013) (n.87) 14.

157 David Betz and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (Routledge 2012) 35-42; Julie Cohen, 'Cyberspace as/and Space' (2010) 107 Colum.L.Rev. 210; David Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stan.L.Rev. 1367, 1378-9; Menthe D, 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 4 Mich.Telecomm.&Tech.L.Rev. 69, 70-1.

158 Joint Chiefs of Staff, 'Cyberspace Operations' (2013) JP 3-12, GL-4 <www.hsdl.org/?view&did=758858> accessed:25.06.2018.

159 Arie Schaap, 'Cyber Warfare Operations: Developments and Use under International Law' (2009) 64 A.F.L.R. 121, 125; Andru Wall, 'Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action' (2011) 3 Harv.Nat'l.Sec.J. 85, 118; Patrick Franzese, 'Sovereignty in Cyberspace: Can it Exist?' (2009) 64 A.F.L.R. 1, 9; Wolff Heintschel Von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 I.L.S. 123, 125.

Firstly, the notion of 'cyberspace' is not China's and Russia's preferred approach. They refer more commonly to the notion of 'information space', and both agreed on a definition: 'the sphere of activity related to creation/development, transformation, transmission, use and storage of information with impact on individual and public awareness, information infrastructure'.[160] Along with Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan, they submitted two codes of conduct to the UNGA.[161] Thus, 'information security in Russian is focused on both the mind and on technical systems',[162] while 'China appears more like Russia than the U.S. in its understanding of information security, with its emphasis on the mental aspect of information security and its extended use of the term itself'.[163] Yet, the term 'cyberspace' is not totally absent from their official discourse, and appears in numerous publications from the Chinese[164] and Russian[165] Ministries of Foreign Affairs (MFA).

---

160 Russian government, Order 'On signing the Agreement between the Government of the Russian Federation and the Government of the people's Republic of China on cooperation in ensuring international information security' (30.04.2015) No.788-p, 9.

161 UNGA, 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (14.09.2011) UN-Doc A/66/359; UNGA, 'Letter dated 9 January 2015' (n.143).

162 Timothy Thomas, 'Information Security Thinking: A Comparison of U.S., Russian, and Chinese Concepts', in Richard Ragaini (ed), *Aids And Infectious Diseases, Proceedings Of The International Seminar On Nuclear War And Planetary Emergencies–26 Session* (World Scientific 2002) 350.

163 Ibid 346. See also: Keir Giles and William Hagestad, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' in Karlis Podins, Jan Stinissen, and Markus Maybaum (eds), *5th International Conference in Cyber Conflict. Proceedings 2013* (NATO CCDCOE Publications 2013); Michael Swaine, 'Chinese Views on Cybersecurity in 'Foreign Relations' (2013) 42 China Leadership Monitor 1.

164 FMPRC, 'Consultation Between Director-Generals of the Departments of Treaty and Law of Ministries of Foreign Affairs of China and Russia Held in Moscow' (2016) <www.fmprc.gov.cn/mfa_eng/wjbxw/t1337836.shtml> accessed:15.02.2018.

165 See: Ministry of Foreign Affairs of the Russian Federation (MID), 'Foreign Minister Sergey Lavrov's interview with Kurdish television channel Rudaw' (2017) <www.mid.ru/en/press_service/minister_speeches/-/asset_publisher/7OvQR5KJWVmR/content/id/2822361> accessed:12.03.2018.;
MID, 'Foreign Minister Sergey Lavrov's remarks and answers to media questions at the Primakov Readings International Forum' (2017) <www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3239504> accessed:12.03.2018.

The term 'cyberspace' is well-accepted outside this area, and is used by almost forty states. However, only Saudi Arabia has adopted the American definition,[166] while India[167] and Montenegro[168] both refer to ISO definition.[169] In parallel, some states refer to 'cyberspace' but without defining it: Chile,[170] Egypt,[171]

[166] MCIT (n.123) A-2.

[167] Ministry of Electronics and Information Technology (MEITY), 'National Cyber Security Policy' (2013) 1 <http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf> accessed:23.08.2016.

[168] Montenegrin Government, 'National Cyber Security Strategy for Montenegro 2013-2017' (2013) 6 <www.unodc.org/res/cld/lessons-learned/national-cyber-security-strategy-for-montenegro-2013-2017_html/National_Cyber_Security_Strategy_for_Montenegro_2013-2017.pdf> accessed:03.10.2016.

[169] ISO, 'Information technology–Security techniques–Guidelines for cybersecurity' (2012) BS.ISO/IEC27032:2012 [4.21] <www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en> accessed 18.04.2018.

[170] Chilean Government (n.101) 1-29.

[171] Egyptian MCIT, 'National ICT Strategy 2012-2017' (2012) 24, 34 <http://mcit.gov.eg/Upcont/Documents/ICT%20Strategy%202012-2017.pdf> accessed:16.09.2017.

Guatemala, [172] Ireland, [173] Jordan, [174] Paraguay, [175] Rwanda, [176] Senegal, [177] and Singapore.[178]

The definitions of the remaining states have at least slight differences. However, most of them are built the same way, trying to answer a dual question: 1) What is cyberspace? and 2) How is it composed?

1) What is cyberspace? Cyberspace is an 'electronic world' (Canada), [179] a 'physical and virtual environment' (Colombia),[180] a 'digital environment' (Czech Republic),[181] a 'virtual space' (Germany),[182] a 'physical and non-physical domain'

---

172 Guatemala MOD, 'Libro de la Defensa Nacional de la República de Guatemala, Evolución 2015' (2015) 12 <www.mindef.mil.gt/pdf/Libro%20de%20la%20Defensa%20Nacional%20de%20la%20Rep%C3%BAblica%20de%20Guatemala,%20Evolucion%20%202015.pdf> accessed:20.09.2017.

173 Department of Communications, Climate Action and Environment, 'National Cyber Security Strategy 2015-2017' (2015) 2, 10 <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf> accessed:16.09.2017.

174 Ministry of Information and Communications Technology (MICT), 'National Information Assurance and Cyber Security Strategy' (2012) 17 <http://nitc.gov.jo/PDF/NIACSS.pdf> accessed:16.09.2017.

175 Gobierno Nacional, 'Plan Nacional de Ciberseguridad' (2016) 26 <http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg> accessed:20.09.2017.

176 Ministry of Information Technology and Communications (MITEC), 'National Cyber Security Policy' (2015) 5 <www.mitec.gov.rw/fileadmin/Documents/Policies/Rwanda_Cyber_Security_Policy.pdf> accessed:16.09.2017.

177 Ministry of Post and Telecommunications, 'Stratégie Sénégal Numérique 2016-2025' (2016) 25, 28 <www.sec.gouv.sn/sites/default/files/Strat%C3%A9gie%20S%C3%A9n%C3%A9gal%20Num%C3%A9rique%202016-2025.pdf> accessed:16.09.2017.

178 Cyber Security Agency, 'Singapore's Cybersecurity Strategy' (2016) 4-10 <www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf> accessed:20.09.2017.

179 Public Safety Canada, 'National Cyber Security Strategy' (2018) 34 <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf> accessed:24.06.2018.

180 CONPES, 'Policy Guidelines' (n.112) 34.

181 Act On Cyber Security and Change of Related Acts ('Act on Cyber Security') (23.07.2014) No.181, §2(a)

182 BMI (n.121) 14.

(Israel),[183] an 'interactive environment' (Latvia),[184] a 'global digital environment' (Mexico), [185] 'a virtual or electronic environment' (Qatar), [186] a 'space of processing and exchanging information' (Poland), [187] an 'environment' (Afghanistan,[188] Turkey),[189] a 'global network' (New Zealand),[190] 'an operating environment' (UK).[191]

2) How is cyberspace composed? It is created by 'information systems and services and electronic communication networks' (Czech Republic), [192] composed of 'computers, computer systems, computer programs (software), and telecommunications, data, and information network' (Colombia),[193] 'all IT [Information Technology] systems linked at data level on a global scale' (Germany).[194] They are created or composed 'of part or all of the following

---

183 Israeli Government, 'Advancing National Cyberspace Capabilities' (07.08.2011) Resolution 3611, 1 <www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf> accessed:16.09.2017.

184 Latvian Government (n.122) 19.

185 Mexican Government, 'Estrategia Nacional de Ciberseguridad' (2017) 27 <www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf> accessed:22.06.2018.

186 Ministry of Transport and Communications (MOTC), 'Qatar National Cyber Security Strategy' (2014) 23 <www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf> accessed:03.10.2016.

187 Ministry of Administration and Digitisation (MAC), 'Cyberspace Protection Policy of the Republic of Poland' (2013) 5 <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf> accessed:03.10.2016.

188 Afghan MCIT (n.125) 14.

189 UDHB, '2016-2019 National Cyber Security Strategy' (n.126) 7.

190 New Zealand Government, 'New Zealand's Cyber Security Strategy' (2011) 12 <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/nzcybersecuritystrategyjune2011_0.pdf> accessed:12.07.2018.

191 British Ministry of Defence (MoD), 'Cyber Primer' (2016) 1 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf> accessed:24.05.2018.

192 Act on Cyber Security (2014) §2.

193 CONPES, 'Policy Guidelines' (n.112) 34.

components: mechanized and computerized systems, computer and communications networks, programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data' (Israel), [195] 'interconnected networks of information technology and the information on those networks' (Canada). [196] They consist of 'information systems' (Afghanistan),[197] 'information systems spread over the entire world and space, the networks interconnecting these systems or independent information systems (Turkey),[198] 'the ICT [Information and Communications Technology] systems, together with links between them and the relations with users' (Poland),[199] are 'constituted by computer and telecommunication networks' (Mexico), [200] 'interdependent information technology infrastructures, telecommunication networks and computer processing systems' (New Zealand). [201] Cyberspace 'results from the interdependent network of information and communications technology (e.g., the Internet, telecommunications networks, computer systems, and embedded processors and controllers) that links people with services and information' (Qatar),[202] or 'includes users, networks, computing technology, software, processes, information in transit or storage, applications services, and systems that can be connected directly or indirectly to the Internet, telecommunications and computer networks' (Latvia).[203] It consists of 'the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded

194 BMI (n.121) 14.

195 Israeli Government (n.183) 1.

196 Public Safety Canada, 'National Cyber Security Strategy' (n.179) 34.

197 Afghan MCIT (n.188) 14.

198 UDHB, '2016-2019 National Cyber Security Strategy' (n.126) 7

199 MAC (n.187) 5.

200 Mexican Government (n.185) 27.

201 New Zealand Government (n.190) 12.

202 MOTC (n.186) 23.

203 Latvian Government (n.122) 19-20.

processors and controllers), and the data therein spanning the physical, virtual and cognitive domains' (UK).[204]

Moreover, Colombia and Mexico add another definitional element: 3) what is cyberspace used for? It is thus the space in which persons 'interact with each other' (Colombia)[205] or 'communicate and interact, and allows the exercise of their rights and freedoms as they do in the physical world' (Mexico).[206]

As for Kenya and Nigeria, they just answer questions 1) and 3), respectively defining cyberspace as '[t]he notional environment in which communication over computer networks occurs'[207] and '[t]he electronic medium of computer networks, in which online communication takes place'.[208] Likewise, only questions 2) and 3) are answered by the Philippines[209] and Trinidad-and-Tobago.[210] Finally, technical definitions are adopted by some states: and the thus answering question 2): 'the combination of globally interconnected, decentralised and ever-growing electronic information systems, and social and economic processes represented in the form of data and information through these systems' (Hungary),[211] 'the information technology network,

---

[204] MoD, 'Cyber Primer' (n.191) 1.

[205] CONPES, 'Policy Guidelines' (n.112) 34.

[206] Mexican Government (n.185) 27.

[207] Kenyan MICT, 'National Cybersecurity Strategy' (2014) 17 <http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf> accessed:16.09.2016.

[208] Office of the National Security Adviser (ONSA), 'National Cybersecurity Strategy' (2017) appendix 2 <https://tekedia.com/wp-content/uploads/2017/04/ncss-STRATEGY.pdf> accessed:28.10.2017.

[209] Office of the President, 'National Cyber Security Plan' (2004) 6-7 <www.dict.gov.ph/wp-content/uploads/2014/07/Cyber-Plan-Pre-Final-Copy_.pdf> accessed:24.06.2018.

[210] Trinidadian Government, 'National Cyber Security Strategy' (2012) 26-7 <www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf> accessed:16.09.2017.

[211] Hungarian Government, 'Government Decision No.1139/2013 on the National Cyber Security Strategy of Hungary' (2013) [3] <www.unodc.org/res/cld/lessons-learned/national_cyber_security_strategy_of_hungary_html/National_Cyber_Security_Strategy_of_Hungary.pdf> accessed:24.09.2016.

telecommunication networks and computer processing systems' (Slovenia),[212] 'the sum of all ICT equipment and services' (the Netherlands).[213]

Interestingly, none of these definitions refers to the multi-layered nature of cyberspace and the different protocols, which are 'sets of rules for message formats and procedures that allow machines and application programs to exchange information' (for instance, the OSI and TCP/IP models).[214]
The OSI model 'qualifies standards for the exchange of information among systems that are "open" to one another for this purpose by virtue of their mutual use of the applicable standards'.[215] To do so, it relies on seven layers: '[e]ach layer performs its functions by invoking the services provided by the layers below it, then it returns the results to the invoking layer above'.[216] 1) The Physical Layer 'tangibly connects computers together via cables and wires'.[217] 2) The Data-Link Layer 'formats, sends, and receives data packets across the network via the Physical Layer'.[218] 3) The Network Layer 'is responsible for selecting a route for the message'.[219] 4) The Transport Layer 'ensures that messages are delivered error-free, in sequence, and with no loss or duplication'.[220] 5) The Session Layer

---

212 Republic of Slovenia, 'Cyber Security Strategy' (2016) 3 (footnote 4) <www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf > accessed:12.10.2016.

213 Advisory Council of International Affairs (AIV)/Advisory Committee on Issues of Public International Law (CAVV), 'Cyber Warfare' (2011) 22/77, 12 <https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf> accessed:20.05.2017.

214 'TCP/IP Protocols' (*IBM*) <www.ibm.com/support/knowledgecenter/en/ssw_aix_72/com.ibm.aix.networkcomm/tcpip_protocols.htm> accessed:24.10.2018.

215 ISO, 'Information Technology–Open Systems Interconnection–Basic Reference Model: The Basic Model' (1994) ISO/IEC7498-1, 1. <https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip> accessed:25.10.2018.

216 Diane Savage, 'Law of the LAN' (1993) 9 Santa Clara Computer&High Tech.L.J. 193, 200.

217 Macklin Everly, 'Net Neutrality and the Department of the Internet: Creating Problems through Solutions' (2017) 42 U. Dayton L.Rev. 55, 69.

218 Ibid.

219 William Fray, 'Network Communications Protocols: The OSI Model' (1993) 5 Trends L.Libr.Mgmt.&Tech. 4, 4..

'opens and maintains communications among all the nodes on a network'.[221] 6) The Presentation Layer has 'to translate the message into a language that the receiving computer can interpret', and 'compresses the data using a compression algorithm'.[222] 7) 'The purpose of the Application Layer is to accept input from a terminal keyboard and to convert it to machine-readable form (bits). It also attaches a header at the beginning of the bit packet, which contains defining data necessary to identify the sending and receiving computers'.[223] In addition, it offers services or applications, such as emails.[224]

The TCP/IP model includes four layers. 1) 'The Network Interface Layer encompasses the Data Link and Physical layers of the OSI model', and thus 'handles placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium'.[225] 2) The Internet Layer 'is analogous to the Network layer of the OSI model', and 'handles addressing, packaging, and routing functions'.[226] 3) The Transport (Host-to-Host) Layer ensures 'that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets'.[227] 4) The Application Layer 'lets applications access the services of the other layers and defines the protocols that applications use to exchange data'.[228]

---

[220] Duncan MacMichael, 'Windows Network Architecture and the OSI Model' (*Microsoft*, 20.04.2017) <https://docs.microsoft.com/fr-fr/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model> accessed:25.10.2018.

[221] Fray (n.219) 4.

[222] Ibid.

[223] Ibid.

[224] Ibid.

[225] 'How TCP/IP Works' (*Microsoft,* 29.10.2008) <https://technet.microsoft.com/pt-pt/library/cc786128(v=ws.10).aspx> accessed:26.10.2018.

[226] Ibid.

[227] 'TCP/IP Protocol Architecture Model' (*Oracle*) <https://docs.oracle.com/cd/E19683-01/806-4075/ipov-10/index.html> accessed:19.10.2018.

[228] 'How TCP/IP Works' (n.225).

Some understanding of cyberspace's technical aspects may nevertheless be found in state definitions, even if such complexity is not reflected. For instance, the term 'telecommunications networks'–defined as the 'electronic system of links and switches, and the controls that govern their operation, that allows for data transfer and exchange among multiple users'[229]–could globally apprehend these layers. It goes the same way for the more abstract 'information technology infrastructure' (which refers 'to the entire stack of underlying elements required to deliver technology to an end-user'),[230] or 'information system' ('an integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products').[231] It may also be noted that–according to the UK–[c]yberspace can be thought of as comprising of six interdependent layers: social; people; persona; information; network; persona; and real'.[232]

It results from the above that 'cyberspace' is a widespread term. In spite of their different approach, it is sometimes used by Russia and China. Moreover, most of the cyberspace definitions seek to answer two questions, i.e. what is cyberspace?; and how it is composed? While this thesis does not intend to create a universal and objective definition of cyberspace, it nevertheless seems that common denominators can be deduced from state practice. Cyberspace is thus understood as 'a virtual and man-made environment, emerging from the networks of information systems interconnected through the Internet, whose good functioning is ensured through physical and digital layers, and allows interactions between users, telecommunication networks and services'.

In sum, states' definitions of cyberspace are rarely identical, but usually similar. The same applies in respect of this thesis' central theme: 'cyber-espionage'.

---

[229] Robert Morrow, 'Telecommunications network' (*Britannica*) <www.britannica.com/technology/telecommunications-network> accessed:20.10.2018.

[230] 'IT Infrastructure' (*DELL-EMC Glossary*) <www.emc.com/corporate/glossary/it-infrastructure.htm> accessed:21.10.2018.

[231] Vladimir Zwass, 'Information system' (*Britannica)* <www.britannica.com/topic/information-system> accessed:22.10.2018.

[232] MoD, 'Cyber Primer' (n.191) 5.

3.2. 'Cyber-espionage'

Many new activities coexist in cyberspace; the distinction between cyber-espionage and cyber-attacks (A), and its relationships with cyber-crime and cyber-security are explained (B). Subsequently this thesis proposes a definition of cyber-espionage (C).

A. The distinction between 'cyber-attacks' and 'cyber-espionage' in state practice

The destructive effect[233] or intent[234] underlying a cyber-operation (rather than the mere theft of information) is usually what allows doctrine to distinguish cyber-espionage and cyber-attacks. The difference between the disruption of a system and the mere theft of information is indeed confirmed by a majority of states.

The traditional definition given by the USA is that a 'computer network attack' (CNA) or an 'attack' means 'actions taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy computers, computer networks, or information residing in computers and computer networks'.[235] The definition

---

[233] Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 37 J.I.L.P. 57, fn 131. See also: Cassandra Kirsch, 'Science Fiction No More: Cyber Warfare and the United States' (2012) 40 Denv.J.Int'l.L.&Pol'y 620, 623; Phillip Pool, 'War of the Cyber World: The Law of Cyber Warfare' (2013) 47 Int.Lawyer 299, 306; Anna Wortham, 'Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?' (2012) 64 Fed.Comm.L.J. 643, 646.

[234] Wall (n.159) 118. See also: Gary Brown and Andrew Meltcaf, 'Easier Said Than Done: Legal Reviews of Cyber Weapons' (2014) 7 J.Nat'l.Sec.L.&Pol'y 115, 117-18; Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 1 Go.J.I.L. 375, 380.

[235] The White House, 'National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23' (2008) [7a]
<https://fas.org/irp/offdocs/nspd/nspd-54.pdf> accessed:25.06.2018.
See also: DoD, 'Joint Terminology for Cyberspace Operations' (2010-2011) 3
<www.nsci-va.org/CyberReferenceLib/2010-11
Joint%20Terminology%20for%20Cyberspace%20Operations.pdf> accessed:13.02.2018.

used by NATO,[236] Australia,[237] and Canada[238] are similar. Italy defines them as '[a]ctivities that are conducted in and through the cyberspace in order to manipulate, obstruct, deny, downgrade or destroy information stored in the ICT networks or in the computer systems, or the ICT networks or in the computer systems themselves'.[239] Colombia and Poland define 'cyber-attack' as follows: '[a]n organized and/or premeditated act by one or more persons to harm or cause problems to a computer system via cyberspace',[240] and 'an intentional disruption of the proper functioning of cyberspace'.[241] According to the Netherlands, it is '[a]n operation to disrupt, damage or destroy computers and networks or the information on them'.[242] Austria suggests that '[c]yber attacks directed against the integrity and availability of an IT system are referred to as cyber sabotage'.[243] Germany has a similar approach.[244] Belgium considers that sabotage is a type of cyber-attack which is 'disrupting the normal functioning of CIS [Computer Information Systems]'.[245] France suggests that 'computer sabotage' means 'rendering partly or totally ineffective the computer system of an organization via a computer attack'.[246] Chile does not define 'cyber-attacks' but two types of them: 'DOS [denial-of-service] and DDOS [distributed denial-

---

[236] NATO, 'computer network attack'
Accessed:*via* Natoterm <https://nso.nato.int/natoterm/Web.mvc> accessed:25.06.2018.

[237] Department of the Prime Minister and Cabinet (PM&C), *Australia's Cyber Security Strategy* (Commonwealth of Australia 2016) 15.

[238] RCAF Commander, *Canadian Forces Aerospace Shape Doctrine 2* (National Defence 2014) 106.

[239] PCM (n.107) 41.

[240] CONPES, 'Policy Guidelines' (n.112) 33.

[241] MAC (n.187) 5.

[242] AIV/CAVV (n.213) Annexe 3.

[243] BKA, 'Austrian Cyber Security Strategy' (2013) 20
<www.digitales.oesterreich.gv.at/documents/22124/30428/AustrianCyberSecurityStrategy.pdf/35f1c891-ca99-4185-9c8b-422cae8c8f21> accessed:02.10.2016.

[244] BMI (n.121) 14-15.

[245] Belgian MOD, 'Cyber Security Strategy for Defence' (2014) 7
<www.ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf> accessed:23.09.2016.

[246] French Government, 'Sabotage'
<www.gouvernement.fr/risques/sabotage> accessed:09.06.2018.

of-service]' attacks and '[a]ttacks against critical infrastructures through the cyberspace'.[247] As to the UK, its position is fluctuating. The British Security Service (MI5) still refers to CNAs that 'disrupt and damage cyberinfrastructure'.[248] Yet–and according to the National Cyber Security Centre (NCSC) in 2016–the feature of 'cyber-attack' was that they did 'cause harm'.[249] In 2018, its definition is the following: '[m]alicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means'.[250]

According to the USA, 'computer network exploitation' (CNE) or 'exploit' means 'enabling'[251]–or 'actions that enable'[252]–'operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks'. NATO defines it as an '[a]ction taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage'.[253] The UK suggests that CNE and cyber-espionage are similar, and defines them as 'the use of a computer network to infiltrate a target computer network and gather intelligence'.[254] Canada says that CNE is 'a directed, covert activity conducted through the use of computer networks to remotely enable access to, collect information from, and/or process information on computers

---

[247] Chilean Government (n.101) 35.

[248] MI5, 'Cyber'
<www.mi5.gov.uk/cyber> accessed:13.01.2018.

[249] UK Government, 'National Cyber Security Strategy 2016-2021' (2016) 74
<www.ncsc.gov.uk/content/files/protected_files/document_files/National%20Cyber%20Security%20Strategy%20v20.pdf> accessed:22.08.2016.

[250] NCSC, 'NSCS Glossary'
<www.ncsc.gov.uk/glossary> accessed:21.02.2018.

[251] GAO, 'Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates' (2011) 2
<www.gao.gov/assets/100/97674.pdf> accessed:01.11.2018.

[252] The White House, 'NSPD-54/HSPD-23' (n.235) 4.

[253] NATO, 'NATO Glossary of Terms and Definitions' (2015) AAP-06, 2-C-11
<http://wcnjk.wp.mil.pl/plik/file/N_20160219_AAP6EN.pdf> accessed:25.06.2018.

[254] UK Government, 'National Cyber Security Strategy 2016-2021' (n.249) 74.

or computer networks'.[255] Italy suggests that they are '[o]perations carried out in cyberspace in order to extract information from targeted ICT networks or computer systems. They are intelligence gathering activities, or actions preparing the execution of a cyber-attack'.[256] CNE is distinguished from cyber-espionage, as the latter is the 'improper acquisition of confidential or classified data, not necessarily of economic or commercial value'.[257] Other definitions of cyber-espionage are the following: the 'theft of information for intelligence purposes' (Australia),[258] '[t]he act or practice of obtaining secrets without the permission of the holder of the information' (Nigeria),[259] '[a cyber-threat] involving, inter alia, the silent gathering of classified information without the permission of the holder of the information' (South Africa),[260] 'the use of an agent in order to obtain information about plans or activities of foreign country or competitive company' (Montenegro),[261] or 'the use of computer networks to gain illicit access to confidential information, typically that by a government or other organization' (Philippines). [262] Belgium suggests that espionage is 'involving unnoticed intrusion of a third party into a CIS [Computer Information System] to read, change, delete or even add information (intrusion)'.[263] According to Austria, '[c]yber attacks directed against the confidentiality of an IT system are referred

---

[255] Melanie Bernier and Joanne Treurniet, 'CF Cyber Operations in the Future Cyber Environment Concept' (2009) 7 <http://cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf> accessed:13.05.2017.

[256] PCM (n.107) 41.

[257] Ibid 13.

[258] PM&C (n.237) 15.

[259] ONSA (n.208) appendix 2.

[260] South African Defence, 'Defence Review 2015' (2014) [75] <www.dod.mil.za/documents/defencereview/defence%20review%202015.pdf> accessed:18.05.2017.

[261] Montenegrin Government (n.168) 7.

[262] Department of Information and Communications Technology, 'National Cybersecurity Plan 2022' (2017) 46 <www.dict.gov.ph/wp-content/uploads/2017/04/FINAL_NationalCyberSecurityPlan2022.pdf> accessed:20.09.2017.

[263] Belgian MOD (n.245) 8.

to as "cyber espionage", i.e. digital spying'.[264] Germany has a similar position, but underlines that they 'are launched or managed by foreign intelligence services'.[265] 'Computer espionage' is also regarded by France as a form of 'computer attack'.[266] The Netherlands defines 'cyber-exploitation' as '[d]igitally copying data on other computers or networks', and 'cyber-espionage' as '[t]he clandestine gathering of information on networks or information systems by governments or enterprises to further their diplomatic, military or economic interests'.[267]

In some states, both destructive and theft activities are gathered under the same term of 'cyber-attacks'. They are defined as '[o]perations carried out deliberately by a person and/or information systems at any place in cyber space for the purpose of compromising the confidentiality, integrity or availability of information systems in national cyberspace' (Turkey),[268] or '[m]alicious acts directed to a computer device, usually through a telecommunications networks' (Morocco).[269] Jordan is also in this situation.[270]

In spite of their varying appellations, most states thus see a difference between operations aiming at or resulting in disruption, and theft. The former will be qualified as 'cyber-attacks' while the latter will be named 'cyber-espionage'. When considered together, the term 'cyber-operation' will be used. This choice is of didactic nature, as it allows better understanding of the American doctrine.

---

[264] BKA, 'Austrian Cyber Security Strategy' (n.243) 20

[265] BMI (n.121) 14-15.

[266] Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), 'Revue stratégique de cyberdéfense' (2018) 11 <www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf> accessed:24.04.2018.

[267] AIV/CAVV, 'Cyber Warfare' (n.213) Annexe 3.

[268] UDHB, '2016-2019 National Cyber Security Strategy' (n.126) 9-10.

[269] Administration de la Défense Nationale, 'Stratégie Nationale en matière de Cybersécurité' (2012) 19 <www.dgssi.gov.ma/dgssi_assets/user_upload/STRATEGIE_NATIONALE.pdf> accessed:23.09.2017.

[270] MICT (n.174) 8

Again, China and Russia seem to have a different perception. They refer to the general notion of 'computer attack', defined as 'a deliberate action through software systems (hardware and software) on the information resources, telecommunication networks and the automated process control systems, being implemented in order to disrupt the running of and (or) to breach security'.[271] Then, they refer to the 'improper use of the information resources', defined as 'the use of information systems and resources without the relevant entitlement or in violation of the established rules, legislation of each of the parties, or the norms of international law'. [272] The other notions include 'unauthorized interference with information resources' and 'threat to information security'.[273] They are respectively defined as, 'the undue influence on the processes of establishing, using, transmitting, processing and storing information', 'factors that endanger the basic interests of the individual, of society and of the state in the information area'.[274] Whether espionage fits or not within these definitions is unclear but again, the term 'cyber-espionage' is not totally absent from Chinese[275] and Russian[276] official communications.

'Attacks' and 'espionage' are not the only activities occurring in cyberspace. 'Cyber-crime' and 'cyber-security' are also common terms, and their relationships with espionage is at present enlightened.

---

[271] Russian government (n.160) 9.

[272] Ibid 10.

[273] Ibid.

[274] Ibid.

[275] See: FMPRC, 'Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on October 13, 2015' (2015) <www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1305571.shtml> accessed:15.02.2018);
FMPRC, 'Ambassador Liu Xiaoming Gives Interview to BBC Newsnight' (2015) <www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbd_665378/t1308244.shtml> accessed:22.01.2018.

[276] MID, 'Foreign Minister Sergey Lavrov's address and answers to questions at the 53rd Munich Security Conference, Munich, February 18, 2017' (2017) <http://www.mid.ru/en/web/guest/meropriyatiya_s_uchastiem_ministra/-/asset_publisher/xK1BhB2bUjd3/content/id/2648249> accessed:22.01.2018.

B. The relationships between 'cyber-crime', 'cyber-security, and 'cyber-espionage' in state practice

There is a consensus surrounding the scope of cyberspace security: preserving the confidentiality, integrity, and availability of data or information. This goal is underlined by Afghanistan,[277] the Czech Republic,[278] Austria,[279] Bangladesh,[280] Belgium,[281] India,[282] Italy,[283] Kenya,[284] Lithuania,[285] Luxemburg,[286] Mauritius,[287]

[277] Afghan MCIT (n.125) 8.

[278] National Security Authority, 'National Cyber Security Strategy for the period from 2015 to 2020' (2015) 5 <www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf>

[279] BKA, 'Austrian Cyber Security Strategy' (n.243) 7.

[280] MOPA (n.124) 9.

[281] Belgian MOD (n.245) 8.

[282] MEITY (n.167) 2.

[283] PCM (n.107) 12.

[284] Kenyan MICT (n.207) 16.

[285] Lithuanian Government, 'Resolution no 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011-2019' (2011) 1 <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf> accessed:29.09.2016.

[286] Gouvernement du Luxembourg, 'Stratégie nationale en matière de cyber sécurité II' (2015) 23 <https://cybersecurite.public.lu/content/dam/cybersecurite/fr/lu-ncss-2-fr-booklet.pdf> accessed:17.10.2016.

[287] Republic of Mauritius, 'National Cyber Security Strategy 2014-2019' (2014) 16 <http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf> accessed:03.10.2016

Montenegro,[288] Norway,[289] Poland,[290] Qatar,[291] Saudi Arabia,[292] Slovakia,[293] Turkey,[294] and Uganda.[295] Little variations appear among Finland,[296] Germany[297] (availability is not mentioned), the Netherlands ('exclusivity' replaces 'confidentiality'),[298] and Switzerland ('authenticity' is added).[299] It is likely that the ISO influenced states, as it defines 'cyberspace security' as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace'.[300] To the extent that it breaches 'confidentiality', 'cyber-espionage' may thus be at odds with 'cyber-security'.

---

[288] Montenegrin Government (n.168) 5.

[289] Norway Ministries, 'Cyber Security Strategy for Norway' (2012) 10, 28-9 <www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf> accessed:01.10.2016.

[290] MAC (n.187) 10.

[291] MOTC (n.186) 4.

[292] Saudi MCIT (n.123) 57.

[293] Slovak Republic, 'National Strategy for Information Security in the Slovak Republic' (2008) 6 <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Slovakia_National_Strategy_for_ISEC.pdf> accessed:01.10.2016.

[294] UDHB, 'National Cyber Security Strategy and 2013-2014 Action Plan' (2013) 9 <www.unodc.org/res/cld/lessons-learned/national_cyber_security_strategy_and_2013-2014_action_plan_html/National_Cyber_Security_Strategy_and_2013-2014_Action_Plan.pdf> accessed:02.10.2016.

[295] National Information Technology Authority (NITA), 'National Information Security Policy' (2014) [5.1] <www.nita.go.ug/sites/default/files/publications/National%20Information%20Security%20Policy%20v1.0_0.pdf> accessed:03.10.2016.

[296] 'Information security' is also used, rather than 'cybersecurity'. See DEFMIN, 'Security Strategy for Society' (2010) 93 <www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf> accessed:02.10.2016.

[297] BMI (n.121) 2.

[298] 'Reliability' is also used rather than 'cybersecurity'. Dutch MOD, 'The Defence Cyber Strategy' (2012) 5 <www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf> accessed:29.09.2016.

[299] VBS (n.111) 7.

[300] Guidelines for cybersecurity ISO/IEC 27032:2012

It transpires from some states' opinions that cybercrime is motived by financial gains, and usually carried out by private actors.[301] Yet, this distinction may mitigate. As was done for espionage, cyber-intrusions are increasingly prohibited by domestic criminal legislations,[302] and it is not impossible for a governmental cyber-spy to be indicted before foreign jurisdictions. For instance, in 2014, a grand jury in Pennsylvania 'indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries'.[303]

C. Conclusion

In spite of different formulations, definitions of 'cyber-espionage', 'computer-network exploitation' and 'cyber exploitation' share similarities. In essence, they answer two questions: 1) The nature and goals of cyber-espionage; and 2) The means or target of cyber-espionage.

(1) On this first aspect, three types of expressions are to be found: those referring to theft ('theft of information', 'improper acquisition'), to the breach of information confidentiality ('illicit access', 'gathering of classified information', various action against the 'confidentiality') or to the clandestine nature of espionage ('unnoticed intrusion', 'silent gathering', 'covert activity'). Cyber-espionage thus appears to be a clandestine activity, involving an access to confidential information, and–hence–illegal in domestic law.

(2) On this second aspect, cyber-espionage uses or is conducted through 'computer networks', or is directed towards 'CIS' and 'ICT'. The 'element of cyber' is to be found here. Cyber-espionage is thus essentially an activity resorting to computer networks, and targeting an information system.

---

[301] SGDSN (n.266) 12; PCM (n.107) 13.

[302] See part III.

[303] Department of Justice (DoJ), 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage' (19.05.2014) <www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> accessed:26.04.2018.

This thesis does not intend to give an objective and universal definition of cyber-espionage, but some details in the use of terminology is required for the purpose of this study.

First, cyber-espionage is state-sponsored.

Second, it is a remote activity, either because it has been launched/sent (backdoors, spyware, spear phishing, Trojan spies) or activated (supply-chain backdoors) outside the borders of the targeted state. 'The supply chain is all of the various stages, in order, of a product's progress from raw materials through production and distribution of the finished product, until it reaches the consumer'. [304] 'Effectively securing the supply chain can be hard because vulnerabilities can be inherent, or introduced and exploited at any point in the supply chain'.[305] This is how specific chips may be inserted in 'computer and networking hardware', subsequently allowing 'the attackers to create a stealth doorway [backdoor] into any network that included the altered machines'.[306] 'There are two ways for spies to alter the guts of computer equipment. One, known as interdiction, consists of manipulating devices as they're in transit from manufacturer to customer […] The other method involves seeding changes from the very beginning'–i.e., 'during the manufacturing process'.[307] The first method was allegedly carried out by the NSA: 'agents carefully open the package in order to load malware onto the electronics, or even install hardware components that can provide backdoor access for the intelligence agencies. All subsequent steps can then be conducted from the comfort of a remote computer'.[308] The second method has allegedly been resorted to by China, where 'chips' were 'inserted at

---

[304] 'Supply chain' (*Collins*) <www.collinsdictionary.com/dictionary/english/supply-chain> accessed:31.10.2018.

[305] NCSC, 'The principles of supply chain security' (28.01.2018) <www.ncsc.gov.uk/guidance/principles-supply-chain-security> accessed:30.10.2018.

[306] Michael Riley and Jordan Robertson, 'The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies', *Bloomberg* (04.10.2018) <www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies> accessed:31.10.2018.

[307] Ibid.

[308] Staff, 'Documents Reveal Top NSA Hacking Unit', *Spiegel* (29.12.2013) <www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html> accessed:31.10.2018.

factories'.[309] Spying through a supply-chain backdoor–to the extent that it needs to be activated and operated remotely–is still considered as cyber-espionage. In contrast, extracting signal from a cable is qualified as tapping. The cable can be tapped at the entry or exit point. For instance, '[t]he GCHQ mass tapping operation' attached 'intercept probes to transatlantic fibre-optic cables where they land on British shores carrying data to western Europe from telephone exchanges and internet servers in north America'.[310] Yet, '[t]he cable iself is vulnerable to attacks', and may be tapped thanks to two main methods: fibre-bending and optical-splitting.[311] With fibre-bending 'the cable's coating is peeled down to the protective material covering the fibre itself, enabling the attacker to bend the cable to a point where light can be collected from the cable'.[312] With optical-splitting, 'the optical cable is split using a clip that cuts into the cable and attaches a second fibre cable, which transmits light from the main fibre to a device controlled by the attacker'.[313] For example, the submarine *USS Jimmy Carter* is allegedly able to 'hook' undersea cables.[314] To the extent that the different tapping techniques require a continuous physical access to the cable,[315] it is regarded as a form of traditional espionage and is not analysed in this thesis. In any case, tapping is not a legal vacuum: it actually falls under the legal framework applicable to the geographical place in which it occurs (high sea, territorial sea, foreign or national territory.

---

[309] Robertson and Riley (n.306).

[310] Evan MacAskill and others, 'GCHQ taps fibre-optic cables for secret access to world's communications', *Guardian* (21.06.2013) <www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed:31.10.2018.

[311] 'Tapping of fibre networks' (*Deloitte*, 2017) 5 <https://zybersafe.com/wordpress/wp-content/uploads/2018/01/Deloitte_Fiber_tapping_Q1_2017_English.pdf> accessed:31.10.2018.

[312] Ibid 6.

[313] Ibid 7.

[314] David Axe, 'The Navy's underwater eavesdropper', *Reuters* (19.06.2013) <http://blogs.reuters.com/great-debate/2013/07/18/the-navys-underwater-eavesdropper/> accessed:31.10.2018

[315] MacAskill and others (n.310).

Third, this thesis acknowledges that 'the distinction between a cyberattack and a cyberexploitation may be very hard to draw from a technical standpoint, since both start with taking advantage of a vulnerability'.[316] As a matter of fact, '[b]oth offensive cyber activity and cyberespionage rely on acquiring unauthorized access to a system, and that often involves damaging a system in some way. The damage may be reducing the effectiveness of the target system's anti-virus software, decreasing the effectiveness of its encryption programs, installing a back door or altering its operating system'.[317] Moreover, establishing intent may be difficult in cyberspace. As underlined by Brown, '[o]ften, military operations in cyberspace and cyberespionage are distinguishable only by intent, which is difficult or impossible for the victim to ascertain […] Discussions about what is okay and what is not would be easier if they focused purely on the activities themselves, rather than trying to pigeonhole cyber behaviors according to intent'.[318] Yet, the intent underlying a cyber-attack is a vital element in many definitions. This element is obvious in Colombian ('premeditated act'), Polish ('intentional'), and Italian definitions ('in order to'). It is also essential in the like American, Australian, Canadian and NATO definitions, all the more with the confirmation from the French official translation, provided by two of them: '[a]ction *destinée à* perturber, rendre inaccessibles, détériorer ou détruire soit les informations résidant dans un ordinateur ou dans un réseau d'ordinateurs, soit l'ordinateur ou le réseau d'ordinateurs lui-même'.[319] Definitions of cyber-espionage are more diverse, but none of them refers to the means allowing intelligence gathering. As acknowledged by Pun, '[t]he core problem raised by the definitions is that the collection of information itself does not specify limitations to the methods'.[320] The intentional element is obviously present in

---

316 Kenneth Dam, William Owens and Herbert Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (N.A.P. 2009) 261.

317 Gary Brown, 'Spying and Fighting in Cyberspace: What is Which' (2016) 8 J.Nat'l.Sec.L.&Pol'y 621, 626.

318 Ibid 635.

319 RCAF Commander, *Doctrine Aérospatiale des Forces Canadiennes-Acquisition de l'Avantage* (Défense Nationale 2014) 121; 'attaques de réseaux informatiques' (*NatoTerm*).

320 Darien Pun, 'Rethinking Espionage in the Modern Era' (2017) 18(1) Chi.J.Int'l.L. 353, 374.

Italian and Montenegrin definitions ('in order to'). Both Belgian ('change, delete or even add information') and American definitions tolerate a degree of disruption. Regarding the latter, Brown has the following words: '[t]he critical phrase is "enabling operations," which includes cyber activity that would otherwise be considered a cyber attack as noted above. That is, an enabling operation could logically include physically damaging one system to facilitate the gathering of intelligence from another system'.[321] This possible overlap between *attacks* and *espionage* (or *exploitation*) could thus have been assimilated by states, which chose to maintain the distinction between them.[322] It is noteworthy, for instance, that the *Office of Personnel Management* (OPM) data breach–during which hackers were able 'to infiltrate and compromise' the information system before stealing information[323]–was still treated as a cyber-espionage case.[324] In contrast, *Sony Pictures* hack stole data, but also 'destroyed 70 percent of Sony Pictures' laptops and computers',[325] using 'a Server Message Block (SMB) Worm Tool to conduct the attacks'.[326] This SMB worm tool was 'equipped with a Listening Implant, Lightweight Backdoor, Proxy Tool, Destructive Hard Drive Tool, and Destructive Target Cleaning Tool'.[327] The latter two were 'intended to destroy data past the point of recovery' and rendered 'victim machines inoperable by overwriting the Master Boot Record'.[328] Obama qualified it as 'an act of cyber

---

321 Brown (n.317) 626.

322 See: ibid 626.

323 House of Representatives (HoR), Committee on Oversight and Government Reform, 'The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation' (07.09.2016) vii <https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf> accessed:01.11.2018.

324 Efrony and Shany (n.62) 603.

325 David Kirkpatrick, Nicole Pelroth and David Sanger, 'The World Once Laughed at North Korean Cyberpower. No More.', *NYT* (15.10.2017) <www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html> accessed:01.11.2018.

326 Mike Lennon, 'Hackers Used Sophisticated SMB Worm Tool to Attack Sony', *SecurityWeek* (19.12.2014) <www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony> accessed:01.11.2018.

327 US-CERT, 'Alert (TA14-353A)-Targeted Destructive Malware' (30.09.2016) <www.us-cert.gov/ncas/alerts/TA14-353A> accessed:01.11.2018.

vandalism that was very costly', but not 'an act of war'.[329] At the end of the day, the perenniality of cyber-espionage calls for a maximal reduction of damage: 'the best cyberexploitation is one that such a user never notices'.[330]

Cyber-espionage will thus be understood as 'a state-sponsored activity, whether launched, deployed or operated remotely through the use of computer networks, which seeks an unauthorized access to confidential data resident on an information-system for intelligence purposes, and involving minimal damage in securing such access'.

Definitions of cyberspace and cyber-espionage have been introduced, and the applicability of international law in this new 'domain' has been ascertained. Yet, developing a conceptual framework is necessary to apply 'international law' to 'cyber-espionage'.

4. Conceptual framework

It is usually considered that international rules emanate from three sources, as mentioned in article 38 of the ICJ Statute: treaty, CIL, and the general principles of law.[331] Some authors now consider the possibility to have 'new sources of international outside of Article 38'.[332] Yet, this thesis focuses on both treaties and CIL, tackling their respective approaches in an *approach to treaty interpretation* (4.1) and an *approach to sources* (4.2). This dichotomy may be explained: the goal of the first exercise is to give meaning to a pre-existing instrument–'the

---

[328] Ibid.

[329] Sean Sullivan, 'Obama: North Korea hack "cyber-vandalism," not "act of war"', *WP* (21.12.2014) <www.washingtonpost.com/news/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/?utm_term=.fa09e66b5422> accessed:01.11.2018.

[330] Dam, Owens and Lin (n.316) 11.

[331] Hugh Thirlway, *International Customary Law and Codification* (Springer 1972) 27; Hugh Thirlway, *The Sources of International Law* (O.U.P. 2014).

[332] Malgosia Fitzmaurice, 'The History of Article 38 of the Statute of the International Court of Justice' in Samantha Besson, Jean d'Aspremont and Séverine Knuchel, *The Oxford Handbook of the Sources of International Law* (O.U.P. 2017) 194.

determination of the content of rules'[333]–while the second focuses on the birth of a new rule–'the ascertainment of the rules themselves'.[334] This approach is well described by Venzke and d'Aspremont. According to the former, 'interpreting and applying the law is understood as distinct from law-making which, as a matter of sources, lies beyond the reach of the everyday operation of the law',[335] even if '[i]nterpretations [...] complement the role of sources in the law-making process'.[336] D'Aspremont calls it the 'twofold dichotomy between bindingness and interpretative effects (and thus, between sources and interpretation)'.[337] On the one hand, 'the identification of norms and standards formally binding upon a legal relation is operated by virtue of the doctrine of the sources of international law that finds its most basic expression in Article 38 of the Statute of the International Court of Justice'.[338] On the other hand, 'the determination of the content of the norms and standards applicable to a given legal relation is carried out on the basis of the doctrine of interpretation, which finds its most refined expression in the 1969 and 1986 Vienna Conventions on the Law of Treaties'.[339] A central notion, used throughout the thesis, is finally explained: *state practice* (4.3).

4.1. Approach to treaty interpretation

The construction of the VCLT needs to be explained (A). However, the normativity of these rules has sometimes been challenged, and this issue needs

---

[333] Jean d'Aspremont, 'The Multidimensional Process of Interpretation' in Andrea Bianchi, Daniel Peat and Matthew Windsor (eds), *Interpretation in International Law* (O.U.P. 2015) 117.

[334] Ibid.

[335] Ingo Venzke, 'Contemporary theories and international lawmaking' in Catherine Brölmann and Yannick Radi (eds), *Research Handbook on the Theory and Practice of International Lawmaking* (E.E. 2016) 70.

[336] Inzo Venzke, 'Sources in Interpretation Theories' in Besson, d'Aspremont and Knuchel (n.332) 402.

[337] Jean d'Aspremont, 'The International Court of Justice, the Whales, and the Blurring of the Lines between Sources and Interpretation' (2016) 27(4) E.J.I.L. 1027, 1028-9.

[338] Ibid.

[339] Ibid.

to be tackled (B). Moreover, some aspects of treaty interpretation have not been defined by the VCLT, for example in respect of both 'constitutive' treaties of international organizations (D) and 'ordinary' treaties (C) which contain different features and which are separately ascertained.

A. The construction of the VCLT rules of interpretation

Before the VCLT's drafting, numerous cases dealt with the modalities of treaty interpretation. Firstly, it had been asserted that establishing the common intention of parties was the goal of interpretation.[340] Then, case-law determined that words are to be interpreted in the context in which they are used.[341] Some judges suggested that subsequent practice[342] or the subject and aim of the convention may be taken into account,[343] while preparatory works may only be resorted to in a subsidiary fashion.[344] This approach has subsequently been endorsed by the ICJ, as 'the first duty of a tribunal which is called upon to interpret and apply the provisions of a treaty, is to endeavour to give effect to them in their natural and ordinary meaning in the context in which they occur'. It is only if 'the words in their natural and ordinary meaning are ambiguous or lead to an unreasonable result' that the tribunal may resort 'to other methods of interpretation'.[345]

---

[340] *Dissenting Opinion* (DO) *Anzilotti* in *Interpretation of the Convention of 1919 concerning the employment of Women during the Night* (Advisory Opinion) [1932] PCIJ Rep Series A/B No.50, 383; *Competence of the General Assembly for the Admission of a State to the United Nations* (Advisory Opinion) [1950] ICJ Rep 4, 8*; DO Winiarski* in *Certain Expenses of the United Nations (Article 17, Paragraph 2, of the Charter)* (Advisory Opinion) [1962] ICJ Rep 151, 230-1.

[341] *Polish Postal Service in Danzig* (Advisory Opinion) [1925] PCIJ Rep Series B No.11, 39; *Competence of the General Assembly* (n.340) 8; *Constitution of the Maritime Safety Committee of the Inter-Governmental Maritime Consultative Organization* (Advisory Opinion) [1960] ICJ Rep 150, 158.

[342] *DO Winiarski* (n.340) 230.

[343] *DO Anzilotti* (n.340) 383.

[344] *DO Anzilotti* (n.340) 388; *DO Alvarez* in *Competence of the General Assembly* (n.340)18.

[345] *Competence of the General Assembly* (n.340) 8.

Such considerations have all been confirmed by the VCLT, which defines a 'general rule of interpretation' (article 31) and 'supplementary means of interpretation' (article 32).

According to article 31(1), '[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose'. 'Context' is then defined in article 31(2). 'The context for the purpose of the interpretation of a treaty shall comprise, in addition to the text, including its preamble and annexes': '[a]ny agreement relating to the treaty which was made between all the parties in connexion with the conclusion of the treaty',[346] and '[a]ny instrument which was made by one or more parties in connexion with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty'.[347] Then, article 31(3) specifies that '[t]here shall be taken into account, together with the context': '[a]ny subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions',[348] '[a]ny subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation',[349] and '[a]ny relevant rules of international law applicable in the relations between the parties'.[350] Finally, article 31(4) mentions that '[a] special meaning shall be given to a term if it is established that the parties so intended'.

According to article 32, '[r]ecourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of article 31, or to determine the meaning when the interpretation according to article 31': '[l]eaves the meaning ambiguous or obscure',[351] or '[l]eads to a result which is manifestly absurd or unreasonable'.[352]

---

[346] VCLT, art.31(2)(a).

[347] VCLT, art.31(2)(b).

[348] VCLT, art.31(3)(a).

[349] VCLT, art.31(3)(b).

[350] VCLT, art.31(3)(c).

[351] VCLT, art.32(a).

[352] VCLT, art.32(b).

These rules are primarily textual, as underlined by the ILC and the ICJ. Waldock himself highlighted that 'the text must be presumed to be the authentic expression of the intentions of the parties […] in consequence, the starting point of interpretation is the elucidation of the meaning of the text, not an investigation *ab initio* into the intentions of the parties'.[353] He was aware that two other approaches (subjective and teleological) existed in doctrine, acknowledged that 'none of these approaches is exclusively the correct one',[354] but finally qualified 'the actual text' as 'the dominant factor in the interpretation of the treaty'.[355] This primacy was confirmed by the ICJ in 1994, as 'interpretation must be based above all upon the text of the treaty'.[356] Divergent approaches have sometimes been used by arbitral tribunals,[357] or even the ICJ.[358]

In spite of this jurisdictional building and conventional consecration, these rules have sometimes been challenged by doctrine.

B. The challenges to the normativity of the VCLT rules of interpretation

Some authors consider that the VCLT does not contain rules *per se*. Klabbers explains that articles 31 and 32 'are best seen as methodological devices', then adds that 'there are various different ways to engage in many activities, without it being possible to specify which one would be the best'.[359] Van Damme thinks

---

[353] Humphrey Waldock, 'Fifth Report on the Law of Treaties' (1965-6) UN-Doc A/CN.4/183, 220.

[354] Humphrey Waldock, 'Third Report on the law of treaties' (1964) UN-Doc A/CN.4/167, 54.

[355] Ibid 56.

[356] *Territorial Dispute (Libya/Chad)* (Judgment) [1990] ICJ Rep 6, [41].

[357] *Case concerning the audit of accounts between the Netherlands and France pursuant to the Additional Protocol of 25 September 1991 to the Convention on the Protection of the Rhine against Pollution by Chlorides of 3 December 1976 (France/Netherlands)* (2004) 25 RIAA 267, [63]-[64]; *Award in the Arbitration regarding the Iron Rhine ("Ijzeren Rijn") Railway (Belgium/Netherlands)* (2005) 27 RIAA 35, [53].

[358] *Nicaragua* (n.46) [275]; Jan Klabbers, 'Treaties, Object and Purpose' (2006) M.P.E.P.I.L., [19].

[359] Jan Klabbers, 'The Invisible College' (*Opinio Juris*, 03.03.2009)

that '[t]he qualification of Articles 31 to 33 VCLT as binding "rules" does not seem satisfactory for norms that govern interpretation'.[360] She thinks that 'it is hard to conceive how the process of interpretation can be governed by legal rules in the ordinary sense of the term, as relatively determinate directions to a given result', and prefers to call them 'principles'.[361]

Waibel qualifies them as an 'intellectual checklist'[362] and 'the lowest common denominator among competing schools of interpretation'.[363] He adds that '[t]he VCLT does not contain interpretative rules, but codified interpretive principles that do not provide step-by-step guidance. They *enable* the interpreter to use a set of methodological tools'.[364] Then, he thinks that '[w]ithin the VCLT's broad parameters, interpreters are able to tailor the VCLT's interpretive framework to their own needs and preferences. They can, by and large, disengage from the VCLT's interpretive principles if and when it suits them'.[365] Moreover, 'it is de rigueur to invoke the VCLT', but '[r]eferences to the VCLT as such do not tell us much about whether an international court or tribunal is in fact deviating from the VCLT's interpretative canon'.[366] He nevertheless suggests a 'way of reconciling the VCLT's unified interpretive framework with interpretive varieties': 'to characterize each and every divergence from the VCLT as an "incorrect" application of the VCLT'.[367]

In spite of these contestations, the VCLT rules remain a dominant and inescapable guide to treaty interpretation. Whilst only 116 states are party to the

---

<http://opiniojuris.org/2009/03/03/the-invisible-college/> accessed:03.05.2017.

[360] Isabelle Van Damme, *Treaty Interpretation by the WTO Appellate Body* (O.U.P. 2009) 35.

[361] Ibid. See also: Vladimir Đuro Degan, *Sources of International Law* (M.N.P. 1997) 92.

[362] Michael Waibel, 'Uniformity versus specialization (2): A uniform regime of treaty interpretation?' in Christian Tams and others (eds), *Research Handbook on the Law of Treaties* (E.E. 2014) 381.

[363] Ibid 380.

[364] Ibid.

[365] Ibid.

[366] Ibid 386-8.

[367] Ibid 410-11.

VCLT, the customary nature of its rules of interpretation has been highlighted by some non-parties,[368] as well as authors[369] (in full,[370] or in part).[371] It has moreover regularly been confirmed by the ICJ.[372] While divergences in the final interpretation may indeed occur depending on the interpreter, the fact remains that the VCLT rules are systematically applied by international courts and tribunals, regardless of their binding or non-binding nature. As d'Aspremont says, they are 'the cards of the game that enjoy almost universal consensus'.[373] As a consequence, 'it does not matter whether they are legal rules properly so-called, or merely guiding principles or directives, as their legal force is unlikely to affect their potential for yielding constraints'.[374]
This thesis will thus reflect this continuity and apply the VCLT rules to the treaties under scope.

However, some aspects of the interpretation of 'ordinary' treaties are not expressly tackled by the VCLT, and necessitate a study of case-law.

---

368 *Kasikili/Sedudu Island (Botswana/Namibia)* (Judgment) [1999] ICJ Rep 1045, [18].

369 For the opposite vision, see: Jean d'Aspremont, 'Sources in Legal-Formalist Theories' in Besson, d'Aspremont and Knuchel (n.332) 376-7.

370 Joost Pauwelyn and Manfred Elsig, 'The Politics of Treaty Interpretation: Variations and Explanations across International Tribunals' in Jeffrey Dunoff and Mark Pollack (eds), *Interdisciplinary Perspectives on International Law and International Relations: The State of the Art* (C.U.P. 2013) 448.

371 Mark Viliger, 'The Rules on Interpretation: Misgivings, Misunderstandings, Miscarriage? The "Crucible" Intended by the International Law Commission' in Enzo Cannizzaro (ed), *The Law of Treaties Beyond the Vienna Convention* (O.U.P. 2011) 117, 121.

372 *Arbitral Award of 31 July 1989 (Guinea-Bissau v Senegal)* (Judgment) [1991] ICJ Rep 53, [48]; *Territorial Dispute (Libya/Chad)* (Judgment) [1990] ICJ Rep 6, [41]; *Legality of the Use by a State of Nuclear Weapons in Armed Conflict* (Advisory Opinion) [1996] ICJ Rep 66, [19]; *LaGrand* (n.79) [99]; *Case concerning Sovereignty over Pulau Ligitan and Pulau Sipadan (Indonesia/Malaysia)* (Judgment) [2002] ICJ Rep 625, [37]; *Avena and Other Mexican Nationals (Mexico v USA)* (Judgment) [2004] ICJ Rep 12, [83]; *Legality of Use of Force (Serbia-and-Montenegro v Belgium)* (Preliminary Objections) [2004] ICJ Rep 279, [100]; *Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Judgment) [2010] ICJ Rep 14, [64]; *Maritime Dispute (Peru v Chile)* (Judgment) [2014] ICJ Rep 3, [57]; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v Serbia)* (Judgment) [2015] ICJ Rep 3, [138].

373 Jean d'Aspremont, 'The Multidimensional Process of Interpretation' in Bianchi, Peat and Windsor (n.333) 116.

374 Ibid 123.

C. The interpretation of 'ordinary' treaties

Some facets of treaty interpretation have not been expressly addressed by the VCLT, but rather by international courts: evolutionary interpretation (a), as well as strict and extensive interpretation (b). A conclusion to this development is then displayed (c).

a. Evolutionary interpretation

In the *South West Africa* case, the ICJ determined that some notions are 'by definition evolutionary' and added that 'an international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation'.[375]

However, Judge Bedjaoui supported the '[p]rimacy of the Principle of the "Fixed Reference" (Renvoi Fixe) over the Principle of the "Mobile Reference" (Renvoi Mobile)',[376] considering that the latter may 'be recommended only in exceptional cases'.[377] He added that, 'in applying the so-called principle of *the evolutionary interpretation* of a treaty [...] the Court should have clarified the issue more and should have recalled that the general rule governing the interpretation of a treaty remains that set out in Article 31 of the 1969 Vienna Convention'. [378]

The ICJ uses the criterion of 'generic term'. Indeed, '[o]nce it is established that the expression [...] was used [...] as a generic term [...] the presumption necessarily arises that its meaning was intended to follow the evolution of the law'.[379] The Court confirmed in 2009 that in some cases, parties' intentions are presumed to confer an evolutionary nature to treaties' terms. Such is the case when generic terms are used and when the treaty was made for a continuing period or drafted

---

375 *South West Africa* (n.72) [31].

376 *SO Bedjaoui* in *Case concerning the Gabcikovo-Nagymaros Project (Hungary/Slovakia)* (Judgment) [1997] ICJ Rep 7, 122.

377 Ibid.

378 Ibid 124.

379 *Aegean Sea Continental Shelf (Greece v Turkey)* (Judgment) [1978] ICJ Rep 3, [77].

for a continuing duration.[380] In 2014, the ICJ also ruled that '[t]he functions conferred on the Commission have made the Convention an evolving instrument'.[381]

The *Iron Rhine* arbitration referred to the *South-West Africa* and *Aegean Sea* cases to determine that generic terms had to be interpreted in an evolutionary manner. While acknowledging that 'it is not a conceptual or generic term that is in issue, but rather new technical developments', the panel considered 'that an evolutive interpretation, which would ensure an application of the treaty that would be effective in terms of its object and purpose, will be preferred to a strict application of the intertemporal rule'.[382]

Case-law proves that the main factor to be considered before activating an evolutionary interpretation is the parties' intentions, as reflected in the text. Similarly, the choice between a strict and an extensive interpretation depends on the parties' intentions.

b. Strict and extensive interpretation

In 1925, the PCIJ already affirmed that 'the rules as to a strict or liberal construction of treaty stipulations can be applied only in cases where ordinary methods of interpretation have failed'.[383] Indeed, '[i]t is a cardinal principle of interpretation that words must be interpreted in the sense which they would normally have in their context, unless such interpretation would lead to something unreasonable or absurd'.[384] The ICJ also underlined that a 'treaty provision which has the purpose of limiting the sovereign powers of a State

---

[380] *Dispute regarding Navigational and related Rights (Costa Rica v Nicaragua)* (Judgment) [2009] ICJ Rep 213, [66].

[381] *Whaling in the Antarctic (Australia v Japan: New Zealand intervening)* (Judgment) [2014] ICJ Rep 226, [45].

[382] *Iron Rhine* (n.357) [79]-[80].

[383] *Polish Postal Service in Danzig* (n.341) 39.

[384] Ibid.

must be interpreted like any other provision of a treaty, i.e. in accordance with the intentions of its authors as reflected by the text of the treaty and the other relevant factors in terms of interpretation'.[385] The *Iron Rhine* award resorted to a slightly different reasoning, as '[t]he doctrine of restrictive interpretation never had a hierarchical supremacy, but was a technique to ensure a proper balance of the distribution of rights within a treaty system', and was 'not in fact mentioned in the provisions of the Vienna Convention'.[386]

c. Conclusion

It is primarily with respect to parties' intentions, as reflected in the text, that treaties have to be interpreted. And it is only following such reasoning that a contemporary or an evolutionary, a strict or an extensive interpretation, is to be promoted. It remains to be seen whether this conclusion is also valid for the interpretation of 'constitutive' treaties of international organizations.

D. The interpretation of 'constitutive' treaties of international organisations

The interpretation of 'constitutive' treaties of international organisations differs from 'ordinary' treaties in two aspects: the theory of implied powers (a), and the special application of article 31 VCLT (b). A conclusion is then displayed (c).

a. The theory of implied powers

As of 1926, the PCIJ considered that a limitation of power of the International Labour Organisation (ILO) would be inconsistent with the aim and scope of the Peace Treaty of Versailles, and would have necessarily been expressed in its provisions.[387]

---

[385] *Navigational and related Rights* (n.380) [48].

[386] *Iron Rhine* (n.357) [53].

[387] *Competence of the International Labour Organization to Regulate, incidentally, the Personal Work of the Employer* (Advisory Opinion) [1926] PCIJ Rep Series B No.13, 18.

This question was then raised with respect to UN powers. In 1949, the ICJ considered that 'the Organization must be deemed to have those powers which, though not expressly provided in the Charter' were 'conferred upon it' because they were 'essential to the performance of its duties'.[388]

According to Judge Alvarez, 'rights' which the institution 'does not possess according to the provisions by which it was created' may be attributed 'by way of interpretation' if they 'are in harmony with the nature and objects' of the institution.[389]

According to Judge Winiarski, the purposes of the United Nations are set in very wide and indefinite terms. However, 'it does not follow [...] that the Organization is entitled to seek to achieve those purposes by no matter what means'.[390] The parties' intention 'was clearly to abandon the possibility of useful action rather than to sacrifice the balance of carefully established fields of competence'.[391] It is only through these 'clearly defined' procedures 'that the United Nations can seek to achieve its purposes'.[392] 'It may be that the United Nations is sometimes not in a position to undertake action which would be useful for the maintenance of international peace and security [...] but that is the way in which the Organization was conceived and brought into being'.[393] Then, '[t]he same reasoning applies to [...] the rule of effectiveness (*ut res magis valeat quam pereat*) and, perhaps less strictly, to the doctrine of implied powers'.[394]

Brölmann refers to the *Reparation* case, the *Effects of Awards* case, and the *Namibia* opinion, noting that there 'are all instances where there was little attention to the "intentions" of the treaty parties, while the degree of teleological reasoning in interpreting the UN Charter exceeded that of traditional interpretive

---

[388] *Reparation for Injuries suffered in the Service of the United Nations* (Advisory Opinion) [1949] ICJ Rep 174, 182-3.

[389] *DO Alvarez* in *Competence of the General Assembly* (n.340) 18.

[390] *DO Winiarski* (n.340) 230.

[391] Ibid.

[392] Ibid.

[393] Ibid.

[394] Ibid.

exercises'.[395] She thus considers that 'a teleological approach applies whenever the interpretation of the constitutive instrument is aimed at determining the competences of the IO, and thus moves within an institutional discourse'.[396]

However, a limit was put onto the theory of implied powers thanks to the advisory opinion of 1996. Indeed, '[i]t is generally accepted that international organizations can exercise [...] "implied powers"'.[397] These powers were defined as follows: 'the necessities of international life may point to the need for organizations, in order to achieve their objectives, to possess subsidiary powers which are not expressly provided for in the basic instruments which govern their activities'.[398] The implied powers are thus limited to those 'subsidiary' and 'necessary' for the IO 'to achieve objectives'. According to Klabbers, this is a landmark case which reveals a 'trend to interpret organizational powers rather more narrowly than in the past'.[399] The 'message' seems 'clear': 'the more well-established international organizations have reached the limits, at least for the time being, of what they can actually engage in'.[400] According to Blokker, 'the recognition of the existence of implied powers was important to assist in the establishment and early years of functioning of international organizations. However, as they have become a well-established phenomenon in international relations, there is room for a more critical appraisal of them'.[401]

Even the ECJ became more cautious regarding the scope of implied powers. In 1971, it concluded that–lacking explicit power to do so–the European

---

[395] Catherine Brölmann, 'Specialized Rules of Treaty Interpretation: International Organizations' in Duncan Hollis (ed), *The Oxford Guide to Treaties* (O.U.P. 2012) 513.

[396] Ibid.

[397] *Legality of the Threat or Use of Nuclear Weapons in Armed Conflict* (Advisory Opinion) [1996] ICJ Rep 66, [25].

[398] Ibid.

[399] Jan Klabbers, *An Introduction to International Institutional Law* (C.U.P. 2012) 70-1.

[400] Ibid.

[401] Niels Blokker, 'International Organizations or Institutions, Implied Powers' (2009) M.P.E.P.I.L., [12].

Community (EC) nevertheless had the power to reach international agreements in the area of transport. Indeed, '[t]o determine in a particular case the Community's authority to enter into international agreements, regard must be had to the whole scheme of the Treaty no less than to its substantive provisions'.[402] In 1991, it concluded that 'authority to enter into international commitments may not only arise from an express attribution by the Treaty, but may also flow implicitly from its provision'.[403]

The 'implied powers' constitute a first particularity in the interpretation of constitutive treaties. A second particularity may be found in a somehow 'special' application of article 31 VCLT.

b. The special application of article 31 VCLT

In 1950, Judge Alvarez considered that 'three categories of treaties'–'peace treaties, in particular those affecting world peace; treaties creating principles of international law; and treaties creating an international organization, notably the world organization'–should not 'be interpreted literally, but primarily having regard to their purposes'.[404]

In 1962, the ICJ mentioned that, when it 'had to interpret the [UN] Charter', it had 'followed the principles and rules applicable in general to the interpretation of treaties', 'since it ha[d] recognized that the Charter is a multilateral treaty, albeit a treaty having certain special characteristics'.[405] Thus, 'the Court was led to consider "the structure of the Charter" and "the relations established by it between the General Assembly and the Security Council"'. In the matter submitted for its attention in 1962, the Court also considered 'the manner in

---

[402] *Commission of the European Communities v Council of the European Communities* (22/70) [1971] ECR 263, [15].

[403] *Draft agreement between the Community, on the one hand, and the countries of the European Free Trade Association, on the other, relating to the creation of the European Economic Area* (1/91) [1991] ECR I-6079, I-1076.

[404] *DO Alvarez* in *Competence of the General Assembly* (n.340) 16-17.

[405] *Certain Expenses of the United Nations* (n.340) 157.

which the organs concerned "ha[d] consistently interpreted the text" in their practice'.[406]

The advisory opinion of 1996 then went further: '[f]rom a formal standpoint, the constituent instruments of international organizations are multilateral treaties, to which the well-established rules of treaty interpretation apply'.[407] However, they 'are also treaties of a particular type', as 'their object is to create new subjects of law endowed with a certain autonomy, to which the parties entrust the task of realizing common goals'.[408] Thus, they 'can raise specific problems of interpretation'–linked to the nature of the IO, its objectives, imperatives and own practice–and these elements 'may deserve special attention when the time comes to interpret these constituent treaties'.[409]

The compliance of regional organizations (EU, Council of Europe) with the VCLT rules raises further discussion. Both the ECtHR and the IACtHR resorted to an evolutionary interpretation, but were careful in referring to the VCLT. Before ruling in *Tyrer* that 'the Convention is a living instrument which, as the Commission rightly stressed, must be interpreted in the light of present-day conditions',[410] the ECtHR had mentioned in *Golder* that it 'should be guided by Art 31 to 33' of the VCLT.[411] The ECtHR has since regularly resorted to the VCLT, including in the famous *Bankovic*[412] and *Bosphorus* cases.[413] In parallel, the IACtHR affirmed that HR treaties are 'live instruments, whose interpretation must go hand in hand with evolving times and current living conditions', but underlined that 'evolutive interpretation is consistent with the general rules of interpretation set forth in Article 29 of the American Convention, as well those

---

[406] Ibid.

[407] *Nuclear Weapons in Armed Conflict* (n.397) [19].

[408] Ibid.

[409] Ibid.

[410] *Tyrer v UK* (1978) 2 EHRR 1, [31].

[411] *Golder* (n.31) [29].

[412] *Banković and ors v Belgium and ors* (2001) 44 EHRR SE5, [55]-[66].

[413] *Bosphorus Hava Yollari Turizm Ve Ticaret Anonim Sirketi v Ireland* (2005) 42 EHRR 1, [150].

set forth in the Vienna Convention on Treaty Law'.[414] It added that, 'when interpreting the Convention it is always necessary to choose the alternative that is most favourable to protection of the rights enshrined in said treaty, based on the principle of the rule most favourable to the human being'.[415] As to the ECJ, it seems to favour a teleological approach. In 1963, it referred 'to the objective of the EEC treaty',[416] and–in 1991–concluded that '[a]n international treaty is to be interpreted not only on the basis of its wording, but also in the light of its objectives'.[417]

c. Conclusion

The parties are not necessarily able to plan every situation the IO will have to face, and they thus benefit from implied powers. However, those powers must be subsidiary and necessary. Moreover, the ICJ continues to apply the VCLT rules of interpretation to constitutive treaties, even if some of their specificities have to be taken into account. Both the ECtHR and the IACtHR refer to the VCLT, and resort to an evolutionary interpretation because they feel it was the parties' intention. Only the ECJ seems to systematically favour teleological interpretation.

A careful investigation of case-law was necessary to reveal that interpretation of both 'ordinary' and 'constitutive' treaties has to be done in accordance with parties' intention, as reflected in the treaty's text. This process is reflected in the approach to sources.

---

414 *Case of the Mapiripán Massacre v Colombia* (Merits, Reparation and Costs) [2005] IACHR Series C No.134, [106].

415 Ibid.

416 *Van Gend en Loos v Nederlandse Administratie der Belastingen* (26/62) [1963] ECR 1, 12.

417 Opinion 1/91 (n.403) I-6101.

4.2. Approach to sources

According to article 38(1) (b) of the ICJ Statute, the Court 'shall apply […] International custom, as evidence of a general practice accepted as law'. This article is the starting point for the dominant theory of CIL, as enshrined by the ICJ and the ILC (A). However, this dominant theory also comes with limits (B). A conclusion is then put forward (C).

A. The dominant theory of the ICJ and the ILC

The elements of CIL formation have been highlighted by the ICJ, and recently codified by the ILC. It is first necessary to identify the constitutive elements of custom, i.e. practice and *opinio juris* (a). Then, their characteristics (b), and evidencing (c) must be assessed.

a. The 'two elements' doctrine

It is sometimes considered that 'the normative definition of custom and its basic constituent element are incorporated into Art. 38',[418] and it is now largely accepted that state practice and *opinio juris* are the two constitutive elements of custom.[419]

Those two elements appeared in the *North Sea Continental Shelf* case. '[A]n indispensable requirement would be that within the period in question, short though it might be, State practice, including that of States whose interests are specially affected, should have been both extensive and virtually uniform in the

[418] Gennadi Danilenko, *Law-Making in the International Community* (M.N.P. 1993) 80; See also David Bederman, *The Spirit of International Law* (UGA Press 2002) 33.

[419] David Bederman, 'Acquiescence, Objection and the Death of Customary International Law' (2010) 21 Duke J.Comp.&Int'l.L. 31, 44; Rudolf Bernhardt, 'Custom and Treaty in the Law of the Sea' (1987) 205 Recueil des Cours 247, 265-6; Alain Pellet and Patrick Daillier, *Droit International Public* (7th edn, L.G.D.J. 2002) 325-34; Gennadi Danilenko, *Law-Making in the International Community* (n.418) 81; Andrew Guzman, *How International Law Works: A Rational Choice Theory* (O.U.P. 2008) 184-5; Max Sorensen, 'Principes de Droit International Public' (1960) 101 Recueil des Cours 1, 36.

sense of the provision invoked; and should moreover have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved'.[420] It was then confirmed that '[n]ot only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it. The need for such a belief, i.e., the existence of a subjective element, is implicit in the very notion of the *opinio juris sive necessitatis'*.[421] Such an approach was strengthened by the *Nicaragua* case. The Court emphasized that 'for a new customary rule to be formed, not only must the acts concerned "amount to a settled practice", but they must be accompanied by the *opinio juris sive necessitatis'*.[422]

In his reports, Michael Wood concludes that, despite a potential 'difference in application of the two-element approach in different fields', 'the underlying approach is the same: both elements are required'.[423] The ILC subsequently concludes that '[t]wo constituent elements' are necessary: '[t]o determine the existence and content of a rule of customary international law, it is necessary to ascertain whether there is a general practice that is accepted as law (*opinio juris*)'.[424] In 'assessing' their 'evidence', 'regard must be had to the overall context, the nature of the rule, and the particular circumstances in which the evidence in question is to be found'.[425] The ILC then concludes that '[e]ach element is to be separately ascertained. This generally requires an assessment of specific evidence for each element'.[426] It is thus a verbatim copy of Wood's recommendations.[427]

---

[420] *North Sea Continental Shelf (Germany/Denmark; Germany/Netherlands)* (Judgment) [1969] ICJ Rep 3, [74].

[421] Ibid [77].

[422] *Nicaragua* (n.46) [207].

[423] Michael Wood, 'Second report on formation and evidence of customary international law' (2013) UN-Doc A/CN.4/672, 12.

[424] ILC, 'Chapter V–Identification of customary international law' (2016) UN-Doc A/71/10, 76.

[425] Ibid.

[426] Ibid.

[427] Michael Wood, 'Third report on identification of customary international law' (2015) UN-Doc A/CN.4/682, 9.

Once it is determined that both practice and *opinio juris* are the constitutive elements of custom, their characteristics have to be determined.

b. The characteristics of practice and *opinio juris*

According to the ICJ, practice must be 'uniform'[428] or 'attain the degree of generality which is constitutive of custom'.[429] However, '[f]or to become binding, a rule or principle of international law need not pass the test of universal acceptance'.[430] Wood's second report thus concludes that '[t]o establish a rule of customary international law, the relevant practice must be general, meaning that it must be sufficiently widespread and representative. The practice need not be universal'.[431] Then, the ICJ mentioned that practice must be 'constant'[432] or constituted by 'repeated and recurrent acts on the international level'.[433] Wood thus concludes that '[t]he practice must be generally consistent'.[434] The *North Sea Continental Shelf* case underlined that 'the passage of only a short period of time is not necessarily, or of itself, a bar to the formation of a new rule of customary international law'.[435] The case's individual opinions are also of interest. Judge Sorensen expressed doubt about the relevance of 'classic doctrine', according to which 'such practice must have been pursued over a certain length of time' or

---

[428] *Asylum case (Colombia/Peru)* (Judgment) [1950] ICJ Rep 26, 276; *Case concerning Right of Passage over Indian Territory (Portugal v India)* (Judgment) [1960] ICJ Rep 6, 40; *North Sea Continental Shelf* (n.420) [74].

[429] *SO Ammoun* in *Barcelona Traction, Light and Power Company, Limited (Belgium v Spain)* (Judgment) [1970] ICJ Rep 3, 307.

[430] *DO Lachs* in *North Sea Continental Shelf* (n.420) 229; See also *SO Ammoun* (n.429) 330.

[431] Wood, 'Second report' (n.423) 41.

[432] *Asylum case* (n.428) 276; *Right of Passage over Indian Territory* (n.428) 60.

[433] *DO Guggenheim* in *Nottebohm Case (second phase) (Liechtenstein v Guatemala)* (Judgment) [1955] ICJ Rep 4, 55.

[434] Wood, 'Second report' (n.423) 41.

[435] *North Sea Continental Shelf* (n.420) [44].

'those who have maintained the necessity of "immemorial usage"'.[436] He highlighted that 'the Court does not seem to have laid down strict requirements as to the duration of the usage or practice which may be accepted as law'.[437] Then, '[t]he possibility has […] been reserved of recognizing the rapid emergence of a new rule of customary law based on the recent practice of States'.[438] Judge Lachs was of the same opinion.[439] Wood subsequently concludes that '[p]rovided that the practice is sufficiently general and consistent, no particular duration is required'.[440]

These conclusions are *grosso modo* confirmed by the ILC. 'The relevant practice must be general, meaning that it must be sufficiently widespread and representative, as well as consistent', and '[p]rovided that the practice is general, no particular duration is required'.[441]

As taking into account the practice of states whose interests are specially affected was deemed necessary by the ICJ[442] and individual opinions,[443] Wood mentions that '[i]n assessing practice, due regard is to be given to the practice of States whose interests are specially affected'.[444] This requirement is only mentioned by the ILC in conclusion 8's comments.[445] The ILC also highlights that 'it is primarily the practice of States that contributes to the formation, or expression, of rules of customary international law', and, '[i]n certain cases, the practice of international organizations'.[446]

---

[436] *DO Sorensen* in *North Sea Continental Shelf* (n.420) 244.

[437] Ibid.

[438] Ibid.

[439] *DO Lachs* in *North Sea Continental Shelf* (n.420) 230.

[440] Wood, 'Second report' (n.423) 45.

[441] ILC, 'Chapter V' (n.424) 77.

[442] *North Sea Continental Shelf* (n.420) [74].

[443] *DO Tanaka* in *North Sea Continental Shelf* (n.420) 175-6; *SO De Castro* in *Fisheries Jurisdiction (UK v Iceland) (Judgment)* [1974] ICJ Rep 3, 90; *DO Petren* in *Fisheries Jurisdiction* (n.443) 161.

[444] Wood, 'Second report' (n.423) 38-40.

[445] ILC, 'Chapter V' (n.424) 95.

[446] Ibid 76.

According to the ICJ, '[t]he States concerned must […] feel that they are conforming to what amounts to a legal obligation. The frequency or even habitual character of the acts is not in itself enough'.[447] Moreover, *opinio juris* cannot be satisfied when a party to a treaty merely complies with its conventional obligations.[448]

The ILC draft conclusions slightly differ from Wood's report,[449] and mention that '[t]he requirement, as a constituent element of customary international law, that the general practice be accepted as law (*opinio juris*) means that the practice in question must be undertaken with a sense of legal right or obligation'.[450] Then, it 'is to be distinguished from mere usage or habit'.[451]

The characteristics of practice and *opinio juris* have been respectively ascertained. Likewise, their evidencing has to be determined.

c. The evidence of practice and *opinio juris*

The ILC affirms that '[s]tate practice consists of conduct of the state, whether in the exercise of its executive, legislative, judicial or other functions'.[452] 'Practice may take a wide range of forms', and it 'includes both physical and verbal acts' and 'may, under certain circumstances, include inaction'.[453] More specifically, '[f]orms of State practice include, but are not limited to: diplomatic acts and correspondence; conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference; conduct in connection with treaties; executive conduct, including operational conduct "on

[447] *North Sea Continental Shelf* (n.420) 77.

[448] Ibid [74]-[76].

[449] Wood, 'Second report' (n.423) 56.

[450] ILC, 'Chapter V' (n.424) 77.

[451] Ibid 77.

[452] Ibid 76.

[453] Ibid 77.

the ground"; legislative and administrative acts; and decisions of national courts'.[454] Finally, '[a]ccount is to be taken of all available practice of a particular State, which is to be assessed as a whole', and '[w]here the practice of a particular State varies, the weight to be given to that practice may be reduced'.[455]

Similarly, '[e]vidence of acceptance as law (*opinio juris*) may take a wide range of forms', which 'include, but are not limited to: public statements made on behalf of States; official publications; government legal opinions; diplomatic correspondence; decisions of national courts; treaty provisions; and conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference'.[456] Finally, '[f]ailure to react over time to a practice may serve as evidence of acceptance as law (*opinio juris*), provided that States were in a position to react and the circumstances called for some reaction'.[457] '[D]ocuments published in the name of a State, such as military manuals and official maps', and '[p]ublished opinions of government legal advisers' are considered as 'official publications'.[458]

The *Gulf of Maine* case highlighted that the 'presence' of 'a set of customary rules' in 'the *opinio juris* of States' had to 'be tested by induction based on the analysis of a sufficiently extensive and convincing practice, and not by deduction from preconceived ideas'.[459] According to Worster, '[d]eductive reasoning is often described as going from "the general to the specific" or "truth-preserving." In essence, a valid deductive argument is one in which the premises–if true–must lead to a true conclusion'.[460] On the contrary, induction 'is often described as

---

[454] Ibid.

[455] Ibid.

[456] Ibid.

[457] Ibid.

[458] Ibid 100.

[459] *Delimitation of the Maritime Boundary in the Gulf of Maine Area (Canada/USA)* (Judgment) [1984] ICJ Rep 246, [111].

[460] William Thomas Worster, 'The Inductive and Deductive Methods in Customary International Law Analysis: Traditional and Modern Approaches' (2014) 45(2) Geo.J.Int'l.L. 445, 447-8.

drawing inferences from specific observable phenomena to general rules, or "knowledge expanding." Here evidence is collected about observable events and a premise is constructed based on the collected data. The degree to which the conclusion is probably true is based on the quality of the evidence used to support it'.[461] Induction is similarly recommended by Wood.[462] However, the ILC draft conclusions suggest that '[t]he two-element approach does not in fact preclude a measure of deduction'.[463]

The ICJ and the ILC have set up a simple and appealing theoretical framework to ascertain the existence of a new customary rule. However, this dominant theory actually reveals some limits.

B. The limits of the dominant theory

Wood's reports and the ILC draft conclusions are inspired by ICJ landmark cases. However, the ICJ case-law is more ambiguous than the ILC reports. Such ambiguity is perceptible with respects to the 'two-element' doctrine (a), as well as with the evidence of practice and *opinio juris* (b).

a. The limits of the 'two elements' doctrine

Some aspects of the dominant theory have been criticized by doctrine. It is sometimes felt that 'the emphasis in proving custom is often on practice',[464] that lesser importance is given to *opinio juris* by the ICJ,[465] or even doubted that the two-element scheme actually explains the formative process of customary

[461] Ibid 448.

[462] Michael Wood, 'First report on formation and evidence of customary international law' (2013) UN-Doc A/CN.4/663, [96].

[463] ILC, 'Chapter V' (n.424) 84.

[464] Maarten Bos, 'The Identification of Custom in International Law' (1982) 25 German Y.B.I.L. 9, 31; Sorensen (n.419) 51.

[465] Peter Haggenmacher, 'La doctrine des deux éléments du droit coutumier international dans la pratique de la Cour internationale' (1986) 1 R.G.D.I.P. 6, 51-8.

norms.[466] The pre-eminence of article 38(1)(b) within the modern theory of CIL is sometimes challenged.[467] Another question is the degree of creativity of the judge,[468] and whether 'States must believe that something is already law before it can become law'.[469]

This last question and the necessity of *opinio juris* were echoed by Judge Lachs and Sorensen. According to the former, '[a]t all events, to postulate that all States, even those which initiate a given practice, believe themselves to be acting under a legal obligation is to resort to a fiction-and in fact to deny the possibility of developing such rules'.[470] Lachs also referred to 'the complexity of this formative process and the differing motivations possible at its various stages' to say that 'it is surely over-exacting to require proof that every State having applied a given rule did so because it was conscious of an obligation to do so'.[471] According to him, proving 'that the rule invoked is part of a general practice accepted as law by the States in question' should be the only requirement.[472] 'In sum, the general practice of States should be recognized as *prima facie* evidence that it is accepted as law'.[473] Judge Sorensen similarly considered that 'the question of the *opinio juris*' was 'a problem of legal doctrine which may cause great difficulties in international adjudication', and thought that 'there may be numerous cases in which it is practically impossible for one government to produce conclusive

---

466 Ibid 111.

467 Jean d'Aspremont, 'The Decay of Modern Customary International Law in Spite of Scholarly Heroism' (2015) G.C.Y.I.L.J. 9, 13; See also Karol Wolfke, *Custom in Present International Law* (Prace W.T.N. 1964) 21-58.

468 Sorensen (n.419) 35-6; Haggenmacher (n.465) 110-25.

469 Michael Akehurst, 'Custom as a Source of International Law' (1976) 47(1) British Y.B.I.L. 1, 32; See also Gennadi Danilenko, , 'The Theory of International Customary Law' (1988) 31 German Y.B.I.L. 9, 15; Anthony D'Amato, *The Concept of Custom in International Law* (Cornell University Press 1971) 67-8; Sorensen (n.419) 50; Hans Kelsen, *General Theory of Law and State* (H.U.P. 1945) 114-15; Josef Kunz, 'The Nature of Customary International Law' (1953) 47(4) A.J.I.L. 662, 667; Raphael Walden, 'The Subjective Element in the Formation of Customary International Law' (1977) 12 Is.L.R. 344, 359-63.

470 *DO Lachs* in *North Sea Continental Shelf* (n.420) 231.

471 Ibid.

472 Ibid.

473 Ibid.

evidence of the motives which have prompted the action and policy of other governments'.[474] As a consequence, 'the practice of States […] may be taken as sufficient evidence of the existence of any necessary *opinio juris*'.[475]

In practice, the ICJ regularly analyses practice and *opinio juris* together. Contrary to the requirements of the ILC draft conclusions, 'each element' is thus not systematically 'separately ascertained'.

In the *Jurisdictional Immunities* case, the Court defined what had to be considered part of state practice and part of *opinio juris*, linking national judgments to the former. Following a lengthy analysis of national courts' practice, the ICJ paradoxically ended up saying that 'practice is accompanied by *opinio juris*, as demonstrated by the positions taken by States and the jurisprudence of a number of national courts […]'.[476] In 1996, the ICJ underlined that 'the members of the international community are profoundly divided on the matter of whether non-recourse to nuclear weapons over the past 50 years constitutes the expression of an *opinio juris*'.[477] Relying on an identical corpus of 'international instruments', 'domestic law', and denunciations 'within national and international fora', the Court considered in 2012 that 'the prohibition of torture' was 'grounded in a widespread international practice and on the *opinio juris* of States'. [478] Judge Van den Wyngaert considered that '[a] "negative practice" of States, consisting in their abstaining from instituting criminal proceedings, cannot, in itself, be seen as evidence of an *opinio juris*'. [479] In 1985, the Court even exclusively relied on state practice: '[i]t is in the Court's view incontestable that […] the institution of the exclusive economic zone […] is shown by the practice of States to have become a part of customary law'.[480]

---

[474] *DO Sorensen* in *North Sea Continental Shelf* (n.420) 246-7.

[475] Ibid.

[476] *Jurisdictional Immunities of the State (Germany v Italy: Greece intervening)* (Judgment) [2012] ICJ Rep 99, [77].

[477] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, [67].

[478] *Questions relating to the Obligation to Prosecute or Extradite (Belgium v Senegal)* (Judgment) [2012] ICJ Rep 422, [99].

[479] *DO Van den Wyngaert* in *Arrest Warrant of 11 April 2000 (DRC v Belgium)* (Judgment) [2002] ICJ Rep 3, [13].

The separate ascertainment of practice and *opinio juris* is thus rarely strictly carried out by the ICJ. Yet, similar limit may be found with respect to the evidencing of practice and *opinio juris*.

b. The limits in evidencing the existence of practice and *opinio juris*

Such limits are perceptible on two aspects. First–and contrary to what the ICJ says it is doing–its methodology is not purely inductive (i). Second, the substance of ICJ's reasoning itself is of unequal rigour (ii).

i. The methodology of the ICJ is not purely inductive

The inductive or deductive nature of ICJ methodology has been discussed in doctrine.[481] D'Aspremont thinks that '[c]oncealing a deductive process behind an inductive smokescreen is probably the *raison d'être* of the theory of customary international law'.[482] According to Talmon, '[t]he main method employed by the Court is not induction or deduction but assertion'.[483] Indeed, '[i]n the large majority of cases, the court does not offer any (inductive or deductive) reasoning but simply asserts the law as it sees it'.[484] Talmon's article raised an important debate. Cohen thinks that 'the lack of clear methodology hints that the ICJ's choice of induction, deduction, or assertion has little to do with methodology and everything to do with justification'.[485] Indeed, '[w]hen the Court invokes

[480] *Continental Shelf (Libya/Malta)* (Judgment) [1985] ICJ Rep 13, [34].

[481] Robert Kolb, 'Selected problems in the theory of customary international law' (2003) 50(2) N.I.L.R. 119, 130-3; Worster (n.460) 503-21.

[482] Jean d'Aspremont, 'Customary International Law as a Dance Floor: Part II' (*EJIL:Talk!* , 15.04.2014) <www.ejiltalk.org/customary-international-law-as-a-dance-floor-part-ii/> accessed:09.02.2017.

[483] Stefan Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion' (2015) 26(2) E.J.I.L. 417, 434.

[484] Ibid.

[485] Harlan Cohen, 'Methodology and Misdirection: Custom and the ICJ' (*EJIL:Talk!*, 01.12.2015) <www.ejiltalk.org/methodology-and-misdirection-a-response-to-stefan-talmon-on-custom-and-the-icj/> accessed:19.08.2016.

each one, it is attempting to justify its authority to interpret or find rules of CIL'. [486] He considers 'the possibility that states prefer the flexibility of methodological uncertainty over tying the ICJ's hands'.[487] Lusa Bordin asserts that the inductive method tends to be applied by the ICJ to reject claims of CIL, but not 'to affirm new rules of custom', as it would expose its reasoning 'to criticism'.[488] This assertion 'allows the Court to clarify the law incrementally while keeping the level of institutional criticism at a chronic (but arguably manageable) level'.[489] According to Wood and Sender, it is in fact unclear whether 'the Court ever applies a truly "deductive" method', as 'abstract terms, such as "induction" and "deduction"' are not used 'to describe what it does'.[490] They think that 'assertion is self-evidently not a methodology for determining the existence of a rule of customary international law'.[491]

In the *North Sea Continental Shelf* case, the ICJ denied the customary nature of the equidistance principle after reviewing fifteen instances of continental shelf delimitation resorting to equidistance.[492] In the *Arrest Warrant* case, a customary exception to incumbent MFA's immunity of jurisdiction was denied after an allegedly careful exam of state practice, 'including national legislation and those few decisions of national higher courts', 'legal instruments creating international criminal tribunals' and decisions from the latter.[493] In her dissenting opinion, Judge Van den Wyngaert investigated the position of various NGO's,

---

[486] Ibid.

[487] Ibid.

[488] Fernando Lusa Bordin, 'Induction, Assertion and the Limits of the Existing Methodologies to Identify Customary International Law' (*EJIL:Talk!,* 02.12.2015) <www.ejiltalk.org/induction-assertion-and-the-limits-of-the-existing-methodologies-to-identify-customary-international-law/> accessed:19.08.2016.

[489] Ibid.

[490] Omri Sender and Michael Wood, 'The International Court of Justice and Customary International Law: A Reply to Stefan Talmon' (*EJIL:Talk!*, 30.11.2015) <www.ejiltalk.org/the-international-court-of-justice-and-customary-international-law-a-reply-to-stefan-talmon/> accessed:24.07.2017.

[491] Ibid.

[492] *North Sea Continental Shelf* (n.420) [79].

[493] *Arrest Warrant* (n.479) [58].

conventions, as well as decisions by domestic and regional courts.[494] These are indeed instances of inductive reasoning.

However, resort to deduction is not rare. 'Although there can be a continental shelf where there is no exclusive economic zone, there cannot be an exclusive economic zone without a corresponding continental shelf. It follows that, for juridical and practical reasons, the distance criterion must now apply to the continental shelf as well as to the exclusive economic zone'.[495] '[S]ince' article 6 of Geneva Continental Shelf Convention 'was not, as were Articles 1 to 3, excluded from the faculty of reservation, it is a legitimate inference that it was considered to have a different and less fundamental status and not, like those Articles, to reflect pre-existing or emergent customary law'.[496] Then, a principle from *Lotus* case was considered 'by analogy, applicable almost word for word, mutatis mutandis, to the present case'.[497] Deduction was similarly used in *Qatar v Bahrain,*[498] *Arrest Warrant*[499] and *Jurisdictional Immunities* cases.[500]

Contrary to what the ICJ says, its reasoning is not always inductive. This idea was well-synthetized by Geiger, as '[i]n general the Court does not follow its self-proclaimed method of finding customary international law'.[501] Moreover, its reasoning proves to be of unequal rigour, with a varying discipline in the ascertainment of practice and *opinio juris*.

---

494 Ibid [27]-[28].

495 *Continental Shelf* (n.420) [33]-[34].

496 *North Sea Continental Shelf* (n.420) [66].

497 Ibid [78].

498 *Maritime Delimitation and Territorial Questions between Qatar and Bahrain (Qatar v Bahrain)* (Judgment) [2001] ICJ Rep 40, [175]-[176].

499 *Arrest Warrant* (n.479) [53]-[4].

500 *Jurisdictional Immunities* (n.476) [95].

501 Rudolf Geiger, 'Customary International Law in the Jurisprudence of the International Court of Justice: A Critical Appraisal' in Ulrich Fastenrath and others (eds), *From Bilateralism to Community Interest: Essays in Honour of Bruno Simma* (O.U.P. 2011) 692.

ii. The substance of ICJ's reasoning is of unequal rigour

A debate exists about the constitutive elements of state practice: whether it includes statements[502] or not,[503] abstentions or not etc.[504] With respect to the former, the risk of 'double counting'–i.e., including verbal acts in both practice and *opinio juris*–has often been highlighted.[505] The quantity and consistency of practice required is sometimes at stake.[506] D'Aspremont mentions various 'stratagems and ploys which are being used to "discover" practice'.[507] According to him, '[t]he most common […] is to turn a declarative process into a constitutive one', which 'is the idea that what is said about a given behaviour is constitutive of that behaviour'.[508] Then, '[a]nother trick is to discover behavioural practice in interpretive practice. According to this approach, what is said about an existing rule feeds into the behavioural practice supporting the customary rule'.[509] He also rejects the fact 'that the practice of international organisations or that of non-state actors is said to be instrumental in the crystallisation of purely inter-state rules'.[510]

A trend in ICJ's case-law is to consider that a rule codified by an ILC project is part of CIL, without any personal investigation.[511] It goes the same way for some

---

[502] Akehurst (n.469) 1-3; Karl Zemanek, 'What is State Practice and Who Makes It?' in Ulrich Beyerlin and others (eds), *Recht zwischen Umbruch und Bewahrung* (Springer 1995) 292.

[503] D'Amato (n.469) 88.

[504] Akehurst (n.469) 10-11; Gennadi Danilenko, 'The Theory of International Customary Law' (n.469) 108; Maurice Mendelson, 'The formation of customary international law' (1998) 272 Recueil des Cours 197, 204-09.

[505] Jean d'Aspremont, 'The Decay of Modern Customary International Law' (n.467) 27.

[506] Akehurst (n.469) 12-30.

[507] Jean d'Aspremont, 'Customary International Law as a Dance Floor: Part II' (n.482).

[508] Ibid.

[509] Ibid.

[510] Ibid.

[511] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v Serbia)* (n.372) [61], [128]; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-and-Herzegovina v Serbia-and-Montenegro)* (Judgment) [2007] ICJ Rep 43, [385], [398], [401];

conventional rules.[512] In the *Nuclear Weapons* advisory opinion, the Court relied on a written statement by only one state–Nauru–to affirm that the principle of neutrality 'is presented as an established part of the customary international law'.[513]

However, giving no justification to validate or reject the qualification of customary rule is even more frequent. In the *Interhandel* case, '[t]he rule that local remedies must be exhausted before international proceedings may be instituted' had been 'generally observed' and was thus 'a well-established rule of customary international law'.[514] No precise instance of practice was mentioned.
In 2008, the Court called both VCDR articles 27[515] and 29[516] a 'rule of customary international law', but without any investigation in state practice and *opinio juris*. This laconism is even more perceptible when the customary nature of a principle is denied. For instance, the Court said that it was not 'aware of a uniform and widespread State practice which might have given rise to a customary rule' permitting or excluding 'appropriation of low-tide elevations'. [517] Similar reasoning was adopted in the *Jurisdictional Immunities* case.[518] In *Diallo* case, the Court 'having carefully examined State practice and decisions of international courts and tribunals in respect of diplomatic protection of *associés* and shareholders' denied 'an exception in customary international law allowing for protection by substitution […]'.[519] However, the quest for state practice was absent as only two cases–*Barcelona Traction* and *Elettronica Siccula*–were actually

Ahmadou Sadio Diallo (Guinea v DRC) (Preliminary Objections) [2007] ICJ Rep 582, [39]; *Difference Relating to Immunity* (n.80) [62]; *Jurisdictional Immunities* (n.476) [56].

[512] *Maritime Delimitation* (n.498) [185]; *Arrest Warrant* (n.479) [52]; *Armed Activities on the Territory of the Congo (New Application: 2002) (DRC v Rwanda)* (Admissibility) [2006] ICJ Rep 6, [46].

[513] *Nuclear Weapons* (n.477) [88].

[514] *Interhandel Case (Switzerland v USA)* (Preliminary Objections) [1959] ICJ Rep 6, 27.

[515] *Certain Questions of Mutual Assistance in Criminal Matters (Djibouti v France)* (Judgment) [2008] ICJ Rep 177, [124].

[516] Ibid [238].

[517] *Maritime Delimitation* (n.498) [205].

[518] *Jurisdictional Immunities* (n.476) [101].

[519] *Diallo* (n.511) [89].

investigated. As mentioned previously, the ILC seems to be aware of this, suggesting that '[t]he two-element approach does not in fact preclude a measure of deduction […]'.[520]

C. Conclusion

This thesis does not seek to renovate the theory of CIL. Admittedly, the ICJ regularly deviates from the theoretical framework it itself propagated, and this reality is not necessarily taken into account by Wood's reports. However, both have the merit of offering clear guidelines. They are moreover approved by a majority of authors, including those who have an interest in cyber-espionage.[521] Wood's works and the ILC draft conclusions are thus this thesis' framework of reference in the quest for new customary rules specific to cyber-spying.

Another notion, regularly used in this thesis, needs to be defined in this conceptual framework: state practice.

4.3. Approach to state practice

This thesis adopts a *source-based* (A) and a *state-centric* approach (B), with a central notion in need of an explanation: *state practice* (C). These choices are explained below.

A. Source-based approach

This thesis resorts to a source-based approach. The 'source thesis refers to the idea that law is identified by its pedigree, itself defined in formal terms, and that, as a result, identifying the law boils down to a formal pedigree test'.[522] It resorts

---

[520] ILC, 'Chapter V' (n.424) 82.

[521] See part III.

[522] Jean d'Aspremont, *Formalism and the Sources of International Law* (O.U.P. 2011) 148.

to 'formal yardsticks to distinguish law from non-law'.[523] This approach is usually favoured by positivists. This doctrine aims at claiming 'fidelity to the law "as it is" rather than as it should be'.[524] According to positivists, '[w]hat counts as law-creating act in any given legal system depends on the practice of its legal officials,[525] while '[g]enuine international law […] can consist of nothing more than those positive rules to which States have explicitly (in the case of treaties) or implicitly (in the case of custom) agreed to abide'.[526] Yet, many authors propose to depart from its 'traditional' form. For instance, Christakis underlines that '[…] the *Lotus* dictum must be read correctly today. It should not be considered as implying the "absolute power" of the will of state or the idea that they are the only subjects of international law. Instead, the *Lotus* dictum should be read in a negative way: states should not be bound *against* their will, by what they have not *explicitly* or *implicitly* consented to'.[527]

Some words should be added regarding the goal of treaty interpretation. The view of 'classical positivist[s]' is well described by Hernández: '[t]he very character of interpretation cannot simply be assumed to have an objective character […] The narrative of classical positivist theorizing on interpretation […] presumes the objectivity of the interpretative process, a process that aims purely to clarify, to develop a method to fill any ambiguities in the fabric of the legal system with the one correct response, based on reason'.[528] D'Aspremont similarly acknowledges that 'it is a truism that none of the traditional methods of interpretation, whether textualism, intentionalism, or purposivism can mechanically produce one single stable meaning. In this sense, there seems to be a wide agreement that meaning is constructed and not extracted through

---

[523] Ibid.

[524] Jean d'Aspremont and Jörg Kammerhofer, 'Introduction' in Jean d'Aspremont and Jörg Kammerhofer (eds), *International Legal Positivism in a Post-Modern World* (C.U.P. 2014) 5.

[525] David Lefkowitz, 'Sources in Legal-Positivist Theories' in Besson, d'Aspremont and Knuchel (n.332) 340.

[526] Ibid 327.

[527] Théodore Christakis, 'Human Rights from a Neo-Voluntarist Perspective' in d'Aspremont and Kammerhofer (n.524) 423.

[528] Gleider Hernández, 'Interpretation' in d'Aspremont and Kammerhofer (n.524) 319.

interpretation'.[529] This thesis postulates that interpretation should theoretically *tend* to objectivity, but acknowledges that, in practice, it can certainly not give birth to 'one true meaning', and that throwing 'all the various elements […] into the crucible' will not give '*the* relevant interpretation',[530] but *a* relevant interpretation–one that is 'acceptable'.[531] This thesis maintains that revealing parties' intention remains the goal of treaty interpretation, and that it is through a textual interpretation that this task has to be completed, in accordance with the VCLT rules. In doing so, it confirms that, 'if intent is to be the goal of interpretation, it cannot be used as a means for attaining it',[532] and resorts to a method that is usually used by 'those who believe meaning is "found" in the interpreted object–the treaty itself'.[533]

Two remarks should nevertheless be added. First, to develop a theory of positivism, and to adjudicate between the various forms of positivism,[534] is outside the scope of this thesis. Second–and to answer Bianchi's concerns, according to whom 'traditional approaches […] shape legal materials and give them form according to some pre-existing models of legal rationality, rarely acknowledged and sometimes taken for granted'[535]–this research is aware that other theories exist, and does not seek adjudicating between them. As underlined by d'Aspremont, 'law's indeterminacy inevitably condemns (international) lawyers to making choice'.[536]

---

[529] D'Aspremont, 'The Multidimensional Process of Interpretation' in Bianchi, Peat and Windsor (n.333) 114.

[530] (1996) 2 Y.B.I.L.C, 219-20.

[531] Ingo Venzke, 'Post-Modern Perspectives on Orthodox Positivism' in d'Aspremont and Kammerhofer (n.524) 209.

[532] Martti Koskenniemi, *From Apology to Utopia* (C.U.P. 2005) 336.

[533] Duncan Hollis, 'Sources in Interpretation Theories: An Interdependent Relationship' in Besson, d'Aspremont and Knuchel (n.332) 425.

[534] Herbert Hart, *The Concept of Law* (2nd edn, O.U.P. 1994); Hans Kelsen, *General Theory of Law and State* (HUP 1945); Joseph Raz, *The Morality of Freedom* (O.U.P. 1986).

[535] Andrea Bianchi, *International Law Theories: An Inquiry Into Different Ways of Thinking* (O.U.P. 2016) 30.

[536] Jean d'Aspremont, 'Herbert Hart in Todays' International Legal Scholarship' in d'Aspremont and Kammerhofer (n.524) 135.

As a central role is given to states in this thesis, its state-centrism should now be explained.

B. State-centrism

This thesis is *state-centric*, as '[t]here is no doubt that, whatever the influence of these non-state actors may be, states and international organizations remain the exclusive international law-makers. This is true for treaty law and, subject to limited exceptions, customary international law'.[537] Thus, and while 'it is beyond doubt that over the two last decades non-state actors have been expending their say in international law-making processes',[538] 'their influence in the institution of the proceedings stands apart from the question of whether they can actually make law'.[539] To the extent that states have the power to make authoritative interpretation, their practice is thus central to the thesis. Actually, and 'while the role of non-state actors has swollen, we simultaneously witness that states have reinforced their grip over law-making processes'.[540] Yet, this thesis gives much weight to the draft conclusions of the ILC, which is 'probably also instrumental in the consolidation of a practice of law-ascertainment',[541] and offers 'quasi-authoritative textual formulations' of 'customary norms'.[542]

In connection with this state-centrism, much importance is given to the practice of these states.

---

[537] Jean d'Aspremont, 'Non-state actors from the perspective of legal positivism' in Jean d'Aspremont (ed), *Participants in the International Legal System* (Routledge 2013) 25.

[538] Jean d'Aspremont, 'The Heterogeneity of International Law-Making processes' in Helene Ruiz-Fabri and others (eds), *Select Proceedings of the European Society of International Law* (Bloomsbury 2010) 298.

[539] Ibid 303.

[540] Ibid.

[541] Jean d'Aspremont, 'Non-state actors from the perspective of legal positivism' in d'Aspremont (n.537) 30.

[542] Venzke, 'Post-Modern Perspectives on Orthodox Positivism' in d'Aspremont and Kammerhofer (n.524) 185.

C. State practice

This thesis considers that international law is mainly produced by states,[543] and that it is essentially through reference to states' willingness that its status will be ascertained at best. Much weight is thus given to state practice, which is placed at the centre of this thesis' reasoning.

What is meant by 'state practice' in the ascertainment of CIL has been made quite clear by the ILC draft conclusions, and explained previously.

Yet, 'subsequent practice' also plays a role in treaty interpretation.[544] Again, the ILC draft conclusions are enlightening on this aspect. They expressly mention that '[s]ubsequent agreements and subsequent practice under article 31, paragraph 3 (a) and (b), being objective evidence of the understanding of the parties as to the meaning of the treaty, are authentic means of interpretation, in the application of the general rule of treaty interpretation reflected in article 31'.[545]

It is underlined that '[a] "subsequent practice" as an authentic means of interpretation under article 31, paragraph 3 (b) consists of conduct in the application of a treaty, after its conclusion, which establishes the agreement of the parties regarding the interpretation of the treaty'.[546]

The ILC also mentions that '[o]ther "subsequent practice" as a supplementary means of interpretation under article 32 consists of conduct by one or more parties in the application of the treaty, after its conclusion'.[547] It is underlined that '[s]ubsequent practice under articles 31 and 32 may consist of any conduct

---

[543] Jean Combacau and Serge Sur, *Droit International Public* (11th edn, L.G.D.J. 2014) 15.

[544] VCLT, art.31(3)(b).

[545] ILC, 'Subsequent agreements and subsequent practice in relation to the interpretation of treaties' (2016) UN-Doc A/71/10, 120

[546] ILC, 'Subsequent agreements and subsequent practice in relation to the interpretation of treaties' (2013) UN-Doc A/68/10, 12.

[547] Ibid.

in the application of a treaty which is attributable to a party to the treaty under international law'.[548]

The method used in this thesis is inspired by the draft conclusions, and incorporates government (including the secret services and cyber-security centres) and parliamentary practice, as reflected in publications, communications, yearbooks, press releases and newspapers. It also includes some judicial cases. Such diversity of materials is not contradictory with the ILC's position, which acknowledges that subsequent practice 'need not meet any particular formal criteria',[549] and that '[t]he number of parties that must actively engage in subsequent practice in order to establish an agreement under article 31, paragraph 3 (b), may vary'.[550] Moreover, [s]ubsequent practice of States in the application of a treaty may certainly be performed by the high-ranking government officials mentioned in article 7 of the 1969 Vienna Convention'.[551] Yet, 'since most treaties typically are not applied by such high officials, international courts and tribunals have recognized that the conduct of lower authorities may also, under certain conditions, constitute relevant subsequent practice in the application of a treaty […] It thus appears that the practice of lower and local officials may be subsequent practice "in the application of a treaty" if this practice is sufficiently unequivocal and if the Government can be expected to be aware of this practice and has not contradicted it within a reasonable time'.[552] Then, '[d]epending on the treaty concerned', the relevant practice 'includes not only externally oriented conduct, such as official acts, statements and voting at the international level, but also internal legislative, executive and judicial acts, and may even include conduct by non-State actors that is attributable to one or more States parties'.[553]

This thesis actually postulates that an accumulation of empirical materials helps revealing the individual position of a state over the regulation of cyber-espionage

---

[548] Ibid.

[549] ILC, 'Subsequent agreements' (2016) (n.545) 164.

[550] Ibid 122.

[551] Ibid 150.

[552] Ibid 150-1.

[553] Ibid 164.

by certain instruments. Whether an agreement–or at least, a *common understanding*–exists or not between parties is then drawn from these patterns of state practice. This method is actually echoed by the ILC, as 'the difference' between 'subsequent agreement' and 'subsequent practice' is that the former 'has the effect of constituting an authentic means of interpretation of the treaty', whereas the latter 'only has this effect if its different elements, taken together, show "the common understanding of the parties as to the meaning of the terms"'.[554] Thus, '[s]ubsequent agreements and subsequent practice under article 31(3) are distinguished based on whether an agreement of the parties can be identified as such, in a common act, or whether it is necessary to identify an agreement through individual acts which in their combination demonstrate a common position'.[555] While state practice is a vital element in this thesis' process of treaty interpretation, a possible caveat exists as to whether the materials used are part of the 'general rule' or the 'supplementary means'. The ILC indeed mentions that 'subsequent practice in the application of the treaty, which does not establish the agreement of all parties to the treaty, but only of one or more parties, may be used as a supplementary means of interpretation'.[556] It is also worth mentioning that '[s]ubsequent agreements and subsequent practice may also contribute to a clarification of the object and purpose of a treaty'.[557]

It thus appears that 'practice' does not have the same meaning within treaty interpretation and the ascertainment of customary rules. This thesis thus adopts a larger vision of state practice in the former exercise than in the latter. For instance, the types of materials used to assess *opinio juris* (public statements, official publications etc.) have been incorporated into 'practice' when it comes to analyse treaties, territorial sovereignty and non-intervention.

---

[554] Ibid 140.

[555] Ibid.

[556] Ibid 129.

[557] Ibid 167.

As underlined by Gardiner, it is 'if the conduct is sufficiently constant and repeated' that it 'amount[s] to practice'.[558] This thesis similarly recommends that consistency and repetition should be taken into account. On some aspects, this research found abundant documentation, and was able to determine the position of the *majority,* identified among the *expressed opinions*. Sometimes, a position was even reiterated in later publications. On others, however, practice was scarce and the research focused on the lack of *express contradictory* positions. Disagreements and ambiguities were systematically underlined.

Some remarks should also be added, regarding possible contradictions within a specific state. First, the expression of a 'collective' feeling should take precedence over an 'individual' one (for instance, a government over a minister). Then, this thesis echoes a remark by Venzke, who thinks that '[t]he state falls into distinct parts, each acting autonomously, often contravening the action of the executive to which international legal positivism has traditionally granted prime place'.[559] In some instances, this research found that the parliament and the government of a specific state had divergent views over cyberspace regulation, rendering guidelines on the assessment of organs' contradictory positions necessary.

A material constraint should also be underlined: while most of the collected state practice is recent (2013-2018)–and privileged by this thesis–some materials may be older. This may be of importance, as technology quickly evolves. This older practice has however been handled with care, contrasted with most recent data or quoted in last resort–when no any or only some states had adopted a position on a specific question.

Another unanswered question is the weight of practice outside treaty interpretation and the ascertainment of customary rules. For instance, state practice remains vital for this thesis when it comes to analysing territorial sovereignty and non-intervention. Lacking a clear methodology, this thesis duplicates the method used to evaluate 'subsequent practice' in the framework of treaty interpretation. Its (large) vision could be synthetized as follows: '[a]ny action, abstention, statement, writing or behaviour of a state's organ or one of

---

[558] James Gardiner, *Treaty Interpretation* (2nd edn, O.U.P. 2008) 260.

[559] Venzke, 'Post-Modern Perspectives on Orthodox Positivism' in d'Aspremont and Kammerhofer (n.524) 197.

its members, attributable to this state, and prone to reveal the position of this state regarding the application of a given legal rule, regardless of the material in which it is expressed'.

FIRST PART – THE RULES CONNECTED TO TERRITORIAL INTEGRITY

I – TERRITORIAL SOVEREIGNTY

One of the rules stemming from the principle of sovereignty is the prohibition on non-consensual, foreign territorial intrusions–even when no use of force or coercive intervention is involved. Their qualification as violations of sovereignty and international law have been regularly underlined–and reparations, required. For instance, the removal of mines by the British Navy in Albanian waters,[560] the abduction of Eichmann by Mossad in Argentina,[561] excavations and military presence by Nicaragua on the territory of Costa Rica,[562] the (accidental) trespass of a Soviet satellite on Canadian territory were all considered violations of sovereignty.[563] An intrusion–in the computer systems of another state–is similarly required by cyber-espionage. This led many scholars to find that cyber-espionage violate sovereignty. Yet, the relevance of territorial sovereignty to cyber-espionage may be questioned, as this intrusion is not physical. Status of doctrine (1) and status of law (2) are thus alternatively ascertained. A conclusive note ends this chapter (3).

1. Status of doctrine

A panorama of the doctrinal works on espionage (1.1), interception of telecommunications (1.2) and cyber-espionage (1.3) is set up.

---

560 *Corfu Channel Case* (n.78) 35.

561 UNSC Res 138 (23.06.1960) [Question relating to the case of Adolf Eichmann].

562 *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica)* (Judgment) [2015] ICJ Rep 665, [93].

563 'Settlement of Claim between Canada and the USSR for Damage Caused by "Cosmos 954"' (02.04.1981) <www.spacelaw.olemiss.edu/library/space/International_Agreements/Bilateral/1981%20Canada-%20USSR%20Cosmos%20954.pdf> accessed:24.10.2018.

1.1. Espionage

Many authors, such as Kish,[564] Kraska,[565] and Chesterman,[566] affirm that espionage is at odds with the principle of territorial sovereignty. Cohen-Jonathan and Kovar consider that 'it is possible to deem espionage as a breach of international law, to the extent that it merges with a violation of the obligation to respect other States' sovereignty'.[567] Wright thinks that both reconnaissance flights and the sending of an agent in peacetime are 'illegitimate enterprises because they manifest a lack of respect for foreign territory'.[568]

However, a theory supported by numerous scholars is that espionage is not illegal *per se*, contrary to its collateral breach of territory. Stone argues that espionage without territorial intrusion is not an international delinquency.[569] Lafouasse distinguishes espionage (unfriendly) and a territorial breach (illegal).[570]

As the prohibition of unauthorized entry into a foreign territory extends to the territorial sea, Chesterman[571] and Williams[572] refer to the *Lotus* case and affirm that intelligence collection is an offence. Along with Kish[573] and Lafouasse,[574]

---

564 Kish and Turns (n.66) 88.

565 James Kraska, 'Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters' (2015) 54 Col.J.T.L. 164, 181.

566 Simon Chesterman, 'The spy who came in from the cold war: intelligence and international law' (2006) 27 Mich.J.Intl.L. 1071, 1082.

567 Gérard Cohen-Jonathan and Robert Kovar, 'L'espionnage en temps de paix' (1960) 6 A.F.D.I. 239, 254.

568 Quincy Wright, 'Legal Aspects of the U-2 Incident' (1960) 54 A.J.I.L. 836, 849.

569 Julius Stone, 'Legal Problems of Espionage in Conditions of Modern Conflict', in Roland Stanger (ed), *Essays on Espionage and International Law* (O.S.U. Press 1962) 34.

570 Lafouasse, *L'Espionnage* (n.66) 236.

571 Chesterman (n.566) 1082-3.

572 Robert Williams, '(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action' (2011) 79(4) Geo.J.Int'l.L. 1162, 1176.

573 Kish and Turns (n.66) 96.

574 Fabien Lafouasse, "L'Espionnage en Droit international' (2001) 47 A.F.D.I. 63, 123-4.

they rely on article 19(2) (c) of the UNCLOS to support the prohibition of intelligence collection in the territorial sea. This provision considers as 'prejudicial to the peace, good order or security of the coastal State [...] any act aimed at collecting information to the prejudice of the defence or security of the coastal State'.[575] Barzon highlights that 'the right of innocent passage' is maintained 'even in case of economic espionage, as long as no prejudice is caused to the particular State interests expressly listed'.[576]

But whether a general prohibition of espionage stems from this provision is uncertain. As Kraska argues, there is a 'debate' about 'the scope of innocent passage and the lawfulness of "non-innocent" passage in the territorial sea'.[577] He personally thinks that espionage activities 'may not qualify as violations of the international law of the sea, or even as inconsistent actions with international law more generally'.[578] According to Lafouasse, the coastal state can only protest against the violation of its territorial sovereignty, which is caused by the non-respect of innocent passage rules. This prohibition would be specific to the law of the sea, without subsequent extension to other environments,[579] or a general prohibition of espionage.[580] McDougal, Lasswell and Reisman have the same opinion, as '[a] number of states maintain fleets of intelligence ships, and it is noteworthy that protests and action against them have sought justification in claims of penetration of the territorial sea or allegations of self-defense, but not in terms of the generic unlawfulness of intelligence activities on the high seas'.[581] Barzon considers that 'espionage still can't be considered a forbidden activity *per se*'.[582]

---

575 UNCLOS, art.19(2)(c).

576 Andrea Barzon, 'An Issue for all Seasons: Peacetime Espionage and International Law' (2018) 10
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3169247> accessed:24.05.2018.

577 Kraska (n.565) 213.

578 Ibid 226.

579 Lafouasse, 'L'Espionnage' (n.574) 124.

580 Lafouasse, *L'Espionnage* (n.66) 281.

581 Myres McDougal, Harold Lasswell, Michael Reisman, 'The Intelligence Function and World Public Order' (1973) 46(3) Temple L.Q. 365, 393.

582 Barzon (n.576) 11.

1.2. Interception of telecommunications

Peters affirms that 'extracting intra-governmental exchange of information seems to interfere with state sovereignty in its most traditional sense'.[583]

1.3. Cyber-espionage

To justify their resort to sovereignty on cyberspace issues, many authors affirm that the Internet require physical infrastructures to function, the latter being built on the territory of a sovereign state.[584]

As 'the simple act of entering an area under territorial sovereignty without previous permission suffices to be a violation' of sovereignty, Delerue suggests that '[t]his conclusion can be extended to cyber-operations'.[585] 'If a cyber-operation penetrates the cyber infrastructures in the territorial sovereignty of a foreign State, this would irrefutably constitute a violation of territorial sovereignty'.[586] This analogy is also used by Shoshan.[587] Antolin-Jenkins thinks that 'entry into computer systems to observe and obtain information [...] may constitute a violation of territorial integrity'.[588] According to Buchan, 'espionage committed in cyberspace does not result in the transgression of the territory of

---

583 Anne Peters, 'Surveillance Without Borders–The Unlawfulness of the NSA-Panopticon' (*EJIL:Talk!*, 04.11.2013) <www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/> accessed:24.03.2015.

584 Thomas Wingfield, *The Law of Information Conflict–National Security Law in Cyberspace* (Aegis Research Corps 2000) 17; Heintschel Von Heinegg (n.159) 128; François Delerue, 'State-sponsored Cyber Operations and International Law' (PhD Thesis, EUI, 2016) 145.

585 Delerue (n.584) 145.

586 Ibid.

587 Ella Shoshan, 'Applicability of International Law on Cyber Espionage Intrusions' (Master thesis, Stockholm University, 2014) 37-8.

588 Vida Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?' (2005) 51 Naval L.Rev. 132, 161.

a State. This is because, to date, States have failed to subject cyberspace to territorial claims in the sense of dividing this domain into territorial units […] States do not possess territory in cyberspace'.[589] Yet, states do 'exert sovereignty in cyberspace, notwithstanding the fact that it is a non-physical domain that transcends territorial borders [...] Thus, the accessing and copying of confidential information located in cyberspace, and which belongs to entities that fall under the sovereignty of a State (whether this is public authorities, private companies, individuals, etc.), is regarded by States as a violation of their sovereignty'. [590] Parajon-Skinner postulates that, '[t]hough the Westphalian version of sovereignty has historically been linked to territorial control, the conceptual underpinnings of sovereignty are not necessarily limited to land or physical spaces. Instead, sovereignty is a principle that is mainly concerned with protecting national power bases and a state's exclusive right to control them'.[591] She continues her reasoning as follows: '[t]oday, a state's ability to safeguard its sovereignty–the essential aspects of its statehood–depends not only on control of its borders, but also on control of its economy and private sources of wealth [...] It follows then that sovereignty also proscribes external attempts to manipulate or infringe on a state's national economic spaces (as defined to include the private sector), including those launched in cyberspace, even if such acts fall below a conventional threshold of force'.[592] Schneier insists on the difference with bugging: '[e]avesdropping isn't passive anymore. It's not the electronic equivalent of sitting close to someone and overhearing a conversation. It's not passively monitoring a communications circuit. It's more likely to involve actively breaking into an adversary's computer network [...] and installing malicious software designed to take over that network [...] it's hacking. Cyber-

---

589 Russell Buchan, 'Cyber espionage and international law' in Russell Buchan and Nicholas Tsagourias (eds), *Research Handbook on international law and cyberspace* (E.E. 2015) 181-2.

590 Ibid 177.

591 Christine Parajon-Skinner, 'An International Law Response to Economic Cyber Espionage' (2014) 46(4) Conn.L.R. 1105, 1179.

592 Ibid.

espionage is a form of cyber-attack. It's an offensive action. It violates the sovereignty of another country [...]'.[593]

At the opposite, Beard thinks that '[a]cts involving unauthorized access to computer systems and networks are also particularly difficult to reconcile with state sovereignty over territory'. [594] Indeed, '[a] nonphysical information "incursion" into an adversary's computer systems or networks is not equivalent to the invasion of another state's territory'.[595] According to Goldsmith, this is just another form of (legal) espionage: '[s]o once again, we see technological innovation making it easier and easier for one nation to gather information in another nation without physically crossing borders. Norms of "territorial sovereignty" have never precluded such offshore espionage [...]'. [596] While 'decried', these activities 'have always been practiced, and are consistent with norms of territorial sovereignty and the limitations on enforcement jurisdiction'.[597] According to Sharp, 'espionage conducted by the non-consensual penetration of another state's computer systems is lawful under existing international law'.[598]

Lafouasse wonders whether 'rules of international law' do 'apply to cyber-espionage'. [599] He considers that 'the legal standing of cyber-espionage is intimately linked to cyberspace's one'.[600] If cyberspace is 'a common space',

---

[593] Bruce Schneier, 'When Does Cyber Spying Become a Cyber Attack?' (*DefenseOne*, 10.03.2014) <www.defenseone.com/technology/2014/03/when-does-cyber-spying-become-cyber-attack/80206/> accessed:14.04.2017.

[594] Jack Beard, 'Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law' (2014) 47 Vanderbilt J.Transnatl.L. 67, 96.

[595] Ibid.

[596] Jack Goldsmith, 'The Internet and the Legitimacy of Remote Cross-Border Searches' (2011) 16 Chicago–Public Law and Legal Theory Working Paper, 11 <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://www.google.fr/&httpsredir=1&article=1316&context=public_law_and_legal_theory> accessed:17.07.2015.

[597] Ibid.

[598] Walter Gary Sharp, *CyberSpace and the Use of Force* (Aegis Research Corporation 1999) 129.

[599] Lafouasse, *L'Espionnage* (n.66) 170-1.

[600] Ibid.

'spying does not come with a violation of national sovereignty and international responsibility'.[601] At the opposite, if 'cyberspace is partially or totally linked to national territory–data circulating on cyberspace are, for a while, on a territory under national sovereignty–spying could violate territorial integrity'.[602] Similarly, Shackelford thinks that '[t]wo options exist': 'the international community could agree that cyberspace is an arena over which nations can and should exercise sovereignty through the effects doctrine' or 'treat cyberspace as an information commons over which no state may claim jurisdiction'.[603] Barzon says that '[t]he fact of gaining access to a cyber-infrastructure, then, could be considered to be an unlawful violation of another's territory only when amounting to a material access (for example in the tangible servers and devices), but one may still wonder whether an intrusion via an intangible malware through the intangible cyberspace could still amount to a sovereignty breach'.[604]

In Tallinn Manual 2.0, Rule 4 mentions that '[a] State must not conduct cyber operations that violate the sovereignty of another State'.[605] However, the rule's comments only consider the situation where cyber-espionage 'by one state' is 'conducted while physically present on the territory of another State': '[f]or example, if organs of one State are present in another State's territory and conduct cyber espionage against it without its consent or other legal justification, the latter's sovereignty has been violated'.[606] The situation envisaged here still requires the sending of an agent abroad. The situation of remote cyber-espionage is actually considered in Rule 32: '[a]lthough peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so'.[607] Consequently, cyber-espionage operations

---

[601] Ibid.

[602] Ibid 19.

[603] Scott Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27 Berk.J.Int'l.L. 192, 211.

[604] Barzon (n.576) 8.

[605] Schmitt, *Tallinn Manual 2.0* (n.53) 17.

[606] Ibid 19.

[607] Ibid 168.

carried out 'in a manner that results in a loss of functionality'[608] or causing damage–even if 'unintended'[609]–allegedly qualify as violations of sovereignty.

Sovereignty is regularly invoked by doctrine with respect to espionage, interception of telecommunications and cyber-espionage. However, it is necessary to determine whether such enthusiasm is shared by states.

2. Status of law

The relation between sovereignty and espionage (2.1), interceptions of telecommunications (2.2), and cyber-espionage (2.3) is analysed.

2.1. Espionage and sovereignty

When acts of espionage are discovered, the same play usually occurs. Espionage victims denounce a breach of sovereignty (A), while authors invoke the necessary protection of national security (B), and a wide variety of concrete consequences occur subsequently (C).

A. The victims of espionage denounce a breach of sovereignty

Land, coastal and aerial espionage cases have traditionally been apprehended through the prism of territorial sovereignty by states.
In the context of land spying, New Zealand denounced 'a breach of New Zealand sovereignty and international law' following the arrest of two Mossad agents on its territory.[610] The same happened for Switzerland.[611]

---

608 Ibid 170.

609 Ibid 173.

610 (2004) 50(7) Keesings, 46124.

611 Tracy Wilkinson, 'Israel Refuses Apology to Swiss in Spy Scandal', *Los Angeles Times* (27.02.1998)
<http://articles.latimes.com/1998/feb/27/news/mn-23642> accessed:23.04.2016.

In the context of aerial spying, the Soviet Union (USSR) referred to the principle during the U-2 crisis.[612] In parallel, Poland remarkably highlighted that 'international law has never concerned itself with peacetime espionage'.[613] The USSR then regularly invoked such violations of sovereignty before the UN in the 60s.[614] China also blamed the 'aggressive crime' and served '213 warnings on U.S. action in sending its military aeroplanes and warships to violate China's airspace and territorial waters'.[615] Following the strike of a Bulgarian airplane, Italy also denounced such intrusions.[616] Cuba criticized the violation of its airspace by an American reconnaissance aircraft.[617]

In the context of coastal spying, a blanket prohibition of spying is not supported by state practice. The entry of the Soviet submarine *Whiskey* into Swedish waters was called a 'flagrant violation of territorial rights' even if 'illegal reconnaissance' was also pointed out.[618] When a foreign submarine was detected in Argentinean waters in 1958, Admiral Rojas pointed out that 'it was on Argentine territorial waters', 'openly in violation of international law', and called it an 'unfriendly act'.[619] Espionage *per se* was not particularly considered. This is also the usual American official position. The legal adviser of the Department of State, William Taft, stated that the UNCLOS 'does not prohibit or regulate intelligence activities'.[620] In 1960, the Soviet dragger *Vega* was 'photographed' with electronic intelligence devices,[621] while an American ship 'was on missile-firing manoeuvres

---

[612] (1960) 6(5) Keesings, 17437.

[613] UNSC, 858th Meeting (24.05.1960) [83].

[614] Joseph Soraghan, 'Reconnaissance Satellites: Legal Characterization and Possible Utilizations for Peacekeeping' (1967) 13(3) McG.L.J. 458, 470-1. He himself quotes Cooper, 'Current Developments in Space Law' (1963) 4 Spaceflight 136.

[615] (1962) 8(12) Keesings, 18951.

[616] (1962) 8(2) Keesings, 18584.

[617] (1984) 30(12) Keesings, 33086.

[618] (1982) 28(5) Keesings, 31512.

[619] 'Admiral sees Unfriendly Act', *NYT* (23.05.1958) 13.

[620] Committee on Foreign Relations of the Senate, 'Convention on the Law of the Sea' (2007) Exec Rept 110-9, 36 <www.congress.gov/110/crpt/erpt9/CRPT-110erpt9.pdf> accessed:29.12.2015.

[621] (1967) 9(3) JAG L.Rev., 22.

south of Long Island'.[622] The protest note subsequently sent by the USA just mentioned that controlling ships was needed.[623] Following the capture of the US Navy ship *Pueblo* by North Korea, tensions arose more on facts (presence of the ships in the territorial or international waters) than on law.[624]

In the *Corfu Channel* case, Albania exposed the commission of 'acts of spying contrary to the Law and prejudicial to the security of Albanian State',[625] and affirmed that '[i]t is impossible for the Court to admit that such practices are in compliance with the right to innocent passage'.[626] Reasoning in terms of (non) innocent passage has since been adopted by the UNCLOS. Sanctions are not really introduced, and a distinction is done between merchant and government ships operated for commercial purposes,[627] and warships.[628] Should a non-innocent passage occur, criminal jurisdiction can be exercised by the coastal state against the first ones, but the second ones may only be required 'to leave the territorial sea immediately'.

On the one hand, sovereignty is a key concept in the vocabulary of states that are victims of espionage. On the other hand, authors of such acts generally seek justification in their own national security.

---

[622] (1960) 6(12) Keesing, 17571.

[623] (1960) 6(7) Keesing, 17551.

[624] (1968) 14(3) Keesings, 22585; (1969) 15(1) Keesings, 23120.

[625] *Corfu Channel (UK v Albania)* (Contre-Mémoire soumis par le Gouvernement de la République Populaire d'Albanie) [15.06.1948], [117] <www.icj-cij.org/files/case-related/1/1492.pdf> accessed:12.10.2015.

[626] *Corfu Channel Case (UK v Albania)* (Duplique présentée par le Gouvernement de la République Populaire d'Albanie conformément à l'Ordonnance rendue le 28 mars 1948 par la Cour Internationale de Justice) [20.09.1948] ICJ Rep 1950, [130]-[131] <www.icj-cij.org/files/case-related/1/10896.pdf> accessed:13.10.2015.

[627] UNCLOS, art.27.

[628] UNCLOS, art.30.

B. The authors of espionage invoke the necessary protection of national security

National security has been invoked by authors of espionage for land, aerial and coastal espionage. During the debate at the UN Security Council (UNSC) concerning the U-2, the British delegation declared that '[w]e all knew that espionage was a fact of life, and a disagreeable one. Moreover, most espionage activities involved the violation of nations' sovereignties'.[629] As to Eisenhower, he affirmed that '[i]t is a distasteful but vital necessity'.[630] China added that espionage 'has been practised from the beginning of organized society' and 'the harsh law of survival in this nuclear age dictates it'.[631] President Castro admitted during a CNN interview that his government engaged in espionage against the USA. Considering the fact that the USA had 'spies in industrial quantities' and the need to infiltrate 'counterrevolutionary movements', he thought that he had 'the right to do this'.[632] The USA denied encouraging or tolerating terrorist activities against Cuba, but did not protest against Havana spying activities. Before the ICJ, the UK 'den[ied] that the ships had instructions to, or that they did in fact, carry out acts of espionage', and affirmed that 'keeping a close watch on shore against the development of further acts of hostility' and 'observation' were made necessary by the circumstances.[633]

To the extent that states attempt to justify their spying activities, a famous statement made in *Nicaragua* case needs to be considered: '[i]f a State acts in a way prima facie incompatible with a recognized rule, but defends its conduct by appealing to exceptions or justifications contained within the rule itself, then whether or not the State's conduct is in fact justifiable on that basis, the

---

[629] (1960) 6(5) Keesings, 17437.

[630] (1960) 42 Dep't St Bull 849, 851.

[631] UNSC, 858th Meeting (24.05.1960) [66].

[632] 'In rare admission, Castro says Cuba has dispatched spies across U.S.', *CNN* (20.10.1998) <http://edition.cnn.com/US/9810/20/cuban.espionage/> accessed:27.06.2018.

[633] *Corfu Channel (UK v Albania)* (Reply submitted, under the Order of the Court of 26th March, 1948, by the Government of the UK) [30.07.1948], [78d] <www.icj-cij.org/files/case-related/1/10895.pdf> accessed:12.10.2015.

significance of that attitude is to confirm rather than to weaken the rule'.[634] However, what was at stake in this case was qualifying the prohibition on the use of force and non-intervention as customary rules, in order to circumvent a reservation made by the USA and have jurisdiction.[635] In contrast, authors of spying do not deny the conventional or customary nature of territorial sovereignty, non-intervention, or the prohibition on the use of force. What is at stake is the *qualification* of their behavior. In the case of traditional espionage, they do not even deny that a breach of sovereignty occured; what they absolutely want to prevent is the qualification of such intrusion as use of force or an act of aggression. *Nicaragua* statement thus lacks relevance in the case of espionage.

Beyond this interplay of speeches, acts of espionage are usually followed by a wide variety of concrete consequences.

C. A wide variety of concrete consequences

Other spying cases reveal a wide variety of reactions, suggesting that states adopt malleable behaviour, and according to their own interests. While the Soviet official Melekh had no immunity and was indicted with espionage in the USA, the charges were dropped on condition that he quit the country. Robert Kennedy affirmed that this choice 'would best serve the national and foreign policy interests of the United States'.[636] The same happened with TASS correspondent in The Hague.[637] While some White Guardsmen had allegedly 'seriously violated the laws of Yugoslavia by their espionage and hostile acts', the government accepted to extradite them to the USSR.[638] Series of protests[639] or counter-

[634] *Nicaragua* (n.46) [186].

[635] Ibid [183].

[636] (1961) 7(12) Keesings, 18279.

[637] (1953) IX(3) Keesings, 12883.

[638] (1949) VII(12) Keesings, 10201.

[639] (1985) 31(11) Keesings, 33991; (1974) 20(7) Keesings, 26595.

accusations[640] have regularly occurred. The so-called agent could also be released following the intervention of his state of allegiance, and related to 'an act of good will',[641] 'executive acts of clemency',[642] 'a friendly gesture',[643] 'political considerations, having regard to the country's higher interests',[644] or even 'the concern expressed by "high officials of the United States"'.[645] Counter-measures sometimes occurred: expulsions of officials and teachers,[646] postponements of negotiations on trade,[647] or air transport agreements,[648] sanctions and deportations of citizens,[649] closure of consulates, travel bans,[650] cancellations of official visits.[651] Other types of reactions involved protests or condemns,[652] threats of deteriorations in relations,[653] counter-accusations,[654] while denial remained the authors' most common reaction.[655] Following the arrest of Günther Guillaume, Chancellor Schmidt declared that spying was incompatible with the spirit of *Ostpolitik*.[656]

---

[640] (1996) 42(4) Keesings, 41071.

[641] (2007) 53(4) Keesings, 47896.

[642] (2007) 53(4) Keesings, 47881.

[643] (1973) 19(2) Keesings, 25711.

[644] (1962) 8(12) Keesings, 18591.

[645] (1963) 9(11) Keesings, 19744.

[646] (1951) VIII(4) Keesings, 11401.

[647] (1960) 43 Dep't St Bull 157, 163-4.

[648] (1963) 9(11) Keesings, 19744.

[649] (2007) 53(4) Keesings, 47881.

[650] (1950) VII-VIII(1) Keesings, 10481; (1956) X(2) Keesings, 14700.

[651] (1982) 28(5) Keesings, 31512.

[652] (1949) VII(4) Keesings, 9945; (1950) VII-VIII(1) Keesings, 10481; (1953) IX(1) Keesings, 12685; (1987) 33(11) Keesings, 35543.

[653] (1998) 44(12) Keesings, 42445.

[654] (1960) 6(6) Keesings, 17498.

[655] (1951) VIII(12) Keesings, 11883; (1953) IX(1) Keesings, 12728; (1953) IX(10) Keesings, 13212; (1961) 7(2) Keesings, 17910; (1989) 35(4) Keesings, 36601; (2005) 51(6) Keesings, 46692.

[656] Ulrich Beyerlin, 'Völkerrechtliche Praxis der Bundesrepublik Deutschland im Jahre 1974' (1976) 36 Z.a.ö.R.V. 760, 836-9.

It results from the above that espionage *per se* is not illegal, contrary to its corollary breach of sovereignty. Moreover, observation by satellites in outer-space has never been considered a violation of sovereignty, contrary to aerial spying. Yet, the premices spied on are the same. In the absence of this territorial intrusion, it is interesting to determine how states perceive the relevance of sovereignty for the interceptions of telecommunications.

2.2. Interceptions of telecommunications and sovereignty

In the *Weber and Saravia* case, the ECtHR had the opportunity to determine whether 'monitoring of wireless telecommunications […] did interfere with the territorial sovereignty of foreign States'.[657] However, it declared the case inadmissible as 'the applicants failed to provide proof in the form of concordant inferences' that a breach of territorial sovereignty occurred.

Switzerland was also unable to find a definitive answer. Acknowledging the diversity of doctrinal arguments and the lack of clarity in conventional and customary law, the confederation confessed that the interceptions of communication on 'users located abroad'–i.e., 'on the territory of another State'–were 'problematical'.[658] 'Lacking its consent, territorial sovereignty' indeed 'prevent[ed] a State from exercising activities on another State's territory'.[659] Switzerland's dilemma was the following: was bugging 'an intrusion and a violation of territoriality' or–to the extent that it was 'conducted from Switzerland'–should it be considered that 'no physical violation on the territory of the other State' occurred?[660] It proposed a third solution: considering 'that

---

[657] *Weber and Saravia v Germany* ECHR 2006-XI 309, [81]

[658] Delegation of Management Commissions, 'Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet «Onyx»)' (10.11.2003) 1404-5 <www.admin.ch/opc/fr/federal-gazette/2004/1377.pdf> accessed:08.04.2016.

[659] Ibid.

[660] Ibid.

the interceptions occur[ed] in outer-space, where communication satellites are located'. [661] As 'outer-space belongs to the international common goods', 'territoriality' would 'not apply', and 'no violation' would occur.[662] Switzerland finally concluded that 'the compliance of interceptions carried out by Switzerland abroad' could not 'be solved by normative or conventional norms. Otherwise, one should renounce to have a foreign intelligence service'. [663] Following the revelations about Echelon, Belgium apprehended the legality of eavesdropping only in terms of HR.[664]

States have avoided adopting a definitive conclusion on the relationship between interception of telecommunications and sovereignty. As a territorial intrusion is similarly absent in the case of cyber-espionage, it is interesting to see whether states have a different attitude.

2.3. Cyber-espionage and sovereignty

State reactions regarding the relation between cyber-espionage and sovereignty are diverse: some of them qualify cyber-espionage as a violation of sovereignty (A), while others consider it is potentially the case (C), or only under certain circumstances (B). Even more deny that cyber-espionage breaches sovereignty (D), resort to unsubstantiated arguments (E), adopt pragmatic measures, renounce to binding rules or push for the adoption of non-binding measures (F). Others adopt an ambiguous position or promote the application of domestic law (G).

---

661 Ibid.

662 Ibid.

663 Ibid.

664 Comité R, 'Rapport d'Activités 2000' (2000) 53 <www.comiteri.be/images/pdf/Jaarverslagen/2000%20fr.pdf?phpMyAdmin=97d9ae9d92818b6f252c014a4a05bdfb> accessed:27.10.2017.

A. States qualifying cyber-espionage as a violation of sovereignty

Following the revelations about NSA's surveillance, three states, the European Parliament, the *Mercado Común del Sur* (MERCOSUR) and the Union of South American Nations (UNASUR) called cyber-espionage a violation of sovereignty. Bolivia said that 'the right to privacy was an issue linked to State sovereignty and to the right to defend natural resources'.[665] Russia called it 'overt hypocrisy in relationships between allies and partners', and 'a direct violation of the state's sovereignty'. [666] Finally, Brazil denounced the 'invasion and capture of confidential information concerning corporate activities and especially of disrespect to national sovereignty'. [667] When the Canadian Communications Security Establishment (CSE/CSEC) was suspected of spying on the Brazilian Ministry of Mines and Energy, a 'violation of national sovereignty' was similarly criticized.[668] The European Parliament 'call[ed] on the US authorities to suspend and review any laws and surveillance programmes that violate[d] […] the sovereignty and jurisdiction of the EU'.[669] Both the MERCOSUR[670] and the UNASUR[671] denounced the violation of sovereignty and the harm caused to the relations with the USA.

---

665 'Third Committee Approves Text Titled 'Right to Privacy in the Digital Age', as It Takes Action on 18 Draft Resolutions' (2013) UN Press Release GA/SHC/4094 <www.un.org/press/en/2013/gashc4094.doc.htm> accessed:30.04.2018.

666 'Putin: cyber espionage is direct violation of state's sovereignty', *Interfax* (11.07.2014) <www.interfax.com/newsinf.asp?id=519963> accessed:26.10.2017.

667 Brazil, 'Statement by H. E. Dilma Rousseff' (24.09.2013) 1-3.

668 Associated Press, 'Brazil accuses Canada of spying after NSA leaks', *Guardian* (08.01.2013) <www.theguardian.com/world/2013/oct/08/brazil-accuses-canada-spying-nsa-leaks> accessed:14.06.2018.

669 European Parliament, 'Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy' (2013) 2013/2682 RSP, [2] <www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_fr.pdf>

670 MERCOSUR, 'Decisión de Mercosur sobre el rechazo al espionaje por parte de los Estados Unidos' (2013) <www.mercosur.int/innovaportal/file/4506/1/decision_sobre_espionaje_es.pdf> accessed:29.10.2017.

671 UNASUR, 'Declaración de Paramaribo' (30.08.2013) [28] <https://repo.unasursg.org/alfresco/service/unasursg/documents/content/SEPTIMA_REUNION_ORDINARIA_DEL_CONSEJO_DE_JEFAS_Y_JEFES_DE_ESTADO_Y_DE_G

In contrast, Belgium and Ecuador qualify cyber-espionage as a violation of sovereignty only under certain circumstances.

B. *States qualifying cyber-espionage as a violation of sovereignty under certain circumstances*

While Professor Schaus's report advised the Belgian Permanent Oversight Committee on the Intelligence and Security Services (Comité R) that any form of (unauthorized) electronic surveillance targeting Belgium was a breach of sovereignty,[672] the latter finally adopted an intermediary position. Capture of data 'targeting a foreign territory' constitutes a 'breach of sovereignty' only when 'unlimited and unauthorized'.[673] The sole 'large scale' surveillance would thus be illegal.[674] Ecuador similarly considers that '[t]he continuing revelations about massive and indiscriminate systems of espionage that are being used to monitor the communications of all citizens all over the world […] infringe the principles of respect for sovereignty and non-interference in the internal affairs of States'.[675]

Some states have however avoided adopting a definitive position on this issue, and only qualify cyber-espionage as a potential violation of sovereignty.

OBIERNO_DE_LA_UNION_DE_NACIONES_SURAMERICANAS__DECLARACION_DE_PARAMARIBO.pdf?noderef=36d7df26-5630-485a-8f1a-02a7341ecc8a> accessed:29.10.2017.

672 Comité R, *Rapport d'Activités 2013* (Intersentia 2014) 207.

673 Comité R, *Rapport d'Activités 2014* (Intersentia 2015) 16 (footnote 43).

674 Ibid 38.

675 UNGA, 'Developments in the field of information and telecommunications in the context of international security' (11.08.2017) UN-Doc A/72/135, 10.

C. States qualifying cyber-espionage as a potential violation of sovereignty

The American DoD, the Canadian government, Australia and the Bahamas qualify cyber-espionage as a potential violation of sovereignty, but do not adopt a definite and clear position.

The American DoD thinks that '[a]n unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty'.[676] When the communications networks of a nation are used for purposes of an electronic attack, the transited states have 'more right to complain' if 'the attacking state obtained unauthorized entry into its computer systems as part of the communications path to the target computer'.[677] Whether the mere transit may 'be regarded as equivalent to a physical trespass into a nation's territory' is not settled, as 'such issues have yet to be addressed in the international community'.[678] However–and contrary to the DOD's position–the White House pushes for a two-tier regime, which would differentiate between commercial espionage (allegedly illegal), and intelligence carried out for intelligence purpose (legal). This position has been supported by the former Director of National Intelligence (DNI) Clappers,[679] by James Lewis before the House of Representatives,[680] and is reflected in the efforts to reach an agreement with China on commercial spying, rather than seeking to prohibit any form of espionage.[681]

---

[676] DoD/Office of General Counsel (OGC), 'An Assessment of International Legal Issues in Information Operations' (1st edn, 1999) 19 <www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf> accessed:23.09.2016.

[677] Ibid 23.

[678] Ibid 19-20.

[679] Sydney Freedberg, 'DNI, NSA Seek Offensive Cyber Clarity; OPM Not An "Attack"', *Breaking Defense* (10.09.2015) <https://breakingdefense.com/2015/09/clapper-rogers-seek-cyber-clarity-opm-not-an-attack/> accessed:19.11.2017.

[680] HoR, 'Cyber Epionage and the Theft of U.S. Intellectual Property and Technology', Testimony before Committee on Energy and Commerce (09.07.2013) 5 <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/ts130709_lewis.pdf> accessed:12.11.2017.

[681] James Lewis, 'The US Really Does Want to Constrain Commercial Espionage: Why Does Nobody Believe It?' (*Lawfare*, 01.07.2016)

This uncertainty is also valid in Australia, as '[c]yber espionage can have a significant impact on Australia's [...] sovereignty'.[682] The Canadian government adopts a confusing position, considering that '[w]hen successful, advanced cyber operations compromise our economic prosperity and sovereignty'.[683] However, what is an 'advanced cyber-operation' is not defined. Following NSA scandal, '[t]he Bahamas faces now where our citizens are questioning what these high ideals of territorial integrity, sovereignty and respect for the rule of law actually mean in practice'.[684] Dutch position is equally ambiguous. In 2011, the Dutch General Intelligence and Security Services (AIVD) adopted the classical position that, lacking the Netherlands' consent, '[a]ll secret intelligence activities performed by foreign intelligence services on Dutch soil represent a breach of Dutch sovereignty'.[685] In its 2015 annual report, the following formula was used: '[w]hen it comes to cyberthreats, the AIVD's primary focus is digital espionage. A breach of sovereignty and often damaging to Dutch political and economic interests, this is almost always carried out by state actors'.[686] The AIVD thus implied that either digital espionage or cyberthreats amounted to a breach of sovereignty. However, the 2016 annual report resorted to a milder–and non-legal–sentence, saying that these cyber-threats 'endanger both commercial

<www.lawfareblog.com/us-really-does-want-constrain-commercial-espionage-why-does-nobody-believe-it> accessed:13.11.2017.

682 Australian Government/Australian Security Intelligence Organisation (ASIO), 'ASIO Annual Report 2015-16' (2016), 25 <www.asio.gov.au/sites/default/files/2016%20ASIO%20Annual%20Report%20UNCLASSIFIED.pdf> accessed:28.10.2017.

683 Public Safety Canada, 'Security and Prosperity' (2016) 10 <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/2016-scrty-prsprty-en.pdf> accessed:11.10.2017.

684 'Bahamas Foreign Affairs Minister addresses OAS Regular Session', *The Bahamas Weekly* (6.06.2014) <www.thebahamasweekly.com/publish/oas-media-releases/Bahamas_Foreign_Affairs_Minister_addresses_OAS_Regular_Session35338.shtml> accessed:28.10.2017.

685 AIVD, 'Analysis of vulnerability to espionage' (2011) 11 <https://english.aivd.nl/binaries/aivd-en/documents/publications/2011/01/13/aivd-analysis-of-vulnerability-to-espionage/aivd-analysis-of-vulnerability-to-espionage.pdf> accessed:01.12.2017.

686 AIVD, 'Annual Report 2015' (2016) 21 <https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2016/05/26/annual-report-2015-aivd/annual-report-2015-aivd.pdf> accessed:01.11.2017.

interests and military effectiveness'.[687] The term 'sovereignty' does not even appear in the 2017 version.[688]

On the contrary, some states totally disavow the relevance of sovereignty to limit cyber-espionage.

D. States denying that cyber-spying is a violation of sovereignty

In contrast, Switzerland considers that 'computer network exploitation is not prohibited by international public law'.[689] Analogy with the legal framework surrounding espionage is openly mentioned, and 'the research of information by foreign computer networks is in principle authorized by international law, as long as relevant conditions are met'.[690] Those 'relevant conditions' nevertheless remain unclear. Moreover, the Swiss Federal Council 'used to denounce intelligence-activities directed towards Switzerland's interests, and to press the responsible states. It is however hard to intervene when such activities do not directly affect Swiss sovereignty, when exclusively carried out from abroad'.[691]

As mentioned previously, Harold Koh–then a Legal Adviser at the Department of State–thought that sovereignty had to be considered when cyber-operations were carried out. A statement by his successor–Brian J. Egan–helps clarifying the American position. It openly refers to Koh's 'remarks in 2012' and proposes

---

[687] AIVD, 'Annual Report 2016' (2017) 5 <https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2017/04/04/annual-report-2016/AIVD+Annual+Report+2016.pdf> accessed:01.11.2017.

[688] AIVD, 'Annual Report 2017' (2018) <https://english.aivd.nl/publications/annual-report/2018/03/09/annual-report-2017-aivd> accessed:23.06.2018.

[689] Lucius Caflisch, 'La Pratique Suisse en Matière de Droit International Public 2009' (2010) 20 R.S.D.I.E. 511, 560.

[690] 'Lucius Caflisch, 'La Pratique Suisse en Matière de Droit International Public 2013' (2015) 25 R.S.D.I.E. 57, 107.

[691] Answer Guy Parmelin to 'Question Glättli Balthasar. Surveillance d'autorités et d'agents publics suisses par le service de renseignement allemand' (7.03.2016) 16.5046 <www.parlament.ch/fr/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=36720> accessed:09.11.2017.

'to build on that statement and offer a few thoughts about the relevance of sovereignty principles to States' cyber activities'.[692] It affirms that 'remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a *per se* violation of international law', underlining that 'there is no absolute prohibition on such operations as a matter of international law'.[693] The continuation of his reasoning is unequivocal. 'This is perhaps most clear where such activities in another State's territory have no effects or *de minimis* effects'.[694] Then, '[m]ost States, including the United States, engage in intelligence collection abroad'.[695]

France also made its position clear, thanks to a statement by Cochard, the vice-director of MFA's *general division for political and security affairs*. After having qualified NSA's espionage as a 'breach of mutual trust'–and affirming that he was aware of Members of Parliament's (MP's) dissatisfaction with French official reaction–he said that 'this domain does not fall within the scope of international law'.[696] He also confessed that 'political pressure' was the only means at France's hand.[697] France also affirms that 'intelligence gathering' is 'a legitimate and necessary prerogative of State',[698] and belongs to the 'resources underpinning our sovereignty'.[699]

When discussing the activities of its own services, the position of the Canadian Parliament is closer to the French position than that of the Canadian

---

[692] Egan (n.61).

[693] Ibid.

[694] Ibid.

[695] Ibid.

[696] AN, 'Audition de M. Pierre Cochard' (01.07.2015) CR No.93, 11 <www.assemblee-nationale.fr/14/pdf/cr-cafe/14-15/c1415093.pdf> accessed:02.11.2017.

[697] Ibid.

[698] AN, 'Surveillance des communications électroniques internationales' (1.10.2015) <www.assemblee-nationale.fr/14/cri/2015-2016/20160002.asp> accessed:02.11.2017.

[699] Commission du livre blanc, *French White Paper on Defence and National Security 2013* (Ministère de la Défense/SGA/SPAC 2013) 20.

government. MP Chisu underlines 'that the foreign intelligence activities of CSEC are critical to fulfilling the government's commitment to address emerging threats to our sovereignty and economy'.[700] 'CSEC detects the activities of foreign terrorist networks and their operational plans', '[b]y targeting and intercepting foreign communications, decoding them, and then analyzing them'.[701] Moreover, 'CSEC has helped to identify and defend our country's interests against the actions of these hostile foreign intelligence agencies'.[702] MP Kent affirms that 'CSEC's collection of foreign intelligence makes an invaluable contribution to the pursuit of Canada's international affairs, its defence and security interests', helping to 'uncover terrorist plots' and to 'save Canadian lives'.[703] With respect to 'Canadian cybersecurity', 'CSEC's contribution' is 'unique', because 'CSEC, through its lawful foreign signals intelligence activities, is able to understand foreign cyberthreats before they can target Canadian systems'.[704]

The UK converges towards this position too, and is eager to resort to the very techniques that are used against its own interests. According to the British Intelligence and Security Committee (ISC), '[w]hile attacks in cyberspace represent a significant threat to the UK, and defending against them must be a priority, we believe that there are also significant opportunities for our intelligence and security Agencies and military which should be exploited in the interests of UK national security. In the Committee's view, these could include [...] Exploitation: Accessing the data or networks of targets to obtain intelligence or to cause an effect without being detected'.[705] Ministry Neville-Jones refers to

[700] House of Commons, Hansard-41 (02.04.2014) 2538.

[701] Ibid.

[702] Ibid.

[703] House of Commons, Hansard-41 (02.04.2014) 2536.

[704] Ibid.

[705] ISC, *Annual Report 2011-2012* (TSO 2012) [110].

various threats: 'state-led espionage', 'out for our valuable intellectual property', and 'non-state actors'.[706] According to her, 'it is our task to disrupt them'.[707]

Reference to legal terms–including sovereignty–is however not systematic in states' discourse. They also regularly resort to unsubstantiated arguments.

E. States resorting to unsubstantiated arguments

What is *not* said or done following accusations of espionage is also of importance. Regarding NSA's activities, neither France nor Germany denounced violation of international law. Angela Merkel affirmed that 'spying between friends just isn't on'.[708] Such a limited response can be easily explained: the German Federal Intelligence Service (BND) was actually cooperating with the NSA.[709] Surveillance by the USA was described by President Hollande as 'unacceptable',[710] and the French President declared that 'these kinds of practices should not happen between allies' after spying by Germany was revealed.[711] Their alleged hypocrisy was hardly concealed by Barack Obama:

---

[706] House of Lords, 'Cyberattacks: EU Committee Report', Col.696 (14.10.2010).

[707] Ibid.

[708] 'WikiLeaks: US spied on Angela Merkel's minister too, says German newspaper', *Guardian* (02.07.2015) <www.theguardian.com/media/2015/jul/02/wikileaks-us-spied-on-angela-merkels-ministers-too-says-german-newspaper> accessed:23.04.2016.
Navarette affirms that 'this kind of sentence [...] points towards the unfriendly act, rather than the international illicit act'. See Inaki Navarette, 'L'Espionnage en Temps de Paix en Droit International Public' (2015) 53 Canadian Y.B.I.L. 1, 48.

[709] Konrad Lischka, 'BND leitet seit 2007 Daten an die NSA weiter', *Spiegel* (08.08.2013) <www.spiegel.de/netzwelt/netzpolitik/geheimdienste-bnd-leitet-seit-2007-daten-an-die-nsa-weiter-a-915589.html> accessed:14.06.2016.

[710] Damien Leloup, 'Révélation après révélation, le silence de la France face à l'espionnage de la NSA', *Le Monde* (23.06.2015) <www.lemonde.fr/pixels/article/2015/06/23/revelation-apres-revelation-le-silence-de-la-france-face-a-l-espionnage-de-la-nsa_4660310_4408996.html> accessed:14.03.2016.

[711] 'French president wants "all information" on reported German spying', *Deutsche Welle* (12.11.2015) <www.dw.com/en/french-president-wants-all-information-on-reported-german-spying/a-18845907> accessed:23.04.2016.

'[m]eanwhile, a number of countries, including some who have loudly criticized the NSA, privately acknowledge that America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities, and that they themselves have relied on the information we obtain to protect their own people'.[712]
Contrary to South American and European countries, Australian Foreign Secretary Julie Bishop was very supportive to the USA, saying that the FiveEyes Agreement 'is about saving lives'.[713]

However, even 'enemies' sometimes fail to denounce violations of international law when they learn about spying. An example is when Israel was suspected of spying on Iran with the spying programs *Flame*,[714] and *Duqu*.[715] Discoveries of cyber-espionage instances without denunciation of sovereignty violations are not rare,[716] but counter-measures are sometimes adopted. After having called spying by Australia an 'unfriendly act', Indonesia decided to suspend intelligence sharing and military cooperation.[717] The latter was indeed unsatisfied that PM Abbott had 'expressed only "regret"' by 'media reporting'.[718]

---

712 'Obama's Speech on N.S.A. Phone Surveillance', *NYT* (17.01.2014) <www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html> accessed:15.11.2017.

713 Katharine Murphy, 'Edward Snowden a traitor but US spy review is welcome, says Julie Bishop', *Guardian* (23.01.2014) <www.theguardian.com/world/2014/jan/23/edward-snowden-a-traitor-but-us-spy-review-is-welcome-says-julie-bishop> accessed:20.01.2016.

714 Thomas Erdbrink, 'Iran Confirms Attack by Virus That Collects Information', *NYT* (29.05.2012) <www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html?_r=1&hp> accessed:10.05.2015.

715 'US accuses Israel of spying on nuclear talks with Iran', *Guardian* (24.03.2015) <www.theguardian.com/world/2015/mar/24/israel-spied-on-us-over-iran-nuclear-talks> accessed:10.05.2015.

716 Pierluigi Paganini, 'Finland's Ministy of Foreign Affairs hit by extensive cyber-espionage', *Security Affairs* (2013) <http://securityaffairs.co/wordpress/19349/cyber-crime/finland-cyber-espionage.html> accessed:13.11.2016;
'La France suspectée de cyberespionnage', *Le Monde* (21.03.2014) <www.lemonde.fr/international/article/2014/03/21/la-france-suspectee-de cyberattaque_4387232_3210.html> accessed:24.05.2015.

717 (2013) 59(11) Keesings, 53009.

718 Ibid.

When important economic interest is at stake, the victim may refuse to comment or have a mild reaction. This usually happens when China is accused of cyber-espionage. While China is Australia's first trading partner and Germany's third one, Australian Foreign Minister Carr underlined that allegations of cyber-espionage did not affect Australia's strategic partnership with China,[719] and Germany just reminded the PRC of the importance of 'abiding by international rules'.[720] Following a report by *Mandiant* accusing China of hacking, 'no senior US official confronted China by name over the issue'.[721] China usually denies being the author of cyber-espionage.[722]

What states say about cyber-espionage is of the highest importance in determining the applicability of sovereignty to cyber-espionage. However, what they *do* is of equal interest.

F. *States adopting pragmatic measures, renouncing to binding rules or pushing for non-binding measures*

Some states have already renounced to adopt conventional rules with respect to cyber-espionage. Switzerland considers that intelligence services have to protect national interest, which explains why no binding agreement prohibiting unlawful intelligence gathering exists.[723] Should such an agreement come into force, the Federal Council thinks that it would anyway be circumvented.[724] Bern finds it

---

[719] (2013) 59(5) Keesings, 52676.

[720] 'Cyber Menace: Digital Spying Burdens German-Chinese Relations', *Spiegel* (25.02.2013) <www.spiegel.de/international/world/digital-spying-burdens-german-relations-with-beijing-a-885444.html> accessed:27.02.2014.

[721] (2013) 59(2) Keesings, 52489.

[722] Ibid.

[723] 'Avis du Conseil Fédéral' to 'Motion Evi Alleman. Affaire Snowden–Accord de non-espionnage avec les Etats-Unis' (19.02.2014) 13.4165 <www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20134165> accessed:09.11.2017.

[724] Ibid.

more relevant to take appropriate preventive measures, rather than intergovernmental treaties.[725] The UK does the same. According to Minister Neville-Jones, law enforcement is needed in cyberspace. However, she is 'more cautious about the question of operating within legal frameworks when it comes to trying to regulate the international scene'.[726] While describing 'a convention that gives us the rules of the road instead of simply codes of conduct' as 'an extremely attractive proposition', she affirms that 'you have to be confident of two things'.[727] First, 'that those who sign conventions will actually then obey their precepts and not seek to go outside them while you observe the rules; otherwise, you are putting yourself at a disadvantage'.[728] Secondly, 'you need to be able to ensure that you can verify what they are doing'.[729] The UK also defends this position before the UNGGE, and 'does not believe that attempts to conclude comprehensive multilateral treaties, codes of conduct or similar instruments would make a positive contribution to enhanced cybersecurity for the foreseeable future'.[730]

Denmark, Finland, Iceland, Norway, Sweden, and the USA have already committed themselves 'to the view that all states should abide by voluntary and non-binding norms of responsible state behavior in cyberspace during peacetime'.[731]

Moreover, states are sometimes more eager to adopt pragmatic measures than denouncing espionage. For instance, following 'concerns [...] over surveillance', Germany 'strongly encourage[d] IT service providers to encrypt

---

[725] Ibid.

[726] House of Lords, 'Cyberattacks: EU Committee Report', Col.696 (14.10.2010).

[727] Ibid.

[728] Ibid.

[729] Ibid.

[730] UNGA, 'Developments' (16.07.2013) (n.87) 18.

[731] 'US–Nordic Leaders' Summit, Joint Statement' (13.05.2016) <https://obamawhitehouse.archives.gov/the-press-office/2016/05/13/us-nordic-leaders-summit-joint-statement> accessed:09.11.2017.

telecommunication and not to forward telecommunication data to foreign intelligence services'.[732] The EU did the same following revelations about Echelon, thus deciding to invest €11 million in a project to improve cryptography.[733] France has also taken concrete measures.[734]

Some states also choose to promote the application of domestic law–rather than international law–to cyber-espionage.

G. States adopting ambiguous positions or promoting the application of domestic law

An ambiguous–and similar–reasoning is adopted by Finland, France and the UK. It consists in denouncing, together, the danger posed by cyber-espionage and cyber-attacks, and–immediately after this–in expressly qualifying the sole operation with a destructive effect as a violation of sovereignty. According to Finland, '[t]he purpose of foreign information systems intelligence may be not only to acquire information, but also to disrupt the operations of the target systems or to damage them by altering or deleting data. Such operations may be interpreted by the government of the target country as the use of force or a violation of sovereignty tantamount to an armed attack'.[735] The UK mentions that, '[b]eyond the espionage threat, a small number of hostile foreign threat actors have developed and deployed offensive cyber capabilities, including destructive ones […] Some states may use these capabilities in contravention of international law in the belief that they can do so with relative impunity'.[736] After

---

[732] UNGA, 'Developments' (30.06.2014) (n.95) 12.

[733] David Alan Jordan, 'Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice Over Protocol' (2005) 47(3) Bost CLR 505, 512.

[734] AN, '1ere séance du 23 février 2000' (2000) <www.assemblee-nationale.fr/11/cra/1999-2000/2000022315.asp#TopOfPage> accessed:09.11.2017.

[735] DEFMIN, 'Guidelines for Developing Finnish Intelligence Legislation' (2015) 73. <www.defmin.fi/files/3144/GUIDELINES_FOR_DEVELOPING_FINNISH_INTELLIGENCE_LEGISLATION.pdf> accessed:13.05.2017.

[736] UK Government, 'National Cyber Security Strategy 2016-2021' (n.249) 18.

having described cyber-espionage as a 'threat', 'cyber-sabotage' is–according to the SGDSN–'affecting sovereign interests'.[737]

Some terms used by Spain, Estonia, the ISC, the Swedish Security Service (SÄPO), the Finnish Security Intelligence Service (SUPO) and the Dutch Military Intelligence and Security Service (MIVD) are also ambiguous. For instance, espionage is described as 'unlawful',[738] 'illegal means',[739] 'causing harm',[740] 'unauthorized',[741] an 'hostile cyber act',[742] or 'foreign hostile activity',[743] 'contrary to national interest',[744] 'a significant threat to security'.[745] However, this characterisation in legal terms could refer to domestic law–rather than international rules. Debates at the French National Assembly and the Canadian Parliament are particularly interesting with respect to this articulation of respective domestic laws. Bajolet's answer to MP Candelier–who asked why NSA mass-surveillance had not stopped in spite of reforms promised by the White House–was evoked in the introduction: 'the NSA has to comply with American law, as the DGSE has to comply with French law. However, American

737 Bruno Sido and Jean-Yves Le Déaut, 'Le Risque Numérique: En prendre conscience pour mieux le maitriser?' (03.07.2015) 10 <www.assemblee-nationale.fr/14/pdf/rap-off/i1221.pdf> accessed:24.11.2017.

738 SAPO, *Swedish Security Service 2013* (Edita 2014) 25.

739 SUPO, 'Finnish Security Intelligence Service' (2011) 12 <www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/26154_2011_Supo-English.pdf?156efc9e4d2ad288> accessed:30.10.2017.

740 Ibid 24.

741 MIVD, '2014 Annual Report' (2015) 37 <www.government.nl/binaries/government/documents/annual-reports/2015/07/21/2014-annual-report-netherlands-defence-intelligence-and-security-service/mivd-openbaar-jaarverslag-2014-engels.pdf> accessed:01.12.2017.

742 Estonian Information Board, 'International Security and Estonia' (2016) 46 <www.valisluureamet.ee/pdf/2016-en.pdf> accessed:29.10.2017.

743 ISC, 'Annual Report 2011-2012' (n.705) 8.

744 Spanish Government, 'Estrategia de Seguridad Nacional' (2013) 34 <www.dsn.gob.es/sites/dsn/files/Estrategia_Seguriad_Nacional_2017.pdf> accessed:29.10.2017.

745 Presidencia del Gobierno, 'Estrategia de Seguridad Nacional' (2017) 62 <www.dsn.gob.es/sites/dsn/files/2017_Spanish_National_Security_Strategy_0.pdf> accessed:29.10.2017.

law does not prohibit such activities'.[746] Yet, he added that France disapproved them.[747] According to MP Kent, 'CSEC must conduct its cyber-protection mission with great care, with adherence to all Canadian laws […]'.[748] This aspect is to be analysed further in this thesis.[749]

3. Conclusion

The apparent consensus surrounding the applicability of international law and sovereignty in cyberspace conceals an incredible cacophony. Logically, one could have expected two trends. Either states consider cyberspace as a territory, thus applying existing international law. Or they define it as something different, a 'virtual space', and choose to develop a new corpus of rules.[750] Curiously, they adopt a hybrid solution, agreeing on the fact that cyberspace is a new space, with specific particularities, but propose to apply pre-existing rules, suited for a physical territory.

Yet, territorial sovereignty is silent regarding cyber-espionage, which is partly explained by the dematerialization of spying activities: the illegality of traditional spying resides only in its corollary physical intrusion, not in espionage *per se*. This conclusion is confirmed by state practice. Certainly, Australia, the Bahamas and the Netherlands could actually be destabilized by the new forms of espionage brought by cyberspace, and choose to adopt a deliberately vague, ambiguous position, which may be described as a 'wait and see' attitude. Admittedly, South American States struggle qualifying cyber-espionage as a violation of sovereignty, and the reasons behind such choices are unclear. Do they actually conclude that a violation of sovereignty occurs, or do they realise that they are 'losing' the 'great game'? But–outside this circle–most states do not think that

---

[746] AN, 'Avis fait au nom de la Commission de la défense nationale et des forces armées' (n.2) 79.

[747] Ibid.

[748] Statement by Hon. Peter Kent, Hansard-41 (2.04.2014) 2536.

[749] See part III.

[750] See Lafouasse, *L'Espionnage* (n.66) 170-1.

cyber-espionage amounts to a violation of sovereignty, and choose to act and react according to their own interests, in weighing up the pros and cons. The USA–the world's foremost economic power, and entangled in a global surveillance scandal–struggles to prove the legality of espionage for intelligence purposes and the illegality of economic spying. Europe's major spies (France,[751] Germany, [752] and the UK), [753] along with Switzerland, do not consider international law as a potential regulator of cyber-espionage. Belgium–which acknowledges 'moderate' intelligence activities and has to comply with ECtHR case law–qualifies the sole 'large-scale' surveillance as illegal. Nordic and Baltic countries do not think that cyber-espionage amounts to a violation of sovereignty, but–probably for political reasons–choose to express it in a subtler way. In such cases, only cyber-attacks are qualified as a breach of sovereignty (Finland), reference is made to unlawfulness in domestic law (Estonia, Finnish and Swedish secret services), or those states push for the adoption of non-binding measures (Denmark, Finland, Iceland, Norway, Sweden). Despite Putin's critics of NSA mass surveillance, Russia's intense spying is an open secret. Their qualification of the PRISM programme as a breach of sovereignty is thus of little legal significance. By comparison, China's reaction was more moderate.[754]

---

[751] Jacques Follorou and Franck Johannès, 'Révélations sur le Big Brother français', *Le Monde* (07.07.2013) <www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html> accessed:19.09.2014.

[752] Maik Baumgärtner, Martin Knobbe and Jörg Schindler, 'German Intelligence Also Snooped on White House', *Spiegel* (22.06.2017) <www.spiegel.de/international/germany/german-intelligence-also-snooped-on-white-house-a-1153592.html> accessed:17.08.2017.

[753] Martin Untersinger, 'Les dérives des espions britanniques', *Le Monde* (23.06.2015) <www.lemonde.fr/pixels/article/2015/06/23/les-derives-des-espions-britanniques_4659585_4408996.html> accessed:02.07.2015.

[754] Hong Lei, the spokesman for Chinese Foreign Ministry, only expressed 'serious concern'. He added that China 'always believe that Internet communication technology should be employed for a country's social-economic development, rather than Internet espionage and monitoring'. See Andrew Jacobs, 'After Reports on N.S.A., China Urges End to Spying', *NYT* (24.03.2014) <www.nytimes.com/2014/03/25/world/asia/after-reports-on-nsa-china-urges-halt-to-cyberspying.html> accessed:22.11.2017.

II – NON-INTERVENTION

According to the *Nicaragua* case, 'the principle' of non-intervention 'forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other State'.[755] Interventions bearing 'on matters in which each State is permitted, by the principle of State sovereignty to decide freely', and involving 'methods of coercion in regard to such choices' are prohibited.[756] The test is thus a two-tier one: (1) methods of coercion; (2) within a state's exclusive domestic jurisdiction.

Some of the matters under exclusive domestic jurisdiction were suggested by the *Nicaragua* case–'the choice of a political, economic, social and cultural system, and the formulation of foreign policy'[757]–and echoed the formulation given in Resolution 2625.[758] In the past, this concept used to be reconciled with the notion of states' *domaine réservé*, which 'describes areas where States are free from international obligations and regulation'.[759] According to the PCIJ, '[t]he question whether a certain matter is or is not solely within the jurisdiction of a State is an essentially relative question; it depends on the development of international relations'.[760] However, doctrine regularly underlines that few domains are now totally isolated from international law.[761]

As to '[t]he element of coercion', the *Nicaragua* case affirmed that it 'defines, and indeed forms the very essence of, prohibited intervention'.[762] This notion of

---

[755] *Nicaragua* (n.46) [205].

[756] Ibid [205].

[757] Ibid [205].

[758] UNGA Res 2625 (XXV) (24.10.1970) [Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations].

[759] Katja Ziegler, 'Domaine Réservé' (2013) M.P.E.P.I.L., [1].

[760] *Nationality Decrees Issued in Tunis and Morocco on Nov. 8th, 1921* (Advisory Opinion) [1923] PCIJ Rep series B No.4, 24.

[761] Philip Kunig, 'Intervention, Prohibition of' (2008) M.P.E.P.I.L., [3]; Verhoeven, 'Non-Intervention: « Affaires intérieures » ou « Vie privée » ?' in *Le droit international au service de la paix, de la justice et du développement: mélanges Michel Virally* (Pedone 1991) 497; Ziegler (n.759) [3].

[762] *Nicaragua* (n.46) [205].

coercion appeared in Resolution 2625, as '[n]o State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind'.[763] The ICJ added that coercion was 'particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State'.[764]

Some details should be added regarding the possible distinction between 'non-intervention' and 'non-interference'. These terms have been used in numerous treaties,[765] UNGA resolutions,[766] and, 'in most contexts, the two terms seem to be used interchangeably'.[767] This terminological duality nevertheless led to the emergence of two doctrinal models.

In the first model, the sole 'intervention' is considered illegal. Henderson thinks that 'a distinction must be drawn between common forms of *interference* and prohibited *interventions*'. [768] Jennings and Watts write that, 'to constitute intervention, the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question. Interference pure and simple is not intervention'.[769] Tallinn

---

763 UNGA Res 2625 (n.758).

764 *Nicaragua* (n.46) [205]

765 Charter of the Organization of American States (Adopted:30.04.1948–EIF:13.12.1951) 119 UNTS 3, arts.3, 19; Constitutive Act of the African Union (Adopted:11.07.2000–EIF:26.05.2001) 2158 UNTS I-37733, art.4; Charter of the Association of Southeast Asian Nations (Adopted:20.11.2007–EIF:15.12.2008) 2624 UNTS 223, art.2(2); Pact of the League of Arab States (Adopted:22.03.1945–EIF:11.05.1945) 70 UNTS 237, art.VIII.

766 UNGA Res 2131 (XX) (21.12.1965) [Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty]; UNGA Res 2625 (n.758); UNGA Res 34/101 (14.12.1979) [Non-interference in the internal affairs of States]. See also: Conference on Security and Co-operation in Europe Final Act (Helsinki, 1975).

767 Michael Wood, 'Non-Intervention (Non-interference in domestic affairs)' (*Encyclopedia Princetoniensis*) <https://pesd.princeton.edu/?q=node/258> accessed:22.11.2017; See also: Karine Bannelier and Théodore Christakis, *Cyber-Attacks, Prevention-Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale 2017) 43; Niki Aloupi, 'The Right to Non-Intervention and Non-Interference' (2015) 4(3) C.J.I.C.L. 566, 572.

768 Christian Henderson, *The Use of Force and International Law* (C.U.P. 2018) 51.

769 Robert Jennings and Arthur Watts, *Oppenheim's International Law-Vol.I: Peace* (9th edn, O.U.P. 2008) 432

Manual 2.0 notes that '[i]nconsistent language is used to address the principle of non-intervention. In particular, States sometimes use the term "interference" in lieu of "intervention" […] For the purposes of this Rule [66], "interference" refers to acts by States that intrude into affairs reserved to the sovereign prerogative of another State, but lack the requisite coerciveness […] The term intervention […] is limited to acts of interference with a sovereign prerogative of another State that have coercive effect […]'.[770] Jamnejad and Wood consider that 'only acts of a certain magnitude are likely to qualify as "coercive", and only those that are intended to force a policy change in the target state will contravene the principle'.[771]

In the second model, a difference might be identified between 'territorial' (non-intervention) and 'political' integrity (non-interference). According to Bannelier and Christakis, '[i]t could be considered that the former refers to the protection of the territory of the State, of its *dominium*, and that its violation would therefore involve the carrying out of material operations in foreign territory; while the latter would refer to interference, without the authorization of the State, in the sphere of the exercise of its national sovereign powers and would, therefore, affect the *imperium* of the State'.[772] Dupuy and Kerbrat have a similar approach.[773] Aloupi supports a 'distinction between non-intervention (territorial integrity) and non-interference (independence and autonomy)', which is 'theoretically clear'.[774]

Unfortunately, declarations and case-law are of little help to cut a clear distinction between 'non-intervention' and 'non-interference'. The blurring probably culminated in Declaration 2625, which is supposed to contain 'principles of international law'. It indeed mentioned that '[n]o State or group of States has the right to intervene, directly or indirectly, for any reason whatever,

---

[770] Schmitt, *Tallinn Manual 2.0* (n.53) 313.

[771] Maziar Jamnejad and Michael Wood, 'The Principle of Non-Intervention' (2009) 22(2) L.J.I.L. 345, 348.

[772] Bannelier and Christakis (n.767) 43.

[773] Pierre-Marie Dupuy and Yann Kerbrat, *Droit international public* (Dalloz 2014), paras 117-119.

[774] Aloupi (n.767) 572.

in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law'.[775] The ICJ found that '[t]he principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference'.[776] It also ruled that 'Uganda had violated the sovereignty and also the territorial integrity of the DRC. Uganda's actions equally constituted an interference in the internal affairs of the DRC […] The unlawful military intervention by Uganda was of such a magnitude and duration that the Court consider[ed] it to be a grave violation' of UN Charter's article 2(4).[777] This thesis thus deems these terms interchangeable.

This essay nevertheless supports a distinction between the *dominium* and the *imperium*, as reflected in the *Nicaragua* case: '[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations […] and international law requires political integrity also to be respected'.[778] Regulations on the use of force–which may breach both the *dominium* and the *imperium*–are tackled in the following chapter. The rule protecting the *dominium* from activities below use of force–territorial sovereignty–was tackled in the previous chapter. 'Non-intervention' (or 'non-interference')–analysed in the present chapter–thus protects states from activities directed against their 'political integrity' (*imperium*), even if they do not involve use of force or a territorial intrusion.

As to the applicability of non-intervention to cyber-activities, Russia, China, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan are among the few to express their view in an abstract manner. They oppose any use of the Internet 'to interfere in the internal affairs of other States or with the aim of undermining

[775] UNGA Res 2625 (n.758).

[776] *Nicaragua* (n.46) [202].

[777] *Armed Activities on the Territory of the Congo (DRC v. Uganda)* (Judgment) [2005] ICJ Rep 168, [165].

[778] *Nicaragua* (n.46) [202].

their political, economic and social stability'.[779] According to China, '[c]ountries shouldn't use ICTs to interfere in other countries' internal affairs and undermine other countries' political, economic, and social stability as well as cultural environment', or take advantage of its dominant position in information space to undermine other countries' right of independent control of ICT products and services'.[780] When acting in 'the global information space', the Russian armed forces 'are guided' by 'non-interference in the internal affairs of other states'.[781] As to the USA, Egan thinks that '[f]or increased transparency, States need to do more work to clarify how the international law on non-intervention applies to States' activities in cyberspace'.[782] Belarus affirms that 'it is crucial to gradually advance the principle of non-interference in the internal affairs of sovereign States and mutual rejection of aggressive actions in the information sphere'.[783]

Here, the key elements of the principle of non-intervention and its applicability in cyberspace have been enlightened. However, its applicability to the specific issue of cyber-espionage needs to be analysed, starting with the status of doctrine (1), and continuing with the status of law (2). A conclusive note ends this chapter (3).

1. Status of doctrine

The status of doctrine regarding espionage (1.1), interception of telecommunications (1.2), and cyber-espionage (1.3) will be discussed in turn.

779 UNGA, 'Letter dated 9 January 2015' (n.143) [3].

780 PRC PMUN, 'Statement by Ms. Liu Ying' (n.118).

781 Russian MOD (n.85) [2.1].

782 Egan (n.61).

783 UNGA, 'Developments' (11.08.2017) (n.675) 6.

1.1. Espionage

According to Wright, '[i]t belongs to each state to define peacetime espionage […] as it sees fit, and it is the duty of other states to respect such exercise of domestic jurisdiction'.[784] Thus, 'any act by an agent of one state committed in another state's territory, contrary to the laws of the latter, constitutes intervention, provided those laws are not contrary to the state's international obligations'.[785] He thus describes espionage as a 'subversive intervention'.[786] Scott refers to the 'traditional doctrinal view', which defines espionage as a prohibited intervention.[787] McDougal, Lasswell and Reisman similarly consider that '[t]he more traditional doctrinal view has been that intelligence gathering within the territorial confines of other states constitutes an unlawful intervention, under both customary and conventional international law'.[788] However, '[i]n terms of the actual volume of this activity […] the number of formal protests which have been lodged have been relatively insignificant. This latter practice suggests a somewhat ambivalent perspective upon the part of national elites in regard to such activities and may indicate a deep but reluctant admission of the lawfulness of such intelligence gathering, when conducted within customary normative limits'.[789] According to Fleck, the ICJ–including in the *Nicaragua* case–'has not taken a position on the issue of peacetime espionage, although it has had the opportunity to do so on a few occasions'. However, 'peacetime rules of international law may be seen as including an implicit prohibition on subversive activities, as reflected in the Friendly Relations Declaration'.[790]

---

[784] Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs' in Stanger (n.569) 13.

[785] Ibid.

[786] Ibid.

[787] Robert Scott, 'Territorially intrusive intelligence collection and international law' (1999) 46 A.F.L.R. 217, 219.

[788] McDougal, Lasswell, Reisman (n.581) 394.

[789] Ibid.

[790] Dieter Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 Mich.J. .Int'l.L. 687, 692.

1.2. Interception of telecommunications

Peters considers that non-public communications among government officials belong to a state's *domaine réservé*. 'It is not the business of other states to gather information on political matters which another state seeks not to communicate […] states are not obliged to make all of their internal decision-making processes public, because this would completely stall politics'.[791] However, coercion 'is lacking, since spying did not seek to pressure the observed states into specific behaviour'.[792] Talmon is of the same opinion.[793]

1.3. Cyber-espionage

Some authors tackle both coercion and exclusive domestic jurisdiction, usually with respect to two events: the specific issue of economic cyber-espionage and the hacking of the DNC.

Concerning economic cyber-espionage, Parajon-Skinner affirms that coercion is not necessarily military, but 'can result from any impediment to a state's ability to "decide freely" in matters that touch on any aspect of that state's sovereignty'.[794] Thus, cyber economic espionage 'can be seen as a form of coercion that impermissibly interferes with both the internal and external affairs of a state'.[795] As a state is allegedly sovereign over its economic–not only territorial–space, 'the principle of non-intervention gives rise to prohibitions on a state's interference in that economic space'.[796] According to Lotrionte, 'the mere collection of protected information does not constitute a coercive act in

---

[791] Peters (n.583).

[792] Ibid.

[793] Stefan Talmon, 'Tapping the German Chancellor's Cell Phone and Public International Law' (*C.I.L.J.*, 06.11.2013) <http://C.I.L.J..co.uk/2013/11/06/tapping-german-chancellors-cell-phone-public-international-law/> accessed:19.10.2015.

[794] Parajon-Skinner (n.591) 1189.

[795] Ibid 1190.

[796] Ibid.

that it does not force the target state to change or forgo a policy on which it has the right to decide'. [797] In contrast, 'economic espionage is distinguishable from traditional espionage in that economic espionage involves the theft of property of entities within a state that will disadvantage the state in the global trade market, negatively impacting the state's policies related to global trade. Often, the resulting damage caused by the economic espionage will require the victim state to alter its domestic and international policies to stem the damage, thus making the economic espionage coercive in the manner intended by the Nicaragua Court, and therefore a wrongful act of intervention'.[798]

Navarette fully disagrees with this 'broad reading' of the principle, as 'the means used have to be coercive *per se*, which differs from the nature of the collected information'. [799] Moreover, '[i]n an era of globalization and economic interdependence, it seems difficult to argue that States benefit from a totally discretionary competence in their economic decisions'.[800] According to him, espionage is not coercive.[801]

With respect to Russian interferences in the American elections, Ohlin analyses the notions of *domaine réservé* and of coercion but finds them maladjusted. He affirms that '[t]he lack of fit with the doctrinal requirements for an illegal intervention against another State's sovereignty is simply an indication that the notions of "sovereignty" and "intervention" […] are poorly suited to analysing the legality of the conduct in this case'.[802] According to Watts, '[t]hat the hacks implicate the political process of the U.S. makes intervention an initially attractive characterization. Interference with another State's system of internal governance is a classic example of prohibited intervention'. However, '[i]n the case of the D.N.C. hacks […] it is not overwhelmingly clear that the U.S. has

---

[797] Catherine Lotrionte, 'Countering State-Sponsored Cyber Economic Espionage Under International Law' (2014-2015) 40 N.C.J.Int'l.L.&Com.Reg. 443, 502.

[798] Ibid.

[799] Navarette (n.708) 30.

[800] Ibid.

[801] Ibid 28.

[802] Jens-David Ohlin, 'Did Cyber Interference in the 2016 Election Violate International Law?' (2017) 95 Tex.L.Rev. 1579, 1580.

been coerced in any significant respect'. At the opposite, 'if a State were to hack election results of another State, a clearer case for prohibited intervention might be made–especially if the victim State were to swear-in the wrong candidate'.[803] Van de Velde is of the same opinion.[804] Barela affirms that 'there is little doubt that a democratic election is an internal affair', and considers adopting the definition of coercion as set up by McDougal and Feliciano, which 'is determined by "consequentiality"'.[805] He thinks that, 'in a democracy, free and fair elections play the essential role of conferring legitimacy on an authority', and qualifies legitimacy as 'a *sine qua non* for the State'.[806] Regarding the dissemination of true information, he thinks that '[t]he fact that the material was shopped to different outlets and released piecemeal for maximum effect certainly speaks to the intent to manipulate'.[807] Concerning the dissemination of fake stories, 'when taken in conjunction with the complete operation to influence opinion, these can be added to the case for coercion'.[808] As a consequence, 'direct and substantial electoral intervention targets a *sine qua non* for the State and should be interpreted as an act of coercion'.[809]

Other authors place greater emphasis on coercion. Barkham affirms that '[t]he purely economic nature of the actions suggests that economic espionage is an act of economic coercion'.[810] Kilovaty has the opposite opinion, as 'cyber-

---

[803] Sean Watts, 'International Law and Proposed U.S. Responses to the D.N.C. Hack' (*justsecurity,* 14.10.2016) <www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/> accessed:25.11.2017.

[804] Jacqueline Van De Velde, 'The Law of Cyber Interference in Elections' (2017) 28-31 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828> accessed:25.11.2017.

[805] Steven Barela, 'Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion' (*justsecurity*, 12.01.2017) <www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion/> accessed:25.11.2017.

[806] Ibid.

[807] Ibid.

[808] Ibid.

[809] Ibid.

[810] Barkham (n.233) 90.

espionage does not coerce a state in its political, economic, social or cultural system's free choices'.[811] Many authors have also written on the Democratic National Committee (DNC) hacking. Forcese refers to the *Nicaragua* case and Joyner's definition of coercion,[812] and then says that '[t]hese strictures clearly implicate some forms of covert action'.[813] He nevertheless mitigates this observation by referring to rule 10 of Tallinn Manual and concludes that '[t]he Russian influence operation seems a plausible candidate for exceeding this threshold, depending on how broadly one construes the requirement of "coercion"'.[814] According to Jupillat, '[c]oercion implies constraint, of at least two kinds'.[815] One resorts to 'force or intimidation' to 'induce compliance against the victim's will', but 'this has little application in the context of espionage'.[816] 'Nevertheless, coercion is also constituted when you have to undergo something being done to you against your will. Here, the coercive power uses its position of superiority to do whatever they please despite the victim's lack of consent'.[817] This 'second definition' is allegedly 'especially relevant to certain cases of cyber-espionage and mass surveillance operations, which continue to exist despite strong opposition from target states'.[818] He adds that '[f]urther indications of *opinio juris* that scale makes cyber-espionage less acceptable is that it does not allow states to guarantee a fundamental right in their own territory'.[819] Then, '[w]hen cyber-espionage does not rise to the level of intervention by itself, it may

---

[811] Ido Kilovaty, 'Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare' (2014) 5(1) N.S.L.B. 91, 107.

[812] Christopher Joyner, 'Coercion' (2006) M.P.E.P.I.L., [1].

[813] Craig Forcese, 'The "Hacked" US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards?' (*justsecurity*, 16.12.2016) <www.justsecurity.org/35652/hacked-election-international-law-silent-faced-clatter-cyrillic-keyboards/> accessed:25.11.2017.

[814] Ibid.

[815] Nicolas Jupillat, 'From the Cuckoo's Egg to Global Surveillance: Cyber Espionage That Becomes Prohibited Intervention' (2017) 42 N.C.J.Int'l.L.&Com.Reg. 933, 949.

[816] Ibid.

[817] Ibid.

[818] Ibid

[819] Ibid 981.

still elicit and therefore be part and parcel of a prohibited act of intervention […] any attempt by a state to manipulate foreign public opinion is widely considered to wrongfully interfere with democratic processes'.[820] Hollis suggests that 'the hackers did not just take the data and use it to inform their own policies or behavior',[821] but 'also leaked it, and did so in a way where the timing clearly sought to maximize attention (and corresponding impacts) on the U.S. domestic political campaign process. Perhaps we need to separate out this incident into two parts–the espionage (i.e., the hack itself) and the interference in the U.S. campaign using the fruits of that espionage'.[822] According to Banks, 'the Russian hack likely was not an internationally wrongful act', as '[t]he Russians exfiltrated and disseminated private information but did not tamper with voting machines or change votes'.[823] Consequently, 'there was no coercion and no unlawful intervention'.[824] According to Tallinn Manual 2.0, '[c]yber espionage per se, as distinct from the underlying acts that enable the espionage […] does not qualify as intervention because it lacks a coercive element'.[825]

Some other authors rely on the criteria of exclusive jurisdiction. According to Buchan, '[t]he recent practice of States' indicates 'that States exert sovereignty over information in cyberspace which belongs to entities and individuals over which they exercise jurisdiction'.[826] '[W]here this information is accessed and copied without authorization, an unlawful intervention occurs'.[827] Shull affirms that '[t]he principle of non-interference is often said to be a corollary of the

---

[820] Ibid 981-2.

[821] Duncan Hollis, 'Russia and the DNC Hack: What Future for a Duty of Non-Intervention?' (*Opinio Juris,* 25.07.2016) <http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/> accessed:25.11.2017.

[822] Ibid.

[823] William Banks, 'State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0' (2017) 95 Tex.L.Rev. 1487, 1501.

[824] Ibid.

[825] Schmitt, *Tallinn Manual 2.0* (n. 53) 323.

[826] Buchan, 'Cyber espionage and international law' (n.589)184.

[827] Ibid.

principle of state sovereignty', whose content 'should naturally follow' its 'contours'.[828] 'Thus, if the intrusion has the potential to significantly undermine the sovereign jurisdiction of a state, it should also offend the principle of non-interference'.[829]

Finally, some writings refer to non-intervention but disregard previously identified criteria. Jackamo thinks that 'global attention will now tend to focus on more subtle forms of intervention, such as [...] industrial espionage'.[830] Tsagourias also affirms that '[u]nder certain circumstances economic cyber-espionage can violate certain international law norms such as those of state-sovereignty and non-intervention'.[831] Lafouasse evokes the possibility that 'e-mails' interception of a government official could have led [...] to hold it as an unlawful interference in the internal affairs of a country'.[832]

In contrast, Hankinson calls 'the recent Russian cyber interference in the 2016 presidential election' a 'gray zone of international cyberspace law' which 'was successfully exploited'.[833] Fleck acknowledges that '[t]he question of whether and to what extent intelligence-gathering activities are wrongful *per se* remains ambivalent in international law. International law clearly prohibits intelligence gathering if coupled with additional elements, such as illegal intervention, breach of foreign sovereignty, or common crimes'.[834] Fidler thinks that '[a]lthough a

---

828 Aaron Shull, 'Cyber Espionage and International Law*',* 6 <api.ning.com/files/Ug-Ogup9PZ*wyVLXDplSNaUjM*f0HUBBaN*HklqwwORwnR7xopUarjsRlt7Db4H6M7Fa271aTs6Abfp4uYRTjlaVVpQwHEAV/giganet2013_Shull.pdf> accessed:17.05 2016.

829 Ibid 7.

830 Thomas Jackamo, 'From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary International Law of Non-Intervention' (1992) 32 Va.J.Int'l.L. 929, 938.

831 Nicholas Tsagourias, 'Economic cyber espionage and due diligence' (Syracuse University, 2015) 1 <insct.syr.edu/wp-content/uploads/2015/06/Tsagourias_Due_Diligence.pdf> accessed:16.09.2015.

832 Lafouasse, *L'Espionnage* (n.66) 169.

833 Olivia Hankinson, 'Due Diligence and the Grey Zones of International Cyberspace Laws' (*MJIL,* 2017) <www.mjilonline.org/due-diligence-and-the-gray-zones-of-international-cyberspace-laws/> accessed:21.02.2018.

834 Fleck (n.790) 708.

victim country could assert that spying violates the principles of sovereignty and non-intervention, state practice has accepted state-sponsored espionage such that these appeals are not serious claims'.[835]

In other words, examining the concepts of exclusive domestic jurisdiction, coercion or both of them allows authors to reach various conclusions, whether in favour or against cyber-espionage. The status of law is now ascertained, thanks to a joint examination of these concepts.

2. Status of law

As mentioned previously, a prohibited intervention implies methods of coercion (2.2) in a field under exclusive domestic jurisdiction (2.1). These two concepts are thus applied to cyber-espionage.

2.1. Exclusive domestic jurisdiction

Resolution 2625 referred to 'armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements', then added that '[e]very State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State'. However, *Nicaragua*'s 'exclusive domestic jurisdiction' downsized this scope. It did not confirm the first formula, but only echoed the second one. Accordingly, any State has the 'choice' of 'a political, economic, social and cultural system'. 'Choice' refers to '[t]he power, right, or faculty of choosing'.[836]

A 'political system' is 'the set of formal legal institutions that constitute a "government" or a "state"'.[837] The potential influence of intelligence activities

---

[835] David Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies' (*ASIL*, 17.03.2013) 2 <www.asil.org/sites/default/files/insight130320.pdf> accessed:17.01.2015.

[836] 'choice' (O.E.D.-Online, O.U.P. 2018).

[837] Alan Heslop, 'Political System' (*Britannica*)

on the free choice of a political system has been denounced by numerous states. According to the former French Interior Ministry, hacking during a presidential campaign is a danger for the country's 'capacity in organizing democratic debate in complete transparency and security' and the 'citizen's right to information'.[838] The SÄPO affirms that some intelligence activities 'serve to put Sweden in a position of dependence, so as to facilitate efforts to influence Sweden's actions',[839] while the government acknowledges that 'IT attacks could […] improperly influence the outcome of democratic elections.[840] Consequently, '[c]ountering the intelligence threat […] plays a pivotal role in maintaining Sweden's political, financial and military freedom of action'.[841] Switzerland considers the hacking of electronic processing systems as a potential intervention,[842] and its MP's similarly denounce risks of electoral manipulation and influence on the results.[843] The Netherlands affirms that '[p]olitical espionage undermines politics and government and is therefore a threat to the democratic legal order'.[844] Moreover, '[o]ther countries endeavour to acquire inside information through digital espionage concerning political decision-making, economic plans and Dutch standpoints and negotiation strategies in a variety of different areas. Using this information, a country can secretly try to

<www.britannica.com/topic/political-system> accessed:24.11.2017.

838 Sénat, 'Séance du 23 février 2017' (2017) CR No.20S, 1814 <www.senat.fr/seances/s201702/s20170223/s20170223.pdf> accessed:04.11.2017.

839 SAPO, *Swedish Security Service 2010* (Davidsons 2011) 18.

840 Prime Minister's Office, 'National Security Strategy' (2017) 18 <www.government.se/4aa5de/contentassets/0e04164d7eed462aa511ab03c890372e/national-security-strategy.pdf> accessed:03.02.2018.

841 SAPO, *Swedish Security Service 2010* (n.839) 18.

842 Caflisch, Pratique Suisse 2013 (n.690) 105.

843 National Council, 'Moratoire sur le vote électronique' (21.09.2017) 17.471 <www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170471> accessed:29.11.2017.

844 Ministry of Security and Justice (MSC)/National Cyber Security Centrum (NCSC), 'Cyber Security Assessment Netherlands 2016' (2016) 9 <www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2016/1/CSAN2016.pdf> accessed:01.11.2017.

influence the decision making on certain subjects so that a decision turns out favourably for that country'.[845]

Latvia criticizes '[t]hese activities […] aimed at changing public opinion and influencing Latvia's domestic political processes as well as discrediting our country and its officials and institutions'.[846] '[E]spionage against New Zealand today includes attempts to influence government policy'.[847] US Representative Raskin denounced 'a concerted effort by Vladimir Putin and his paid agents to commit cyber-espionage and sabotage of America's democratic institutions'.[848] Regarding traditional espionage, the sole invocation of non-intervention is to be found in the UNSC debate following the U-2 crash. The French delegate, Mr Berard, said that the qualification of aggression for such a flight was dubious but added: '[t]he incident of 1 May and the overflights denounced by the USSR Government really come within the category of intelligence activities. Undoubtedly they are regrettable and admittedly they imply interference in the internal affairs of a country'.[849]

An 'economic system' is 'a set of institutions for decision making and for the implementation of decisions concerning production, income, and consumption within a given geographic area'.[850] This domain may also be subject to influence. The director of the French National Cybersecurity Agency (ANSSI) denounced 'attempts of intervention and influence', and those who 'are eager to prevent' France 'from protecting its main economic and scientific interests'.[851] The latter

---

845 MSC/NCSC, 'Cyber Security Assessment Netherlands 2014' (2014) 70 <www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2014/1/Cyber%2BSecurity%2BAssessment%2BNetherlands%2B2014.pdf> accessed:01.11.2047.

846 Security Police, 'Annual report about the activities of the Security Police in 2015' (2016) 7 <http://dp.gov.lv/en/?rt=documents&ac=download&id=15> accessed:29.09.2016.

847 Michael Cullen and Patsy Reddy, 'Intelligence and Security in a Free Society' (2016) G.24a 27 <www.parliament.nz/resource/en-nz/51dbhoh_pap68536_1/64eeb7436d6fd817fb382a2005988c74dabd21fe> accessed:01.11.2017.

848 HoR, Committee on the Judiciary, No.HJU138000 (18.05.2017) 1079-1085.

849 UNSC, 858th Meeting (24.05.1960) [9].

850 Paul Gregory and Robert Stuart, *The Global Economy and Its Economic Systems* (Cengage 2013) 46.

851 AN, 'Compte rendu intégral' (13.04.2015)

indeed contribute to the 'country's competitiveness' and 'help creating numerous jobs'.[852] This was confirmed by the director of the Central Directorate of Interior Intelligence, as interference may be directed against French 'savoir-faire', 'jobs' and 'research'.[853] According to delegate Revel, 'trade secrets' are subject to 'interference and espionage'.[854] Switzerland describes attacks on banks' computer network as a potential intervention.[855]

A 'social system' is 'the patterned series of interrelationships existing between individuals, groups, and institutions and forming a coherent whole'.[856] Few references are made by states about hacking's impact on social systems. According to Estonia, '[o]ne of the main objectives of foreign security and intelligence services is to obtain information containing state secrets, thus allowing the respective foreign country to influence decision making on matters of sociopolitical, economic and military importance in line with its own interests'.[857]

As to influences on 'cultural system'–with 'culture' being defined as '[t]he distinctive ideas, customs, social behaviour, products, or way of life of a particular nation, society, people, or period'[858]–no such reference is to be found.

<www.assemblee-nationale.fr/14/cri/2014-2015/20150212.asp#P511027> accessed:03.11.2017.

[852] Ibid.

[853] AN, 'Audition de M. Patrick Calvar' (26.02.2013) CR No.59, 2 <www.assemblee-nationale.fr/14/pdf/cr-cdef/12-13/c1213059.pdf> accessed:26.11.2017;
See also AN, 'Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016' (02.03.2017) 35-7 <www2.assemblee-nationale.fr/static/14/DPR/i4573.pdf> accessed:02.11.2017.

[854] AN, 'Audition, ouverte à la presse, de M. Louis Schweitzer, commissaire général à l'investissement et Mme Claude Revel, déléguée interministérielle à l'intelligence économique' (16.12.2014) CR No.20, 4-5 <www.assemblee-nationale.fr/14/pdf/cr-eco/14-15/c1415020.pdf> accessed:02.11.2017.

[855] Caflisch, Pratique Suisse 2013 (n.690) 105.

[856] 'social system' (Merriam-Webster) <www.merriam-webster.com/dictionary/social%20system> accessed:05.11.2018.

[857] Security Police, 'Annual report about the activities of the Security Police in 2016' (2017) 9 <www.dp.gov.lv/en/?rt=documents&ac=download&id=20> accessed:05.10.2017.

[858] 'culture' (O.E.D-Online, O.U.P. 2018).

'Foreign policy' may be defined as 'the policy of a sovereign state in its interaction with other sovereign states'.[859] Yet, the information on the formulation of other states' foreign policy is an essential component for one's national security, and is highly valuable.

The protection of this 'political, economic, social and cultural system' is actually close to Western counter-intelligence agencies' spheres of competence. Most of them refer to the need to safeguard the democratic system: Estonia, Germany, the Netherlands etc.[860] In addition to this need, some also aim at protecting the States' economic well-being: Belgium, France, Spain, Switzerland, the UK etc.[861]

However–and with an ever-increasing growth in international law–less and less aspects of the states' 'political, economic, social and cultural system' remain under the state's exclusive domestic jurisdiction. Moreover, one can have doubts about the coercive nature of cyber-espionage.

2.2. Methods of coercion

As mentioned previously, spying may be directed against 'political, economic, social and cultural systems' which are under a state's exclusive jurisdiction. However, this is not enough to be illegal, as '[t]he element of coercion […] defines, and indeed forms the very essence of, prohibited intervention'.[862] Assimilating cyber-espionage to a prohibited intervention is actually bound to fail, as coercion is defined as the 'compulsion of a free agent by physical, moral, or economic force or threat of physical force'.[863] The French translation–'contrainte'–is even clearer, and may be defined as follows: '[a]ction de contraindre, de forcer quelqu'un à agir contre sa volonté; pression morale ou

[859] 'foreign policy' (Merriam-Webster) <www.merriam-webster.com/dictionary/foreign%20policy> accessed:06.11.2017.

[860] See part III.

[861] Ibid.

[862] *Nicaragua* (n.46) [205].

[863] Black's Law Dictionnary (Black's) (10th edn 2014), 'coercion'.

physique, violence exercée sur lui'.[864] Coercion thus implies that the state is forced to do–or to abstain from doing–something against its own will. At no moment is a state forced with cyber-espionage. This does not mean that cyber-espionage has no effect on its victim's behaviour; to combat cyber-espionage, a state may have to make diplomatic or legislative changes, take concrete measures etc. For instance, Denmark considers that, '[a]s hacker groups continuously perfect their technical skills and capabilities, state institutions will be forced to heighten their security levels and are thus engaged in a constant cyber-race'.[865] But nothing constrains it to act in such a way. Switzerland adopts the following reasoning: while 'spying is generally at odds with States' domestic law [...] international public law does not prohibit computer-network exploitation. By analogy with espionage, an operation targeting a computer network may be described as an "unfriendly act"'.[866]

In the sphere of competence of intelligence services, the necessity to prevent espionage is usually distinguished from the need to prevent more disruptive activities, such as threats to the independence or the democratic institutions. Such is the case in Belgium,[867] Canada,[868] Czech Republic,[869] Ghana,[870] Greece,[871]

---

[864] 'contrainte', (Larousse) <www.larousse.fr/dictionnaires/francais/contrainte/18670#pWqM8QLtC0uMc51R.99> accessed:05.12.2017.

[865] Centre for Cybersecurity (CFCS), 'The Cyber threat against Denmark' (2016) 4 <https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20-%20The%20cyber%20threat%20against%20Denmark.pdf> accessed:29.10.2017.

[866] Caflisch, Pratique Suisse 2013 (n.690) 106.

[867] Loi Organique des Services de Renseignement et de Sécurité ('L.R&S') (30.11.1998) MB 30.01.1999, 2827, arts 8(1)(a), 8(1)(g).

[868] Canadian Security Intelligence Service Act ('CSIS Act') RSC 1985 c C-23, s2.

[869] The Act on Intelligence Services of the Czech Republic ('BIS Act') (07.07.1994) No.153/1994, §5.

[870] The Security and Intelligence Agencies Act (1996) No.256, ss12(1)(c)-(d).

[871] Law on National Intelligence Service and other provisions ('Law No.3649') (03.03.2008) No.3649, FEK 132 A 39/3.03.2008, arts.4(1)(1), 4(1)(4).

Italy, [872] Kenya, [873] Luxembourg, [874] Mexico, [875] Montenegro, [876] Papua New-Guinea,[877] and Switzerland.[878] Sweden[879] also seems to share this view.

The case-law of the Canadian Federal Court in the *CSIS Act* case is of major interest. Justice Blanchard was asked to deliver a warrant, pursuant to articles 12 and 21 of the CSIS Act, whose goal was to intercept telecommunications outside Canada.[880] He concluded that the Court was 'without jurisdiction to issue the warrant sought',[881] and the application was dismissed. The fact that the 'intrusive activities that [were] contemplated in the warrant sought [were] activities that clearly impinge[d] upon […] principles of territorial sovereign equality and non-intervention' was decisive.[882] However, a subsequent ruling by Justice Mosley illuminates Blanchard's position.[883] According to article 21, pursuant to which the warrant was asked, 'the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose [...] to install, maintain or remove any thing'. [884] According to Justice Mosley, '[t]he 2007 warrant application before Justice Blanchard sought authority to install, maintain or

---

872 Law on Intelligence System for the Security of the Republic and new Provisions governing Secrecy ('Law 124/2007') (03.08.2007) No.124, OJ No.187 of 13.08.2007, ss6(1), 6(3).

873 National Intelligence Service Act 2012, s2(1) (interpretation of 'counter-surveillance' 'threat').

874 Loi portant réorganisation du Service de renseignement de l'État ('Loi SRE') (05.07.2016) A129, art.3(2).

875 Ley de Seguridad Nacional (2005) DOF 31-01-2005, arts.5(I)-(II), 5(IV).

876 Law on the National Security Agency (2015) No.08/15, art.14(1)-(5).

877 National Intelligence Organization Act 1984 ('NIO Act') s2 (interpretation of 'security').

878 Loi fédérale sur le Renseignement ('LRens') (25.09.2017) RO 2017, 4095ss, art.6; CP (Switzerland) title 13.

879 SAPO, *Swedish Security Service 2013* (Edita 2014) 23.

880 Federal Court, *Re Canadian Security Intelligence Service Act* (2007) 2008 FC 301

881 Ibid [71].

882 Ibid [50].

883 Federal Court, *Re Canadian Security Intelligence Service Act* (2009) 2009 FC 1058, [46].

884 CSIS Act, art.21(3)(c).

remove anything required [text omitted]. It is clear from the warrant application itself and from Justice Blanchard's reasons that this was intended to include the authority to [text omitted] in the foreign jurisdictions in order to install the means by which the communications, information and records [text omitted]'.[885] He added that 'the application before Justice Blanchard contemplated intrusive activities in foreign jurisdictions', which were 'not being sought in the present application'.[886] Some parts of the provisions remain classified ('text omitted'), but it can be understood that a territorial intrusion 'in the foreign jurisdictions' was necessary, 'in order to install the means' of surveillance.[887] This is even more obvious when it was mentioned that '[t]he norms of territorial sovereignty do not preclude the collection of information by one nation in the territory of another country, in contrast to the exercise of its enforcement jurisdiction'.[888] Justice Mosley then affirmed that, '[a]s Professor Jack Goldsmith argues in *The Internet and the Legitimacy of Remote Cross-Border Searches* […] technological innovation has simply made it easier to do this without physically crossing borders'.[889] Yet, in this article, Goldsmith affirms that cyber-espionage is lawful in international law.[890] Justice Mosley also referred to the Convention on Cybercrime, mentioning that 'it is not intended to affect measures taken by the subscribing parties to protect their national security'.[891] Justice Mosley concluded that 'Canada has given CSE a mandate to collect foreign intelligence including information from communications and information technology systems and networks abroad [...] CSIS is authorized to collect threat related information about Canadian persons and others and, as discussed above, is not subject to a territorial limitation'.[892]

---

[885] *Re Canadian Security Intelligence Service Act* (n.883) [43].

[886] Ibid [65].

[887] This interpretation is shared by Van Ert. See Gib Van Ert, 'Canadian Cases in Public International Law in 2009-10' (2010) 48 Canadian Y.B.I.L. 493, 497-501.

[888] *Re Canadian Security Intelligence Service Act* (n.883) [74].

[889] Ibid [74].

[890] Goldsmith (n.596) 11.

[891] *Re Canadian Security Intelligence Service Act* (n.883) [72].

[892] Ibid [75]. Navarette subsequently concludes that 'a general conclusion that may be drawn [...] is that the rule of territoriality for purpose of execution does not, in its present state, prohibits

As of today, cyber-espionage has only been described as a foreign intervention by North Korea. Regarding 'the massive electronic surveillance activities conducted by' the USA, North Korea declared that 'massive espionage activities were targeting Heads of State, who were symbols of State sovereignty, resulting in rampant violations and interference in internal affairs'.[893]

Some ambiguities may be found in some instances of state practice. Australian legislation considers that 'acts of foreign interference' may be carried on for purposes of 'intelligence' and 'affecting political or governmental processes', or include activities that 'are otherwise detrimental to the interests of Australia'.[894] Denmark calls 'hack-and-leak-operation[s]' an 'ambition to influence internal affairs in other countries'.[895] However, these qualifications do not automatically equate to the notion of prohibited intervention in international law, thus maintaining the mystery. As Switzerland puts it, there is a 'limit between the lawful influence and the unlawful constraint'.[896] The New Zealand Security Intelligence Service (NZSIS) sometimes use 'espionage' and 'foreign interference' interchangeably,[897] other times it distinguishes them.[898] The Dutch position is paradoxical. On the one hand, the Netherlands considers that

---

cyber reconnaissance or the transnational interception of communications'. See Navarette (n.708) 35.

893 UN Press Release GA/SHC/4094 (n.665).

894 Australian Security Intelligence Organisation Act 1979, s4.

895 CFCS, 'The Cyber threat against Denmark' (2017) 5 <https://fe-ddis.dk/cfcs/CFCSDocuments/The%20cyber%20threat%20against%20Denmark%202017.pdf> accessed:29.10.2017.

896 Federal Department of Justice and Police/DFAE, 'Avis de droit sur les bases légales des opérations dans les réseaux informatiques par les services du DDPS' (2009) 204 <www.parlament.ch/centers/documents/fr/gutachten-ejpd-computernetz-vbs-2009-03-10-f.pdf> accessed:10.11.2017.

897 NZSIS, 'Annual Report for the year ended 30 June 2014' (2014) G.35, 11 <www.nzsis.govt.nz/assets/media/annual-reports/nzsis-ar14.pdf> accessed:01.11.2017; NZSIS, 'Annual Report for the year ended 30 June 2013' (2013) G.35, 25 <www.nzsis.govt.nz/assets/media/annual-reports/nzsis-ar13.pdf> accessed:01.11.2017.

898 NZSIS, '2016 Annual Report' (2016) G.35, 16 <www.nzsis.govt.nz/assets/media/annual-reports/nzsis-ar16.pdf> accessed:01.11.2017.

'[p]olitical espionage undermines political and governmental authority and is therefore a threat to the democratic legal order'.[899] On the other hand, it considers that 'state actors are using digital resources for the purpose of exerting influence and engaging in sabotage and espionage'.[900]

Divulgence of obtained information is, however, more problematic, and various reactions have been prompted by Russia's interference in the American elections. French MFA Ayrault said at the Parliament that any foreign interference in the presidential campaign of 2017 would be 'a breach of the principle of non-intervention' that could justify 'retaliatory measures'.[901] He added that 'no foreign power is allowed to influence Frenchmen's choice, no foreign power is allowed to choose the next President of the Republic'.[902] By contrast, Obama referred to 'Russia's efforts to undermine established international norms of behavior, and interfere with democratic governance'.[903] As suggested by Goodman, '[a]ll official statements by the Obama administration appear to include a studied avoidance of whether the Russian actions do or do not violate international law [...] It is safe to assume the specific word choice in the President's statement is highly deliberate'.[904] As to State Department Legal Adviser Brian Egan, he explicitly referred to the *Nicaragua*

---

899 MSC, 'Cyber Security Assessment Netherlands' (n.844) 9.

900 Dutch Government, 'Building Digital Bridges' (2017) AVT17/BZ122203, 3 <www.government.nl/binaries/government/documents/parliamentary-documents/2017/02/12/international-cyber-strategy/International+Cyber+Strategy.pdf> accessed:01.11.2017.

901 Martin Untersinger, 'Cyberattaques: la France menace de « mesures de rétorsion » tout Etat qui interférerait dans l'élection', *Le Monde* (15.02.2017) <www.lemonde.fr/pixels/article/2017/02/15/cyberattaques-la-france-menace-de-mesures-de-retorsion-tout-etat-qui-interfererait-dans-l-election_5080323_4408996.html> accessed:14.04.2017.

902 Ibid.

903 The White House, 'Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment' (29.12.2016) <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity> accessed:03.10.2017.

904 Ryan Goodman, 'International Law and the US Response to Russian Election Interference', (*Just Security, 2017*) <www.justsecurity.org/35999/international-law-response-russian-election-interference/> accessed:25.11.2017.

case and affirmed that 'States' cyber activities could run afoul of this prohibition'.[905] According to him, 'a cyber-operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention'. [906] However, none of these behaviours actually describe the Russian activities. The UK has a similar approach, considering that acts such as 'the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state, intervention in the fundamental operation of Parliament, or in the stability of our financial system' must 'surely be a breach of the prohibition on intervention in the domestic affairs of states'.[907]

3. Conclusion

Whether physical or not, materialised or dematerialised, espionage *per se* cannot be considered a prohibited intervention. States indeed acknowledge that foreign intelligence services seek to influence their political, economic and social systems, and cyber-espionage indeed interferes with them. Yet, none of them has ever pretended that cyber-spying was coercive. This element is lacking from the mere information collection, as the state is not constrained to act in any way.[908] It is however necessary to distinguish between information gathering and its leak, which constitute separate actions. The latter–as during the 2016 American elections–is a different activity and a more controversial issue. Both

---

[905] Egan (n.61).

[906] Ibid.

[907] AGO (n.88).

[908] When 'documents, data and other property which belongs to Timor-Leste and/or which Timor-Leste has the right to protect under international law' were seized by Australian agents in the offices of Timor-Leste's legal adviser in the Australian Capital Territory, Timor-Leste itself invoked a more specific 'right of confidentiality and non-interference with the communications between States and their legal advisers'. The inviolability of a State's property and '[t]he principle of good faith in the conduct of international negotiations and proceedings' were also invoked. See *Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia)* (Memorial of Timor-Leste) [2014] [1.2, 6.2, 6.15-6.23] <www.icj-cij.org/files/case-related/156/18699.pdf> accessed:12.01.2016.

the Czech Republic and Lithuania describe them as 'information operations'[909] or 'the dissemination of information which incites to change the constitutional order […] by force'.[910] Their goal is indeed to influence voters' behaviour, not directly manipulating the elections' results. Similar activities involving the 'spotlight' of 'some videos thanks to technical process' on 'social networks' were described by ANSSI director Poupard as 'modification influence'.[911] According to him, authors 'play with rules, there is no cyber-attack *per se*'.[912] Besides, at no point has the American government described the Russian action as a prohibited intervention, and it is difficult to prove any form of constraint on electors.

[909] Czech Security Information Service (BIS), 'Annual Report of the Security Information Service for 2015' (2016) 9
<www.bis.cz/vyrocni-zpravaEN890a.html?ArticleID=1104> accessed:16.11.2017.

[910] Lithuanian MND, 'National Security Strategy' (2016) 13
<https://kam.lt/download/57457/2017-nacsaugstrategijaen.pdf> accessed:21.06.2018.

[911] Senat, 'Cyberinterférences dans les processus électoraux–Audition de M. Guillaume Poupard' (01.02.2017)
<www.senat.fr/compte-rendu-commissions/20170130/etr.html#toc2> accessed:04.11.2017.

[912] Ibid.

III – JUS AD BELLUM

Is intelligence gathering an enemy of territorial integrity or an ally of peace preservation? On the one hand, article 2(4) of the UN Charter mentions that '[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations'. In parallel, article 51 mentions that '[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security […]'. On the other hand, the opinion of governments is well-reflected in the words of Richard Helms, the former Director of Central Intelligence: 'I was, and still am, convinced that there is no greater threat to world peace than poorly informed or misinformed leaders and governments […] The first line of defense remains a competent intelligence service'.[913] While decried, espionage could ultimately serve international peace. The relationship between this activity and JAB, which is now embodied in the UN Charter, is thus interesting. The use of force is usually described as the resort to armed or military force by a state, directed against the territory, ship or aircraft of another state,[914] and their most severe forms are called 'armed attacks' and give rise to an authorization of self-defence. Yet, many of the terms used in articles 2(4) and 51 are left undefined, thus allowing many extrapolations about their scope–including their potential application to cyberspace and cyber-intrusions.

A preliminary study of state practice reveals that a majority of states consider the UN Charter as applicable in cyberspace. This is also the conclusion reached by the UNGGE.[915] In their answers to the UNGGE, the UN Charter is deemed to

[913] Charles Lathrop, *The Literary Spy* (Y.U.P. 2004) 208.

[914] Oliver Dörr, 'Use of Force, Prohibition of' (2011) M.P.E.P.I.L., [11], [24].

[915] UNGA, 'Developments in the field of information and telecommunications in the context of international security' (22.07.2015) UN-Doc A/70/174, 12.

be applicable in cyberspace by Australia,[916] Canada,[917] Georgia,[918] Germany,[919] Norway,[920] Qatar,[921] and Sweden.[922] The USA, Denmark, Finland, Iceland, Norway, and Sweden 'affirm that existing international law, in particular the UN Charter, applies to state conduct in cyberspace'.[923] Russia proposes to strengthen '[c]yberspace security' in accordance with 'the UN Charter provisions'.[924] Moreover, the Russian armed forces 'are guided' by 'non-use of force or threat of force' and the 'right to the individual or collective self-defence'.[925] In their code of conduct, China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan pledge 'to comply with the Charter of the United Nations' in cyberspace.[926] While China is opposed to the application of self-defence in response to cyber-attacks,[927] it 'holds that information technology should be used in accordance with the Charter of the United Nations and the basic principles of international relations [...]'.[928] 'Japan is of the view that existing international law, including the U.N. Charter [...] naturally applies to acts in

---

916 UNGA, 'Developments' (30.06.2014) (n.95) 2. UNGA, 'Developments' (15.07.2011) (n.141) 6.

917 Canada, 'Developments' (n.91) [2].

918 Georgia, 'UN General Assembly Resolution 68/243' (n.92) 5-6.

919 Germany, '"Report on Developments in the Field of Information and Telecommunications in the Context of International Security" (RES 69/28)' (2015) 1 <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/08/GermanyISinfull.pdf> accessed:25.06.2018.

920 UNGA, 'Developments' (11.08.2017) (n.675) 20.

921 UNGA, 'Developments in the field of information and telecommunications in the context of international security–Report of the Secretary-General' (20.07.2010) UN-Doc A/65/154, 9.

922 Sweden, 'Submission by Sweden to UNGA resolution 68/243' (n.96) 6

923 'US–Nordic Leaders' Summit, Joint Statement' (n.731).

924 Russian MOD (n.85) [3.1]

925 Ibid.

926 UNGA, 'Letter dated 9 January 2015' (n.143) 4.

927 AN, 'Audition de M. Gérard Araud, représentant permanent de la France auprès des Nations Unies' (12.06.2013) CR No.71, 11 <www.assemblee-nationale.fr/14/pdf/cr-cafe/12-13/c1213071.pdf> accessed:02.11.2017.

928 UNGA, 'Developments in the field of information and telecommunications in the context of international security' (02.07.2007) UN-Doc A/62/98, 7.

cyberspace'.[929] The UK thinks that the rules surrounding the use of force are applicable in cyberspace.[930] 'When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense […]'.[931] Slovakia mentions that '[t]he misuse of cyberspace can become one of the ways of waging war'.[932] Croatian '[n]ational interest and all the necessary activities will be pursued according to the principles, values and obligations based on […] the Charter of the United Nations'.[933] Malta considers it has the right to protect its own territory and infrastructures from aggressions, and thus, 'to defend its cyber-space territory'.[934] Cyber-space is no exception. The applicability of the UN charter is also acknowledged by Chile,[935] and Mexico.[936]

Some states share the particularity of acknowledging the applicability of the UN Charter and, in parallel, exposing the limits of this approach. Canada affirms that '[m]uch like the procurement system, the laws of warfare struggle to keep pace with current technology. Alternate means of modern warfare, such as cyber-attack or the use of unmanned robotic systems, are not addressed in the United Nations Charter. There is probably a need to revisit the existing provisions in international law'.[937] According to Japan, 'the international community has

---

929 ISPC, 'International Strategy on Cybersecurity Cooperation' (2013) [4.3.2] <www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf> accessed:23.08.2016.

930 Foreign and Commonwealth Office (FCO), 'Response to General Assembly resolution 71/28 "Developments in the field of information and telecommunications in the context of international security"' (2017) 7-8 <https://s3.amazonaws.com/unoda-web/wp-content/uploads/2017/09/UK-ES-and-full.pdf> accessed:24.06.2018.

931 The White House, 'International Strategy for Cyberspace' (n.84) 14.

932 Slovakian MOD, 'The White Paper on Defence of the Slovak Republic' (2013) [52] <www.mosr.sk/data/WP2013.pdf> accessed:15.05.2016.

933 Croatia, 'Croatian National Cyber Security Strategy' (2015) OG 108/2015, 23 <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf> accessed:13.09.2016.

934 MCDMS (n.127) 21.

935 Chilean MND, 'Aprueba' (n.103) 4.

936 Presidencia, 'CLAN 2016' (n.98).

diverging views concerning the fundamental matters of cyberspace, including how international law applies'. [938] It evokes the UNGGE works before underlining that they merely contain 'recommendations on how to apply the principles of international law to acts using cyberspace and on voluntary, non-binding norms of state behavior'.[939] Indeed, 'there is still no wide consensus on norms covering the conduct of states and international cooperation in cyberspace'.[940] Finland notes that '[t]he great powers equate cyber-attacks with military action which can be met with any available means',[941] but underlines that '[a]t present, the international community is debating whether cyberattacks in some situations can rise above the threshold of armed attack, as defined in the UN Charter'.[942]

The French position is even more destabilizing. On the one hand, France 'welcomes the GGE's acknowledgement that international law is applicable in cyberspace, including [...] the Charter of the United Nations [...]'.[943] On the other hand, in a 2013 White Paper approved by President Hollande the 'relative inadequacy of the instruments of global governance' was highlighted,[944] as 'the principles underpinning the international order need[ed] to be clarified and consolidated'.[945] After having underlined that the army should not be the sole entity to deal with cyber-governance, ANSSI director Poupard called for a global

---

[937] Canadian Army Land Warfare Centre, *No man's land: tech considerations for Canada's future army* (National Defence 2014) 2-37, 2-38.

[938] Japanese MOD, 'Defence of Japan 2016' (2016) 155 <www.mod.go.jp/e/publ/w_paper/pdf/2016/DOJ2016_1-3-5_web.pdf> accessed:15.05.2017.

[939] Ibid 155-6.

[940] Japanese MOD, 'Defence of Japan 2014' (2014) 111 <www.mod.go.jp/e/publ/w_paper/pdf/2014/DOJ2014_1-2-5_web_1031.pdf> accessed:15.05.2017.

[941] DEFMIN (n.106) 17.

[942] Ibid 33.

[943] 'Réponse de la France à la résolution 68/243 relative aux « Développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale » (2014) [3] <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/10/France.pdf> accessed:30.05.2016.

[944] Commission du livre blanc, *French White Paper* (n.699) 31.

[945] Ibid.

reflexion on applicable rules. He then highlighted that '[a]s of today, there are no commonly accepted rules, and nobody infringes them in any manner'.[946] He had previously called cyberspace a 'Far-West',[947] affirming that international rules remained to be established in cyberspace.[948]

In contrast, Spain 'considers that States should continue reflecting on how the principles and norms of international law should be interpreted and applied in cyberspace; especially those relating to the threat or use of force [...].[949] Ukraine asked for 'international legal instruments' that would contain 'regulation of issues related to cyberwar, cyber-aggression […]'.[950]

Bearing this panorama in mind, it is necessary to focus on cyber-espionage, in terms of its status in doctrine (1), and in law (2). A conclusion is then available (3).

1. Status of doctrine

Doctrine about espionage (1.1) and cyber-espionage (1.2) has to be alternatively analysed.

---

946 Sénat, 'Comptes-Rendus de la Commission des Affaires Etrangères, de la Défense et des Forces Armées' (1.02.2017)
<www.senat.fr/compte-rendu-commissions/20170130/etr.html> accessed:30.10.2017.

947 Martin Untersinger, 'Cybersécurité: pour Jean-Yves Le Drian, "la menace est à nos portes"', *Le Monde* (25.01.2017)
<www.lemonde.fr/pixels/article/2017/01/25/cybersecurite-menaces-averees-ou-marketing-de-la-peur_5068669_4408996.html> accessed:18.05.2017.

948 'Guillaume Poupard: « Il faut établir le droit international dans le cyberespace »' (*France24,* 03.04.2017)
<www.youtube.com/watch?v=4qEq0AR-GzI> accessed:14.05.2017;
Sénat, 'Comptes-Rendus de la Commission des Affaires Etrangères, de la Défense et des Forces Armées' (01.02.2017)
<http://www.senat.fr/compte-rendu-commissions/20170130/etr.html> accessed:18.05.2017.

949 UNGA, 'Developments in the field of information and telecommunications in the context of international security–Report of the Secretary-General' (22.07.2015) UN-Doc A/70/172, 13.

950 UNGA, 'Developments' (2013) (n.87) 14.

1.1. Espionage

A considerable amount of work has been devoted to the relationship between cyber-espionage and the use of force. This interest is a recent phenomenon, as few authors analyse traditional spying in light of the UN Charter, and essentially in late works. In this vein, Blake and Imburgia argue that 'the international community generally has not characterized spying, intelligence and related activities as a "threat or use of force"'. [951] This position is shared by Weissbrodt.[952] While contending that 'particular forms of espionage may give rise to the use of force', Scott acknowledges in parallel that '[t]he right of self-defense may also justify the collection of intelligence'.[953] Lubin defines a 'Jus Ad Explorationem' that can 'be read into the Charter Article 51 global security structure'.[954] It means that 'to the extent that a specific intelligence gathering activity can be shown to serve either the short-term national security interest of a particular state, or the long-term goals of international stability and international peace and security, that operation would surely comply with the Charter, and indeed most operations do'.[955]

1.2. Cyber-Espionage

Rather than resorting to Vienna Convention rules of interpretation, a majority of authors has elaborated specific meta-rules when it comes to cyber-threats. The application of these meta-rules–which may be defined as 'rule[s] governing the content, form or application of other rules'[956]–is studied in the first instance

---

[951] Duncan Blake and Joseph Imburgia, "'Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of defining them as "Weapons"' (2010) 66 A.F.L.R. 157, 186.

[952] David Weissbrodt, 'Cyber-Conflict, Cyber-Crime, and Cyber-Espionage' (2013) 22 Minn.J.Int'l.L. 347, 371.

[953] Scott (n.787) 224

[954] Asaf Lubin, 'Espionage as a Sovereign Right under International Law and its Limits' (2016) 24(3) I.L.S.A. Quarterly 22, 26.

[955] Ibid.

[956] 'Meta-rule' (Oxford Living Dictionary) <en.oxforddictionaries.com/definition/us/metarule> accessed:15.04.2017.

(A). A more traditional approach–based on the initial will of states or their subsequent practice–is yet still used by a minority (B).

A. Arguments based on meta-principles of interpretation

Among meta-principles of interpretation, the consequentialist–or effect-based approach–is the mainstream trend regarding the application of the UN Charter (a). To a lesser extent, analogy (b), and a target-based approach (c) also appear.

a. Arguments based on a consequentialist and effects-based approach

Doctrine systematically studies cyber-attacks and cyber-espionage through the prism of the UN Charter. Lacking a physical intrusion, it has been proposed to evaluate the consequences of the cyber-operation, rather than the presence of an armed attack *stricto sensu*. Two trends exist: focusing either on the effects in the virtual space (i) or the consequences in the physical space (ii). Some authors also consider economic espionage as a specific issue (iii).

i. Arguments based on the effects in the virtual space

Hanford explains that '[s]cholars argue that cyber espionage fails to constitute a cyber-attack, because the operation fails to disrupt or destroy a computer network. Additionally, states fail to claim that cyber-espionage constitutes a prohibited use of force'.[957] Gervais claims that 'cyber-espionage and exploitation fails to rise to the level of warfare because the purpose or outcome of both cyber-espionage and exploitation is to monitor information and not to affect a computer system's functionality'.[958] Watts argues that '[r]ather than disrupt the

---

For a discussion on meta-rules of interpretation, see: Bradley Shingleton, 'Law, Principle and the Global Ethics' in Bradley Shingleton and Eberhard Stilz (eds), *The Global Ethic and Law: Intersections and Interactions* (Bloomsbury 2016) 53-5.

[957] Elizabeth Hanford, 'The Cold War of Cyber Espionage' (2014) 20(1) P.I.L.R. 22, 24.

[958] Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) J.L.&Cyber Warfare 8, 24.

target system, CNE tools merely collect information and report to their handler'.[959] For similar reasons, Schaap affirms that they 'should not be considered cyber warfare operations'.[960] As cyber-exploitation does not affect the functionality of the system, amend or delete resident data, Roscini also considers it never amounts to the use of force.[961]

In their reasoning, the crucial point is that espionage cannot be a cyber-attack–and, as a consequence, use of force–because it fails to 'disrupt', 'destroy' or does not 'affect' the 'functionality' of computers and data. A clear distinction is thus drawn between the destructive cyber-attacks and the non-destructive cyber-espionage. As mentioned in the introduction, this taxonomy is the one favoured by the doctrine of the US armed forces. It is worth mentioning that the initial definition proposed by the American Navy in 1995 referred to the intent behind the action. At that time, an 'electronic attack' involved 'the use of electromagnetic or directed energy to attack personnel, facilities, and/or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability'.[962]

ii. Arguments based on the effects in the physical space

According to Buchan, both the Tallinn Manual and '[c]ommentators have [...] argued that Article 2(4) should be reinterpreted so as to apply to cyber-attacks which although not manifesting physical harm nevertheless cause damage and disruption equivalent to a kinetic attack'.[963] Lacking such consequences, he affirms that cyber-espionage is neither use of force, nor an armed attack.[964]

---

[959] Sean Watts, 'Combatant Status and Computer Network Attack' (2010) 50 Va.J.Int'l.L. 391, 400.

[960] Schaap (n.159) 139.

[961] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (O.U.P. 2014) 65.

[962] Department of the Navy, 'Implementing Instruction for Information Warfare Command and Control Warfare' (18.01.1995) 3420.260, Enclosure 2, 2. <www.hsdl.org/?view&did=439853> accessed:20.04.2016.

[963] Buchan, 'Cyber espionage and international law' (n.589) 187.

[964] Ibid.

Weissbrodt affirms that 'Flame [a spying malware] does not– in its present state– constitute a use of force because it does not have any potential to do damage'.[965] Solis mentions that 'reference to fatalities and property destruction suggests an objective guide for determining when a cyber-operation constitutes a cyber-attack'.[966] Weissbrodt[967] and Solis[968] both conclude that cyber-espionage does not allow responding with the use of armed force. Shackleford and Andres think that '[n]either cybercrime nor espionage can rise to the level of an act of war, even with State complicity'.[969] Following Dinstein's position which is that violent effects are necessary, Blank concludes that, 'hacking into an enemy computer to gather intelligence to be used in the launching of an attack' does not qualify as cyber-attack.[970] Wortham affirms that, '[w]hile a cyber-attack can constitute a use of force if the effects are such that they traditionally would have been achieved through a kinetic attack, cyber-exploitation is regarded differently'.[971] She then suggests that, '[u]nder the current legal structure, cyber-exploitation by itself seems to clearly never constitute a use of force […] most countries consider cyber-exploitation a new form of espionage, and espionage traditionally does not constitute a use of force'.[972] However, 'perhaps the combination of an identified vulnerability and other intelligence information that shows the likelihood of a future attack would be able to constitute a threat of force'.[973] Roscini also considers that 'stealing sensitive military information by penetrating into the ministry of defence's computers when "no immediate loss of life or destruction

---

965 Weissbrodt (n.952) 381.

966 Gary Solis, 'Cyber Warfare' (2014) Mil.L.Rev. 1, 12.

967 Weissbrodt (n.952) 381.

968 Gary Solis, 'Cyber Warfare' (n.966) 11.

969 Scott Shackelford and Richard Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2011) 42 Geo.J.Int'l.L. 971, 980.

970 Laurie Blank, 'International Law and Cyber Threats from Non-State Actors' (2013) 89 I.L.S. 406, 430.

971 Wortham (n.233) 655.

972 Ibid.

973 Ibid 656.

results" does not qualify as an armed attack'.[974] Watts suggests that 'cyber-theft, cyber-espionage, cyber-exploitation, and mere disruptions of service, even if committed in connection with an armed conflict, fail to rise to the level of attack at all and therefore do not implicate the prohibition of perfidy'.[975] Poché evokes Stuxnet as follows: '[h]ad the "spies and unwitting accomplices" only inserted information-gathering tools, this would have been an act of simple espionage presumed legal under international law. However, the aim was to produce destructive results akin to bombing or planting explosives. This nullifies any presumptive legality argument'.[976] Roberts recommends that 'the U.S. should favor a more expansive interpretation of the Charter with respect to cyber warfare'.[977] Cyber-espionage 'would not create the effects necessary to reach the threshold of "force" or "armed attack"', and '[t]he result would be that the U.S. could continue engaging in information-gathering and other beneficial national security measures without violating international war law'.[978] Waxman adopts a similar position.[979]

In this type of position, the crucial point is that espionage is not a use of force because it fails to have consequences similar to those of an armed attack. Emphasis is placed on the effects in the physical world: loss of life, injury, or destruction of property.

An interesting parallel may be drawn with the original definition of 'information operations' proposed by the Office of General Counsel (OGC) in 1999, as well as positions adopted by Dinstein, Sharp and Schmitt between 1999 and 2002. The OGC indeed acknowledged that '[i]t is by no means clear what information

---

974 Roscini (n.961) 71.

975 Sean Watts, 'Law-of-War Perfidy' (2014) Mil.L.Rev. 106, 169-70.

976 Charles Poché, 'This means War! (Maybe?): Clarifying Casus Belli in Cyberspace' (2013) 15 Or.Rev.Int'l.L. 413, 432-3.

977 Shaun Roberts, 'Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors' (2014) 41(3) N.Ky.L.Rev. 535, 565.

978 Ibid.

979 Matthew Waxman, 'Cyber Attacks as "Force" under UN Charter Article 2(4)' (2011) 87 I.L.S. 43, 48.

operations techniques will end up being considered to be "weapons," or what kinds of information operations will be considered to constitute armed conflict'.[980] However, '[i]f the deliberate actions of one belligerent cause injury, death, damage, and destruction to the military forces, citizens, and property of the other belligerent, those actions are likely to be judged by applying traditional law of war principles'.[981] According to Sharp, '[a]ny computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce the effects of an armed attack prompting the right of self-defense'.[982] Dinstein affirmed in 2002 that 'the crux of the matter is not the medium at hand […] but the violent consequences of the action taken',[983] and acknowledged eleven years later that 'a cyber-operation does not pass muster as an "attack" if it is limited to [...] intelligence gathering'.[984] According to Schmitt, '[c]omputer network attack is new wine in old bottles',[985] but 'it becomes necessary to shift cognitive approach if one wishes to continue to operate within the existing framework'.[986] He recommended '[a] useful approach': 'to dispense with instrument-based criteria in lieu of consequence-based standards'.[987] He affirmed that '[t]his seeming dissonance between the ultimate Charter goals and the prescriptive norms designed to achieve them is the product of a very rational cost-benefit analysis. Although the international community is in fact concerned with consequences of an action, fashioning an easily applied consequence-based standard would have been difficult. As a result, a form of prescriptive shorthand

---

[980] DoD/OGC, 'An Assessment' (n.676) 8.

[981] Ibid.

[982] Sharp (n.598) 133.

[983] Yoram Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 I.L.S. 99, 103.

[984] Yoram Dinstein, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference' (2013) 89 I.L.S. 276, 284.

[985] Michael Schmitt, 'Computer Network Attack: The Normative Software' (2011) 4 Y.B.I.HL. 53, 55.

[986] Michael Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Col.J.T.L. 885, 913.

[987] Schmitt, 'Computer Network Attack' (n.985) 63.

has been employed in the Charter'.[988] He finally proposed his seven criteria to determine whether a computer-network operation (CNO) amounts to use of force: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, responsibility.[989] Most of them are now incorporated in Tallinn Manual 2.0,[990] which mentions that '[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force'.[991]

iii. Arguments based on the specificity of economic espionage

Some scholars apply the UN Charter to economic espionage. Barkham confesses that '[u]nder a traditional Article 2(4) analysis, there would be no weapon used and no property destroyed, so the act would not be a use of force'.[992] He nevertheless affirms that 'applying the consequence-based approach, the attack on the company (and by extension the company's home state) would appear to be a use of force'.[993] According to Brenner and Crescenzi, 'the long term national security implications (a decline in economic competitiveness) stemming from the systemic theft of intellectual property has consequences no less serious than a real-world terrorist attack'.[994] They then affirm that '[e]conomic espionage is often characterized as a type of warfare; while it does not involve a physical attack upon a nation-state's territory, it does represent an attack by one sovereign upon the essential interests of another' and 'an attempt to undermine the security and stability of a sovereign nation'.[995] 'Though economic espionage is, in certain

[988] Ibid.

[989] Ibid 63-5.

[990] Schmitt, *Tallinn Manual 2.0* (n.53) 334-6.

[991] Ibid 330.

[992] Barkham (n.233) 90.

[993] Ibid.

[994] Susan Brenner and Anthony Crescenzi, 'State-Sponsored Crime: The Futility of the Economic Espionage Act' (2006) 28 Hous.J.Int'l.L. 389, 390-1.

[995] Ibid 449.

senses, analogous to an act of war, it is unlikely that countries will treat it as an act of warfare'.[996] According to Melnitzky, '[…] once it is accepted that an armed attack can occur without physical damage, to limit the use of active defenses to cyber "attacks"–the corruption of data–as opposed to cyber "espionage"–the theft of data–is an overly mechanical distinction […]'.[997] Cyber-espionage can indeed be quickly changed into an attack, and 'should be treated as a potential one from the outset'.[998] He thinks that this approach's requirement is 'that a cyberattack must cause damage only previously possible by traditional military force'.[999] 'Chinese cyber-espionage against the United States has reached such a massive scale that it more closely resembles an act of looting, which before the Internet could have only occurred coupled with military occupation, rather than a series of criminal acts'.[1000] As a consequence, some particular forms of espionage–including by computer–may raise issues of self-defence.[1001]

The three previous forms of reasoning may be qualified as consequentialist, as they rely on the effects of an operation for the purpose of applying the UN Charter. It is however not the only type of meta-principles used, as analogy also appears in doctrinal works.

b. Arguments based on analogical reasoning

Traditional espionage is usually considered a violation of domestic law, rather than international law. Most of analogies related to cyber-spying describe it as a form of espionage, which is consequently not unlawful in international law. According to Gervais, '[t]he goal of cyber exploitation is to obtain information

996 Ibid footnote 254.

997 Alexander Melnitzky, 'Defending America against Chinese Cyber Espionage through the Use of Active Defences' (2012) 20 Cardozo J.Int'l.&Comp.L. 537, 567.

998 Ibid 566.

999 Ibid.

1000 Ibid 539.

1001 Ibid 564-5.

from a computer network without the user's knowledge, which amounts to a modern form of espionage'.[1002] Yet, '[e]spionage is illegal under the domestic laws of most nations, but it is not illegal under international law' and 'it does not violate international laws of war'. [1003] Roscini thinks that '[s]ome cyber-exploitation operations are a contemporary form of military reconnaissance or espionage. It should be recalled that espionage is not prohibited by international law, although it is usually criminalized at domestic level'. [1004] Kostadinov says that in '[t]he international community predominates the opinion that cyber-exploitation is the modern equivalent of the good old spying, which is usually not considered a use of force'.[1005] According to Lotrionte, cyber-espionage 'constitutes the acquisition of information to inform policymakers about actual or potential threats, and does not rise to the level of a use of force or armed attack under international law'.[1006] If 'in line with the same objectives of traditional espionage', it 'may be seen as acceptable state practice'.[1007] It is thus 'another form of technology-enabled espionage or intelligence collection and as such is distinguishable from other intelligence functions that are more equivalent to low-intensity conflict'.[1008] Beard thinks that 'such acts are widely recognized as lying outside *jus ad bellum*'.[1009] Lobel similarly assesses that '[a] CNE is a form of espionage and, as in the physical domain, is not barred by the law of war but rather by domestic law'.[1010] Schmitt also supports this approach, as '[…] cyber exploitation is a pervasive tool of modern espionage. Although highly invasive, espionage does not constitute a use of force (or armed attack) under

---

[1002] Gervais (n.958) 21.

[1003] Ibid.

[1004] Roscini (n.961) 66.

[1005] Dimitar Kostadinov, 'Cyber Exploitation' (*Infosec Institute,* 25.02.2013) <http://resources.infosecinstitute.com/cyber-exploitation/> accessed:21.08.2016.

[1006] Lotrionte (n.797) 476.

[1007] Ibid 477.

[1008] Ibid 476.

[1009] Beard (n.594) 127.

[1010] Hannah Lobel, 'Cyber War Inc: The Law of War Implications of the Private Sector's Role in Cyber Conflict' (2012) 47 Tex.Int'l.L.J. 617, 623.

international law absent a non-consensual physical penetration of the target state's territory […]'.[1011] Moreover, 'it is well accepted that the international law governing the use of force does not prohibit […] espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate'.[1012] Lin draws an analogy between cyber-espionage and 'the act of flying near an adversary's borders without violating its airspace [...] to gather intelligence'.[1013] He concludes that '[t]hough such an act might well be regarded as unfriendly, it almost certainly does not count as a use of force'.[1014]

Many authors rely on the U-2 precedent to affirm that cyber-espionage cannot be a use of force. On this occasion, the resolution project brought by Khrushchev before the UNSC–and qualifying such a flight as an unlawful form of use of force–was rejected. Relying on this incident, Antolin-Jenkins says that 'there appears to be some international consensus that espionage itself is not an illegal act in international relations'.[1015] He subsequently considers that cyber-espionage 'may constitute a violation of territorial integrity', but 'does not constitute either an armed attack or use of force'.[1016] According to Sharp, '[i]f the unlawful penetration of a state's airspace by the military aircraft of another state is not a use of force within the meaning of Article 2(4), it is certain as well that a virtual penetration of a state's cyberspace is not a use of force'.[1017] Wingfield has an identical approach.[1018]

The problem of malwares conceived to spy, but potentially upgraded for purposes of cyber-attacks raise similar analogies. Before the UNSC, the Soviet government had indeed underlined that 'flights over its territory [...] are

---

[1011] Michael Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited' (2011) 56 Vill.L.Rev. 569, 576.

[1012] Ibid 577.

[1013] Herbert Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4(1) J.Nat'l.Sec.L.&Pol'y 63, 79.

[1014] Ibid.

[1015] Antolin-Jenkins (n.588) 161.

[1016] Ibid.

[1017] Sharp (n.598) 127

[1018] Wingfield (n.584) 353-4.

particularly dangerous because United States bombers are continuously making flights with atomic and hydrogen bombs on board, especially in the direction of the frontiers of the USSR'.[1019] This argument was rejected. Pelican thus affirms that '[s]urveillance aircraft and reconnaissance satellites could be equipped with volatile weapons to deploy and deceive the surveilled until it is too late',[1020] but 'espionage by those means persists and the international community appears to tolerate it'.[1021] 'Based on those analogies, cyber-espionage should not be treated any differently'.[1022]

More audacious analogies are proposed by Weissbrodt and Murphy. Weissbrodt relies on Wingfield's list of threats of force, which includes 'initial troop movements' and 'massing of troops on a border'.[1023] 'It could be argued that a CNO that is conducting cyber-espionage but has the capability to launch a cyber-attack is analogous to initial troop movements or the massing of troops on a border'.[1024] However, a CNO that is only collecting information is espionage, and is not considered a threat or use of force.[1025] According to Murphy, '[i]f one views data as a form of property, indeed a very important form of property in the modern world, a mass loss of data could constitute an armed attack'.[1026]

Grosswald seems to find espionage and cyber-attacks equivalent.[1027] He then mentions that small-scale attacks might be considered use of force, but do not

---

[1019] UNSC, 858th Meeting (24.05.1960) [12].

[1020] Luke Pelican, 'Peacetime Cyber-Espionage: A Dangerous but Necessary Game' (2011-2012) 20 CommLaw Conspectus 363, 385.

[1021] Ibid.

[1022] Ibid.

[1023] Weissbrodt (n.952) 382.

[1024] Ibid.

[1025] Ibid.

[1026] John Murphy, 'Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?' (2013) 89 I.L.S. 309, 325.

[1027] Levi Grosswald, 'Cyberattack Attribution Matters Under Article 51 of the U.N. Charter' (2011) 36 Brook.J.Int'l.L. 1151, fn 107.

trigger the right to self-defence, except if they are part of a series of attacks.[1028] Dever affirms that 'stealing someone's personal information would be considered a cyberattack, but would not be considered to be the use of force'.[1029]

Drawing analogies between cyber-espionage and traditional espionage or other behaviours is thus recurrent in doctrine. Another form of meta-principle applied to cyber-espionage is the target-based approach.

c. Arguments based on a target-based approach

The crux of this approach is that self-defence is allowed when the critical infrastructures of a state are targeted. For instance, Sharp thinks that '[t]he right to respond in anticipatory self-defense does not apply to the penetration of all government computer systems during peacetime, but it should apply presumptively to those sensitive systems that are critical to a state's vital national interests'.[1030] An intrusion in such structures is considered 'an unlawful use of force that may constitute an armed attack prompting the right of self-defense'.[1031] He also recommends that states adopt rules of engagement reflecting this.[1032] Joyner and Lotrionte rely on the nature of the information stolen: '[i]f certain data are considered vital to national security (i.e. information that is "classified"), that information may be afforded special protections under the regime of self-defence'.[1033]

[1028] Ibid 1176-7.

[1029] James Dever and John Dever, 'Cyberwarfare: Attribution, Preemption, and National Self Defense' (2013) 2 J.L.&Cyber Warfare 25, 30.

[1030] Sharp (n.598) 129

[1031] Ibid 134.

[1032] Ibid 130.

[1033] Christopher Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12(5) E.J.I.L. 825, 855.

The resort to meta-principles of interpretation is thus omnipresent in the application of the UN Charter to cyber-espionage. However, some authors reject their use, and prefer to refer to the initial will of states or subsequent practice.

B. Arguments based on the initial will of states or subsequent practice

According to Sulmasy and Yoo, '[t]here appears to be little evidence that the representatives of the leading powers at the San Francisco conference believed Article 2 or Article 51 of the UN Charter would prohibit intelligence collection, or that the United States and the other members of the Security Council, when they ratified the Charter, did so with that understanding. Indeed, the practice of these states in the years following the adoption of the Charter would suggest the opposite'.[1034]

Beard affirms that '[a] nonphysical information "incursion" into an adversary's computer systems or networks is not equivalent to the invasion of another state's territory' as it lacks 'physical incursion', which is 'a fundamental component of illegal uses of force'.[1035] Beard then suggests that 'imposing the *Jus Ad Bellum*' on '[d]amaging acts of espionage and other unfriendly forms of information exploitation' would end up 'diminish[ing] restrictions on the use of force, thereby significantly weakening key safeguards upon which the international community relies and undermining the UN Charter's central purpose of maintaining international peace and security'.[1036] He then tackles the case of 'a hostile cyber act against an economic target' and considers 'far more likely' that it 'will constitute an economic, property, or security crime under a state's domestic law than an act of violence governed by the IHL [international humanitarian law] regime or an armed attack for purposes of the *jus ad bellum*'.[1037] The regime would be similarly weakened if the existence of an armed attack was

---

[1034] Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence Operations and International Law' (2007) 28 Mich.J.Int'l.L. 625, 628.

[1035] Beard (n.594) 96.

[1036] Ibid 117.

[1037] Ibid 128.

made dependent upon monetary losses following data exploitation.[1038] He concludes that hostile cyber acts (including espionage) lay outside the JAB and IHL frameworks.[1039]

O'Connell denounces 'the new interpretations of the rules on the use of force in order to have the right to respond to cyber problems with military force'.[1040] She explains that '[p]art of the obstacle in persuading governments that the military paradigm is the wrong one for cyber-security is the fact that most of the international law scholars working on security question from the early days of the Internet were in the military or had close ties to it'.[1041]

Kirchner notes that '[c]ountries such as Georgia, Iran or Estonia which have suffered cyberwar attacks have not reacted with armed force and *de lege lata* a cyberattack does not amount to an armed attack which would have permitted an armed reaction'.[1042]

According to Shackelford and Andres, '[s]tate practice demonstrates that many states are pushing the thresholds between intervention, use of force, and armed attacks higher so as to tolerate an increasing degree of cyber-espionage and other aggressive cyber-activities'.[1043]

The status of doctrine reveals a diversity of arguments, based on meta-principles, States' initial will or subsequent practice. In contrast, this thesis intends to study the status of law by resorting to the VCLT rules of interpretation.

[1038] Ibid 130.

[1039] Ibid 140.

[1040] Mary-Ellen O'Connell, 'Cyber Security without Cyber War' (2012) 17(2) J.Conflict&Sec.L. 187, 190.

[1041] Ibid 199.

[1042] Stefan Kirchner, 'Protection of Privacy Rights of Internet Users Against Cross-Border Government Interference' (2014) 42 I.J.L.I. 493, 498.

[1043] Shackelford and Andres (n.969) 1015.

2. Status of law

This research reveals that the majority of authors proposes to adapt articles 2(4) and 51 to cyber-attacks and cyber-spying, thanks to the use of meta-principles of interpretation. This dissertation actually intends to be critical of their argument. While this thesis confirms that most states consider international law as globally applicable in cyberspace, few of them have accepted the recurrent modalities of transposition found in doctrine. More fundamentally, this research objects to the non-application of the VCLT rules in most of doctrinal works.[1044] This is precisely what this thesis intends to bridge now. The terms of the treaty (2.1), and its object and purpose are defined (2.2), before an evaluation is carried out (2.3).

2.1. Definition of the UN Charter's central terms

As mentioned previously, many key concepts of the UN Charter are left defined, including in articles 2(4) (A) and 51 (B). At present, this thesis attempts to compensate this lacuna.

A. Definition of the terms of article 2(4)

'Threat or use of force' (a), 'territorial integrity, political independence, and any other manner inconsistent with the purpose of the UN' (b), and 'international relations' (c) are the fundamental terms of article 2(4), and need to be defined.

a. Threat or use of force

This thesis supports the idea that 'force' only means 'armed force'. This is first highlighted by the provision's context as the preamble of the UN Charter

[1044] With the exception of Buchan, Gervais and Schmitt, who refer to article 31 to determine whether a CNA violates article 2(4). See Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17(2) J.Conflict&Sec.L. 211, 215; Gervais (n.958) 26-30; Michael Schmitt, 'Computer Network Attack' (n.985) 62.

mentions that 'armed force shall not be used'. Article 44 also connects 'use of force' and 'armed force': '[w]hen the Security Council has decided to use force it shall, before calling upon a Member not represented on it to provide armed forces […] invite that Member […] to participate in the decisions of the Security Council concerning the employment of contingents of that Member's armed forces'. Moreover, the ICJ considers that only military interventions 'of such a magnitude and duration' may be considered use of force.[1045] Finally, this interpretation is confirmed by the *travaux préparatoires* as the Brazilian proposal to include 'the threat or use of economic measures' in article 2(4) was dismissed.[1046]

b. Territorial integrity, political independence, and any other manner inconsistent with the purpose of the UN

First, 'it is generally agreed that the notion of territorial integrity must be taken to refer to effective control and possession and not, necessarily, to a *de iure* recognized title to the territory in question. Consequently, loss of territorial integrity of a State implies loss of control and possession of the land, airspace, or sea, totally or partially, regardless of whether the former was based upon a legal title or a *de facto* situation'.[1047]

Second, 'the political independence of a State is infringed in all cases in which foreign acts tend to control the organs of a State and influence their capacity to decide through the threat or use of force or through subversive measures or pressures exerted upon them'.[1048]

Third, the expression 'any other manner inconsistent with the purpose of the United Nations' reveals that some acts may be considered a use of force, even if they are not directed against territorial integrity or political independence.

[1045] *Armed Activities* (n.777) [65].

[1046] UNCIO, Vol VI (1945) 558-9 <http://digitallibrary.un.org/record/1300969/files/UNIO-Volume-6-E-F.pdf> accessed:30.03.2018.

[1047] Samuel Blay, 'Territorial Integrity and Political Independence' (2010) M.P.E.P.I.L., [8].

[1048] Ibid [9].

Actually, '[e]very State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing' their commission when they 'involve a threat or use of force'.[1049]

c. International relations

'International relations' should be read as 'interstate relations', which means that '[t]he use of force solely within a State is not covered', that '[t]he international relations of a State are not affected if it consents to the use of armed force by another State in its own territory, including its territorial waters', and that 'it does not apply to military acts of protection by a State within its own territory against intruding persons, ships or aircraft'.[1050]

After having defined the central elements of article 2(4), the notion of 'armed attack', which is contained in article 51 needs to be analysed.

B. Definition of armed attack in article 51

As the French version of the UN Charter reveals, 'armed attack' must be understood as an '*agression armée*' ('armed aggression'). Such an armed attack is the *sine qua non* condition to activate self-defence. According to the *Nicaragua* case, 'States do not have a right of "collective" armed response to acts which do not constitute an "armed attack"'.[1051]

However, no definition or example of 'armed attack' is mentioned in article 51. An outstanding issue is whether resolution 3314, which 'lists examples of "acts of aggression""[1052]–pursuant to article 39–may also serve as a reference to define instances of 'armed attack'–pursuant to article 51. According to resolution 3314,

[1049] Dörr (n.914) 15.

[1050] Peter Randelzhofer and Oliver Dörr, 'Article 2(4)' in Bruno Simma and others (eds), *The Charter of the United Nations: A Commentary* (3rd edn, O.U.P. 2012) 214-15.

[1051] *Nicaragua* (n.46) [211].

[1052] Peter Randelzhofer and Georg Nolte, 'Article 51' in Simma (n.1050) 1410.

acts of aggression are carried out by foreign armed forces and include: invasion, attack and occupation of a foreign territory,[1053] bombardment or use of weapon against a foreign territory,[1054] blockade of ports and coasts,[1055] attacks on foreign forces or fleets,[1056] the breach of a troops-stationing agreement,[1057] to put its territory at disposal of a state B to attack a state C.[1058] It may also consist in sending irregular organized armed troops.[1059]

Theoretically, the notions of 'armed attack' and 'act of aggression' are different. First, they differ regarding who identifies them. According to article 39, the Security Council 'determine the existence' of acts of aggression (as well as the existence of threats or breaches of the peace). As to article 51, it is primarily conceived for the member state under attack–as well as those who could assist him–'until the Security Council has taken the measures necessary to maintain international peace and security'.

Then, their scope is theoretically different. Contrary to 'armed attack', 'act of aggression' found a definition in resolution 3314: 'the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations […]'.[1060] It is usually understood that the notion of 'armed attack' is narrower than the notion of 'act of aggression', a view expressed by many states within the *Special Committee on the Question of Defining Aggression.*[1061] They were

---

1053 UNGA Res 3314 (XXIX) (14.12.1974) [Definition of Aggression], art.3(a) (Annex).

1054 Ibid art.3(b).

1055 Ibid art.3(c).

1056 Ibid art.3(d).

1057 Ibid art.3(e).

1058 Ibid art.3(f).

1059 Ibid art.3(g).

1060 Ibid, art.1. See also: Rome Statute of the International Criminal Court (Adopted:17.07.1998–EIF:01.07.2002) 2187 UNTS 3, art.8bis.

1061 UNGA, 'Colombia, Cyprus, Ecuador, Ghana, Haiti, Iran, Madagascar, Uganda and Yugoslavia: proposal' (24.03.1969) UN-Doc A/AC.134/L.16.

'[c]onvinced that armed attack (armed aggression) is the most serious and dangerous form of aggression'.[1062]

The ICJ also mentioned the 'specific intention of harming'[1063] in the case of an armed attack, while nothing similar exists for the act of aggression.[1064]

Finally, the ICJ referred to the 'scale and effects' of an operation to distinguish between an armed attack and a mere 'frontier incident'.[1065] Resolution 3314 mentions that '[t]he first use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression', while 'the fact that the acts concerned or their consequences are not of sufficient gravity' may lead to the rejection of such a qualification.[1066]

However, both notions converge in practice, as revealed by ICJ case-law. Twice, the Court relied on resolution 3314 and its article 3(g) to assess instances of armed attacks,[1067] even mentioning–without further details–that '[t]here appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks'.[1068] Their proximity is also regularly underlined by doctrine.[1069] Some authors even think that both notions are identical. For instance, Zourek rejects the theory according to which the notion of 'aggression' in articles 39 and 51 are different.[1070] Abi-Saab considers that the 'acts' enumerated in resolution 3314 'meet the prerequisite of the resort to self-defence, whether committed by state's regular forces or irregular forces'.[1071]

[1062] Ibid.

[1063] *Oil Platforms (Iran v USA) (Judgment)* [2003] ICJ Rep 161, [64].

[1064] Yoram Dinstein, 'Aggression' (2015) M.P.E.P.I.L., [18}

[1065] *Nicaragua* (n.46) 195.

[1066] UNGA Res 3314 (n.1053) art.2.

[1067] *Nicaragua* (n.46) [195]; *Armed Activities* (n.777) [146].

[1068] *Nicaragua* (n.46) [195].

[1069] Randelzhofer and Nolte (n.1052) 1407.

[1070] Jaroslav Zourek, 'La définition de l'agression et le droit international : développements récents de la question', (1958) 92 Recueil des Cours 755, 816-817

[1071] George Abi-Saab, 'Cours général de droit international public' (1987) 207 Recueil de Cours 9, 362.

Randelzhofer and Nolte affirm that 'the difference between the two is so small that it is often overlooked'.[1072] As a consequence, resolution 3314 remains a good indicator of what may count as an armed attack under article 51.

The definitions of the central terms of the UN Charter have been specified. However, they are only one aspect of the application of the VCLT rules, to the extent that the treaty's object and purpose also guide the interpretation.

2.2. Definition of the object and purpose of the UN Charter

The object and purpose of the treaty may be found in both the UN Charter's preamble and article 1. The priorities set in the preamble may be categorized as follows. Firstly, the prevention of war, which consists in 'maintain[ing] international peace and security' and making sure that 'armed force shall not be used'. Secondly, a societal concern is revealed: 'to reaffirm faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small', as well as 'employ[ing] international machinery for the promotion of the economic and social advancement of all peoples'. Thirdly, the Charter promotes 'justice' and the 'respect of treaties'. Article 1 reiterates the need to maintain peace and international security, 'and to that end', to resort to collective measure to prevent threat to peace, the suppression of aggression, and the peaceful settlement of international disputes. Friendly relations and international cooperation are also mentioned. It is in light of these objects and purposes that UN Charter's terms are now interpreted.

2.3. Evaluation of the treaty

This thesis argues that cyber-spying does not amount to a breach of the UN Charter. To do so, it adopts a four-tier reasoning. First, the use of meta-

[1072] Randelzhofer and Nolte (n.1052) 1407-08.

principles remains controversial (A). Second, cyber-espionage does not amount to use of force or an armed attack (B). Third, hacking is not directed against territorial integrity or political independence (C). Fourth, espionage is not inconsistent with the UN's object and purpose (D).

A. The validity of meta-principles is disputed

As evoked previously, the application of the UN Charter to cyberspace is quasi-unanimously acknowledged by states. However, the validity of meta-principles is disputed.

The effect-based approach has been adopted by seven states. According to the USA, 'if cyber-operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under *jus ad bellum*, then such cyber-operations would likely also be regarded as a use of force'.[1073] Logically, right to self-defence 'may be triggered by cyber-operations that amount to an armed attack or imminent threat thereof'.[1074] Moreover, '[t]here is no legal requirement that the response in self-defense to a cyber armed attack take the form of a cyber-action, as long as the response meets the requirements of necessity and proportionality'.[1075] Due to some difficulties (actors and motives unknown, lack of direct death and destruction), the USA admits that difficulties may arise when determining whether an armed attack occurred.[1076] Yet, 'such ambiguities and room for disagreement do not suggest the need for a new legal framework specific to cyberspace'.[1077] Actually, 'they simply reflect the challenges in applying the Charter framework that already exists in many contexts'.[1078]

[1073] DoD/OGC, 'Department of Defense Law of War Manual' (2015, updated 2016) [16.3.1] <www.defense.gov/Portals/1/Documents/law_war_manual15.pdf> accessed:21.08.2016.

[1074] Ibid [16.3.3].

[1075] Ibid [16.3.3.2].

[1076] UNGA, 'Developments' (15.07.2011) (n.141) 18.

[1077] Ibid.

[1078] Ibid.

Switzerland adopts the same approach: 'it is not the type of weapon used, but their effect which is crucial. If the intensity of a computer attack is equal to that of an armed aggression, acts of self-defence shall theoretically resort to same or different weapons'.[1079] Hungary is also of this opinion, as '[d]epending on the damage caused, a non-armed attack may be considered equal to an armed assault. Such threats are constituted primarily by cyber-warfare [...]'.[1080] The Dutch secret services think that, '[f]or a cyber-attack to justify the right of self-defence, its consequences must be comparable with those of a conventional armed attack. If a cyber-attack leads to a considerable number of fatalities or large-scale destruction of or damage to vital infrastructure, military platforms and installations or civil property, it must be equated with an "armed attack"'.[1081] This position is 'largely in line with the government's position'.[1082] According to Belgium, the UN Charter 'does not describe any specific weapons of which impact or damages are significant enough for the attack to be described as armed. However, this is the case when there are fatalities or when vital or military infrastructure has been destroyed or severely damaged'.[1083] The former French Minister of Defence, Le Drian, affirmed that a cyber-attack could, with respect to its effects, be considered as an armed attack.[1084] The UK 'considers it is clear that cyber-operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self-defence'.[1085]

[1079] Caflisch, Pratique Suisse 2009 (n.689) 555-6.

[1080] Hungarian MOD (n.117) [52].

[1081] AIV/CAVV, 'Cyber Warfare' (n.213) 35-6.

[1082] Dutch Government, 'Government response to the AIV/CAVV report on cyber warfare' (2012) 5 <www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf> accessed:01.11.2017.

[1083] Belgian MOD (n.245) 7.

[1084] 'Cyberdéfense–Discours de Jean-Yves Le Drian' (*Ministère de la Défense*, 12.12.2016) <www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/cyberdefense-discours-de-jean-yves-le-drian-lundi-12-decembre-2016> accessed:11.05.2017.

[1085] AGO (n.88).

Analogical reasoning is openly resorted to by the USA and Switzerland.
The USA affirms that '[g]enerally, to the extent that cyber-operations resemble traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, then such cyber-operations would likely be treated similarly under international law'.[1086] Switzerland notes that 'there is currently no specific rules of international law' concerning CNE.[1087] 'However, an analogy may be established with the rules of international law related to espionage to define what are the conditions to resort to CNE'.[1088]

As to the target-based approach, the existence of critical infrastructures is mentioned by Afghanistan, [1089] Austria, [1090] Bangladesh, [1091] Belgium, [1092] Colombia, [1093] Cyprus, [1094] the Czech Republic, [1095] Estonia, [1096] Ethiopia, [1097]

[1086] DoD/OGC, 'Law of War Manual' (n.1073) [16.3.2].

[1087] Caflisch, Pratique Suisse 2013 (n.690) 106.

[1088] Ibid.

[1089] Afghan MCIT (n.125) 5, 10.

[1090] BKA, 'Austrian Cyber Security Strategy' (n.243) 14, 20.

[1091] MOPA (n.124) 2.

[1092] Belgian MOD (n.245) 7.

[1093] CONPES, 'Policy Guidelines' (n.112) 33.

[1094] Office of the Commissioner of Electronic Communications and Postal Regulation, 'Cybersecurity Strategy of the Republic of Cyprus' (2012) 6, 20 <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf> accessed:02.10.2016.

[1095] National Security Authority, 'National Cyber Security Strategy' (n.278) 7.

[1096] Ministry of Economic Affairs and Communication, 'National Strategy for Cyber and Information Security' (2014) 2-3, 6 <www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf> accessed:23.09.2016.

[1097] Computer Crime Proclamation (07.07.2016) No.958-2016, FNG No.83, 9104, s2(10).

Finland,[1098] Germany,[1099] Hungary,[1100] Italy,[1101] Ireland,[1102] Jamaica,[1103] Japan,[1104] Jordan, [1105] Kenya, [1106] Luxembourg, [1107] Mauritius, [1108] Montenegro, [1109] Norway,[1110] Paraguay,[1111] Qatar,[1112] Rwanda,[1113] Saudi Arabia,[1114] Slovakia,[1115]

[1098] DEFMIN (n.106) 12.

[1099] BMI (n.121) 6-7, 15.

[1100] Hungarian MFA, 'Hungary's National Security Strategy' (2012) 13-15 <http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf> accessed:24.09.2016.

[1101] PCM (n.107) 42.

[1102] Irish DoD, 'White Paper on Defence' (2015) 14 <www.defence.ie/WebSite.nsf/WP2015E> accessed:16.09.2017.

[1103] Jamaican Government, 'National Cyber Security Strategy' (2015) 31 <http://mset.gov.jm/sites/default/files/pdf/Jamaica%20National%20Cyber%20Security%20Strategy.pdf> accessed:16.09.2017.

[1104] Japanese Government, 'Cybersecurity Strategy' (2015) 25-28 <www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf> accessed:21.05.2017.

[1105] MICT (n.174) 6.

[1106] Kenyan MICT (n.207) 17.

[1107] Gouvernement du Luxembourg, 'Stratégie nationale en matière de cyber sécurité' (2011) 4-6 <www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Luxembourg_2011_Orig_Fr_CSB_Strat__gie_final_20111122_.pdf> accessed:29.09.2016.

[1108] Republic of Mauritius (n.287) 14.

[1109] Montenegrin Government (n.168) 4.

[1110] Norway Ministries (n.289) 10-12, 28.

[1111] Gobierno Nacional (n.175) 38.

[1112] MOTC (n.186) 4.

[1113] MITEC (n.176) 7.

[1114] Saudi MCIT (n.123) 79-82.

[1115] Slovak Republic (n.293) 11-12.

South Africa,[1116] Trinidad-and-Tobago,[1117] Turkey,[1118] and Uganda.[1119] Such reference is also present in the agreement between Russia and China,[1120] and the code of conduct between China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan.[1121] Most of these countries recognize that an attack on critical infrastructures could provoke loss of lives and destruction. However, none of them pretends that the mere targeting of these infrastructures amounts to use of force.

In parallel, many states underline the obscurity surrounding the relationship between cyber-operations and armed attacks. Japan specifies that '[t]here is still no accepted international common opinion on the relationship between cyber-attacks and armed attacks, however the possibility of cyber-attacks corresponding to armed attacks being carried out in this way is undeniable'.[1122] The Netherlands (in spite of their support for the consequentialist approach),[1123]

[1116] State Security Agency, 'National Cybersecurity Policy Framework for South Africa' (2015) 20
<www.gov.za/sites/www.gov.za/files/39475_gon609.pdf> accessed:15.05.2017.

[1117] Trinidadian Government (n.210) 13

[1118] UDHB, 'National Cyber Security Strategy and 2013-2014 Action Plan' (n.294) 9.

[1119] NITA (n.295) [1.2.1]-[1.2.2.].

[1120] Russian government (n.160) 5.

[1121] UNGA, 'Letter dated 9 January 2015' (n.143) 5.

[1122] ISPC (n.90) 12.

[1123] Kingdom of the Netherlands (n.109) 4.

Spain,[1124] Australia,[1125] India,[1126] Japan,[1127] Qatar,[1128] South Korea[1129] consider in their answers to the UNGGE that further work on how existing international law may apply to cyberspace is necessary.

The validity of meta-principles–which is favoured in doctrine–is thus not unanimously accepted by states. Considering this, this thesis now applies the VCLT rules of interpretation to the UN Charter, and reveals that spying is actually not equivalent to an armed attack or use of force.

B. Spying is not equivalent to an armed attack or use of force

The UN charter 'provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed'.[1130] However, this essay does not acknowledge that spywares are weapons. A weapon is '[a]n instrument used or designed to be used to injure or kill someone',[1131] 'a thing designed, intended or used for inflicting bodily harm or physical damage',[1132] or 'a means of gaining an advantage or defending oneself'.[1133] If cyber-spying may help in 'gaining an

---

[1124] UNGA, 'Developments in the field of information and telecommunications in the context of international security Report of the Secretary-General' (18.09.2014) UN-Doc A/69/112/Add.1, 5.

[1125] UNGA, 'Developments' (30.06.2014) (n.95) 2; UNGA, 'Developments' (15.07.2011) (n.141) 6.

[1126] India, 'Subject: UNGA Resolution 70-237 entitled–Developments in the field of Information and telecommunications in the context of international security', 4 <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/10/India.pdf> accessed:25.06.2018.

[1127] UNGA, 'Developments' (19.07.2016) (n.93) 12.

[1128] UNGA, 'Developments' (2010) (n.921) 10.

[1129] 'Report by the Republic of Korea' (2016) 1 <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/08/ROKISinfull.pdf> accessed:17.06.2017.

[1130] *Nuclear Weapons* (n.477) [39].

[1131] Black's (n.863) 'weapon'.

[1132] William Boothby, 'Weapons, prohibited' (2015) M.P.E.P.I.L., [1].

[1133] Ibid.

advantage', it is not 'designed, intended or used for inflicting bodily harm or physical damage'.

Whether 'cyber-weapons' exist or are regulated in cyberspace is moreover debated in state practice. The USA affirms that '[t]here is currently no international consensus regarding the definition of a "cyber-weapon"'. [1134] Slovakia highlights that 'the development of weapon systems for unconventional domains and spaces is not at present fully limited by the existing system of political and legal arrangements in the area of arms control, which poses a serious security problem'. [1135] Russia actually refers to the notion of 'information weapons', which help 'waging information war'. [1136] It has nevertheless been underlined in the introduction that its notion of 'information space' is wider than the notion of 'cyberspace'.

Interestingly, the Wassenaar Arrangement [1137] and the EU Regulation 428/2009[1138] aim at restricting the exportation of 'intrusion software'. However, these software are described as 'dual-use', which are defined by the European Commission as 'goods, software and technology that can be used for both civilian and military applications and/or can contribute to the proliferation of

---

[1134] DOD Cyberspace Policy Report, 'A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934' (2011) 8 <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf> accessed:05.09.2016.

[1135] Slovakian MOD, 'White Paper on Defence of the Slovak Republic' (2016) [44] <www.mosr.sk/data/WPDSR2016_LQ.pdf> accessed:15.05.2017.

[1136] Russian MOD, 'Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space' (2011) 5 <www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf> accessed:22.02.2017.

[1137] Wassenaar Arrangement Secretariat, 'List of Dual-Use Goods and Technologies and Munitions List' (2017) Public Doc Vol II, 4.D.4 <www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf> accessed:15.06.2018.

[1138] Commission Delegated Regulation of 12.10.2015 amending Council Regulation (EC) No.428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items, 23.

[…] WMD'.[1139] They are thus not considered as weapons *per se*. More significantly, the UN Arms Trade Treaty does not refer to cyber-tools.[1140]

Then, cyber-spying does not belong to any of the activities described in resolution 3314. While its article 4 specifies that 'the acts enumerated [...] are not exhaustive and the Security Council may determine that other acts constitute aggression under the provisions of the Charter', some observations may be made.[1141] Any behaviour mentioned in resolution 3314 involves a physical trespass, either *via* the movement of armed troops or the use of a physical weapon; this element seems to be the very characteristic of an act of aggression. The preamble similarly refers to 'the conditions created by the existence of all types of weapons of mass destruction' and reaffirms 'that the territory of a State shall not be violated by being the object, even temporarily, of military occupation or of other measures of force [...] and that it shall not be the object of acquisition by another State resulting from such measures or the threat thereof'.[1142] Even after the cyber-attacks against Estonia in 2007, a NATO official revealed that '[n]ot a single Nato defence minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future'.[1143]

In addition, a majority of states deny the fact that cyber-espionage amounts to use of force or an armed attack. According to the USA, '[i]t might be hard to sell the notion that an unauthorized intrusion into an unclassified information

---

[1139] European Commission, 'Dual-use trade control' <http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/> accessed:29.04.2017.

[1140] Arms Trade Treaty (adopted 02.04.2013).

[1141] As resolution 3314 is not a treaty, whether and how the VCLT rules of interpretation may be applied remain uncertain. As Wood put it once, 'there is little authority on the interpretation of non-treaty texts'. See Michael Wood, 'The Interpretation of Security Council Resolutions' (1998) 2 M.P.Y.U.N.L. 73, 86.

[1142] UNGA Res 3314 (n.1053) preamble.

[1143] Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', *Guardian* (17.05.2007) <www.theguardian.com/world/2007/may/17/topstories3.russia> accessed:17.10.2016.

system, without more, constitutes an armed attack'.[1144] The Dutch secret services affirm that, '[u]nder international law, cyber-espionage can lead only to diplomatic retaliation, no matter how harmful the loss of information is'.[1145] When Finland considered the adoption of new intelligence legislation in 2015, it said that '[t]he foreign information systems intelligence proposed in the present report would not be on the level of cyber-attacks and thus equivalent to the use of force; it would involve acquiring information as part of other intelligence-gathering'.[1146] It underlined that '[t]he basic purpose of information systems intelligence would be to collect information on information systems as covertly as possible, not to disrupt the target system or to alter or delete data contained therein'.[1147] While 'case-law and legal opinions concerning cyber-operations are still only emerging and a threshold for what constitutes an attack in a cyber-environment has not been defined in international law, it would seem that information systems intelligence equivalent to intelligence-gathering could not be considered a use of force violating international law, and certainly not an attack'.[1148] Moreover, '[t]his view is supported by the fact that apparently so far, no government has undertaken military defence measures against a government targeting information systems intelligence against it'.[1149] Finally, 'action against cyber-systems has so far not been undisputedly and publicly declared as equivalent to an armed attack in the international community'.[1150]

The only contrary positions have been adopted by Indonesia and Mexico. According to the former 'extraterritorial surveillance' is 'a violation of international law and the United Nations Charter'.[1151] According to the latter, 'spying against Mexican citizens' is 'contrary to the UN Charter and the case-law

---

[1144] DoD/OGC, 'An Assessment' (n.676) 18.

[1145] AIV/CAVV (n.213) 17 (footnote 19).

[1146] DEFMIN, 'Guidelines' (n.735) 73.

[1147] Ibid.

[1148] Ibid 73-4.

[1149] Ibid 74.

[1150] Ibid.

[1151] UN Press Release GA/SHC/4094 (n.665).

of the ICJ'.[1152] Following cyber-spying on *Gemalto* firm, Jan-Philipp Albrecht (a Member of the European Parliament) also said that it was 'an act of aggression according to international law'.[1153] However, such sporadic reactions hardly counterbalance the previous reasoning.

In any case, neither espionage nor cyber-espionage allows the resort to preemptive or preventive self-defence. A textual interpretation of article 51 does not authorize it: '[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack *occurs* against a Member of the United Nations […]'. First, to 'occur' means 'to happen, come about, take place, esp. without being arranged or expected'.[1154] Second, article 51 does not refer to any 'threat' of armed attack, whereas 'threat' appears in other provisions of the Charter–a point already made by Corten.[1155] Preemptive and preventive self-defence were moreover expressly rejected during the *travaux préparatoires*, especially by the American delegation: 'Mr. Gates posed a question as to our freedom under this provision in case a fleet had started from abroad against an American republic, but had not yet attacked. To this Commander Stassen [An American delegate] replied that we could not under this provision attack the fleet but we could send a fleet of our own and be ready in case an attack came'.[1156] Then, 'Mr. Hackworth expressed the view that the present draft greatly qualified the right of self-defense by limiting it to the occasion of an armed

---

1152 Paula Chouza, 'México rechaza "categóricamente" cualquier labor de espionaje', *El Pais* (02.09.2013)
<https:/elpais.com/internacional/2013/09/02/actualidad/1378158712_855137.html> accessed:29.11.2017.

1153 Martin Untersinger, 'Cartes SIM piratées, une guerre froide au sein de l'Union européenne', *Le Monde* (23.02.2015)
<www.lemonde.fr/pixels/article/2015/02/23/piratage-de-gemalto-une-guerre-froide-au-sein-de-l-union-europeenne_4581935_4408996.html> accessed:14.03.2015.

1154 'occur' (O.E.D-Online, O.U.P. 2018)

1155 Olivier Corten, 'La légitime défense préventive: un oxymore?' (*UN WebTV,* 24.03.2017)
<http://webtv.un.org/watch/olivier-corten-sur-la-l%C3%A9gitime-d%C3%A9fense-pr%C3%A9ventive-un-oxymore/5511732829001> accessed:09.09.2018.

1156 'Minutes of the Thirty-Eighth Meeting of the United States Delegation' (14.05.1945) 1 F.R.U.S.
<https://history.state.gov/historicaldocuments/frus1945v01/d226> accessed:06.09.2018.

attack. Mr. Stassen stated that this was intentional and sound. We did not want exercised the right of self-defense before an armed attack had occurred'.[1157] Subsequent practice does not support preemptive or anticipative self-defence either. Following the Millennium summit, the Secretary-General affirmed that '[t]he short answer is that if there are good arguments for preventive military action, with good evidence to support them, they should be put to the Security Council, which can authorize such action if it chooses to [...] We do not favour the rewriting or reinterpretation of Article 51'.[1158] 'However, a threatened State, according to long established international law, can take military action as long as the threatened attack is *imminent*'.[1159] The Non-Aligned Movement–with 120 members–supports a 'restrictive' reading of article 51.[1160] Following *Operation Opera*, the UNSC 'strongly condemn[ed] the military attack by Israel in clear violation of the Charter of the United Nations and the norms of international conduct'.[1161] Yet, Israel had called the bombing of this Iraki atomic reactor 'an elementary act of self-preservation' and invoked its 'inherent right to self-defence', as 'there was less than a month to go before Osirak might have become critical'.[1162]

Cyber-espionage is thus not equivalent to an armed attack or use of force. Moreover, it is not directed against a state's territorial integrity or political independence.

[1157] 'Minutes of the Forty-Eighth Meeting (Executive Session) of the United States Delegation' (20.05.1945) 1 F.R.U.S. <https://history.state.gov/historicaldocuments/frus1945v01/d243> accessed:06.09.2018.

[1158] UNGA, 'Follow-up to the outcome of the Millennium Summit' (02.12.2004) UN-Doc A/59/565, [190].

[1159] Ibid [188].

[1160] Non-Aligned Movement, 'Final Document' (2016) [25.2] <http://cns.miis.edu/nam/documents/Official_Document/XVII-NAM-Summit-Final-Outcome-Document-ENG.pdf> accessed:10.09.2018.

[1161] UNSC Resolution 487 (1981) [1].

[1162] Shirley Scott, Anthony Bilingsley and Christopher Michalesen, *International Law and the Use of Force: A Documentary and Reference Guide* (ABC-CLIO 2009) 131-2.

C. Spying is not directed against territorial integrity or political independence

Cyber-espionage might help securing information that will then be used in an action directed against territorial integrity or political independence. However, it has previously been explained why cyber-espionage *per se* is not at odds with territorial integrity,[1163] or political independence.[1164] It does not even correspond to 'any other manner inconsistent with the purpose of the UN'. The servers or computers containing the stolen data are perhaps not even on the same territory as the information's owner.

States have never seriously considered that spying–even in its traditional form–could breach the UN Charter.

Following the shooting down of the U-2, Khrushchev said that the 'U.S. Government is crudely flouting the universally accepted standards of international law and the lofty principles of the U.N. Charter'.[1165] At the time, 'Soviets did not […] know under what article of the U.N. Charter they would bring the plane incident before the Security Council'.[1166] At pilot Gary Powers' trial, Prosecutor Rudenko affirmed that '[t]here is every reason to conclude that the incursion of a foreign plane, such as the incursion of the U-2 spy plane, undoubtedly constitutes an act of aggression'.[1167] Yet, it seems that Khrushchev himself thought the argument was not viable.[1168] The debate at the UNSC finally focused on the notions of 'aggressive acts' and sovereignty,[1169] and the draft

---

[1163] See Chapter I-I.

[1164] See Chapter I-II.

[1165] (1960) 6(5) Keesings, 17437.

[1166] 'Eastern Europe Region, Soviet Union, Cyprus' (1958-1960) X(1) F.R.U.S. (Document 147) <https://history.state.gov/historicaldocuments/frus1958-60v10p1/d147> accessed:27.04.2016.

[1167] 'Comments on Trial of US Spy Powers', *USSR International Affairs* (19.08.1960) 141.

[1168] Spencer Beresford, 'Surveillance Aircraft and Satellites: A Problem of International Law' (1960) 27(2) J. Air L. 107, 114.

[1169] (1960) 6(6) Keesings, 17498.

resolution brought by the USSR was rejected.[1170] Only Poland affirmed that this flight was 'a violation of the United Nations Charter, particularly Articles 1, 2 and 78'.[1171] On the contrary, the French delegation expressed 'serious doubts about the aggressive nature of the acts'.[1172] The UK similarly considered that '[i]t must be perfectly clear to all of us that this act involved no use of force or threat of the use of force against the Soviet Union'.[1173] Tunisia underlined that '[a]t no time have we been told that the aircraft was armed, or was followed or accompanied by other armed aircrafts' and denied the qualification of aggression.[1174] China affirmed that, '[a]s regards the U-2 affair, the word "aggression" clearly does not apply'.[1175] Finally, '[t]he U.S. Government [did] not deny that it [had] pursued such a policy for purely defense purposes. What it emphatically [did] deny is that this policy [had] any aggressive intent'.[1176] France underlined that 'it is the practice, open to criticism perhaps but generally recognized, that such activities should not lead to recourse to international bodies'.[1177] It was also highlighted that '[t]here are no rules of international law concerning the gathering of intelligence in peace-time. The proof that no international offence is involved is furnished by the fact that the aggrieved State cannot demand reparations from the State for which the intelligence agent was working'.[1178] After an RB-47 was shot down, a similar draft resolution failed.[1179] When North Korea seized the American ship *Pueblo*, a 'crude aggressive act' was

[1170] Ibid.

[1171] UNSC, 858th Meeting (24.05.1960) [83]-[85]

[1172] Ibid [8].

[1173] Ibid [25].

[1174] UNSC, 859th Meeting (25.05.1960) [10].

[1175] UNSC, 858th Meeting (24.05.1960) [66].

[1176] (1960) 42 Dep't St Bull 849, 852.

[1177] UNSC, 858th Meeting (24.05.1960) [9].

[1178] Ibid

[1179] (1960) 43 Dep't St Bull 1, 244.

denounced. However, the debate then dealt more with the presence of the ship in territorial or international waters than with the spying activities.[1180]

Cyber-spying is thus directed against none of these elements. Moreover, it is not inconsistent with the object and purpose of the UN.

D. Spying is not inconsistent with the UN's object and purpose

As mentioned previously, preventing war is the main goal of the UN Charter. War is '[a] state of armed conflict between different countries or different groups within a country'.[1181] As a consequence, hacking–which is not 'a state of armed conflict'–cannot be deemed inconsistent with the UN object and purpose.

Moreover, an in-depth analysis of state practice actually reveals an essential preoccupation of states: defending themselves against external and internal threats. In states' mind, intelligence-gathering is an essential component of their national security, a tool of self-preservation and decision-making. No one seriously considers that it is a use of force or an armed attack, and some states–unsatisfied with their intelligence capacities–even plan to increase them.
While describing espionage on state and companies' IT systems as a serious threat to national security, France says that '[i]ntelligence activities and secret operations are becoming more important in a strategic context marked by the growing role of non-state players'.[1182] Moreover, the French Government underlines the need to 'develop combat capabilities' in cyberspace, and to adopt an 'active defence strategy' that would 'combine an intrinsic protection of systems, permanent surveillance, quick reaction and offensive action', thus 'imposing a strong governmental impulsion and a mindset change'.[1183] 'The

[1180] (1968) 14(3) Keesings, 22585; (1969) 15(1) Keesings, 23120.

[1181] 'war' (Oxford English Dictionary)
<en.oxforddictionaries.com/definition/war> accessed:14.05.2017.

[1182] Commission du livre blanc, *French White Paper* (n.699) 71.

[1183] Commission du livre blanc (n.119) 53.

active defence requires a real capacity of "borders" surveillance'.[1184] According to the UK, 'cyber-intelligence, surveillance and reconnaissance' are among the 'roles identified with cyber-operations'.[1185] Then, '[t]he Government will [...] secure the UK's advantage in cyber space' and '[g]ather intelligence on threat actors'. [1186] Moreover, the British Defence Secretary Philip Hammond announced that 'we are developing a full-spectrum military cyber-capability, including a strike capability'.[1187]

The American DoD considers that the legality of peacetime intelligence and counterintelligence activities 'must be considered on a case-by-case basis'.[1188] 'The United States conducts such activities via cyberspace, and such operations are governed by long-standing and well-established considerations, including the possibility that those operations could be interpreted as a hostile act'. [1189] However, a memo by CIA Director John Brennan underlined the need to 'place our activities and operations in the digital domain at the very center of all our mission endeavors' and the creation of a 'Directorate of Digital Innovation'.[1190] This was interpreted as a 'major expansion of the CIA's cyber-espionage capabilities'.[1191]

[1184] Jean-Marie Bockel, 'Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense' (18.07.2012) No.681, 71 <www.senat.fr/rap/r11-681/r11-6811.pdf> accessed:17.11.2017.

[1185] MoD, 'Land Operations' (2017) [7-48] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/605298/Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web.pdf > accessed:24.01.2018.

[1186] Cabinet Office, 'Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space' (2009) 4 <www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf > accessed:08.09.2016.

[1187] UK Government, 'New cyber reserve unit created' (29.09.2013) <www.gov.uk/government/news/reserves-head-up-new-cyber-unit> accessed:22.07.2016.

[1188] DoD/OGC, 'Law of War Manual' (n.1073) [16.3.2].

[1189] Ibid.

[1190] CIA, 'Unclassified Version of March 6, 2015 Message to the Workforce from CIA Director John Brennan: Our Agency's Blueprint for the Future' <https://www.cia.gov/news-information/press-releases-statements/2015-press-releases-statements/message-to-workforce-agencys-blueprint-for-the-future.html> accessed:14.07.2018.

[1191] Franz-Stefan Gady, 'CIA to Expand Cyber Espionage Capabilities', *The Diplomat* (24.02.2015)

The Czech Military Intelligence (MI) 'is a provider of up-to-date, independent, multisource, objective, and complex intelligence information. It integrates espionage and counter-espionage activities and ensures information support for a decision-making process at the top national political-military level. Its priorities are annually set by the Government'.[1192] Moreover, 'MI uses the principles of project management and augments its capabilities by operating in cyberspace. At the same time, MI applies new technologies in all of the covered intelligence fields',[1193] and 'a comprehensive inter-field analysis'.[1194]

According to New Zealand, '[i]nformation about cyber-threats can come from a variety of sources', including 'classified intelligence'. Moreover, 'New Zealand's intelligence agencies may also use cyber-tools to gather intelligence and information for the protection of New Zealand's interests'.[1195]

Amos Yadlin–the Head of the Israeli Directorate of Military Intelligence–publicly acknowledged that '[u]sing computer networks for espionage is as important to warfare today as the advent of air support was to warfare in the 20th century'.[1196] Following the revelations about the spying software *Flame*, Israel did not seek to deny responsibility. According to Israeli Vice-Premier Moshe Yaalon, '[w]hoever sees the Iranian threat as a significant threat is likely to take various steps, including these, to hobble it [...] Israel is blessed with high technology, and we boast tools that open all sorts of opportunities for us'.[1197]

<http://thediplomat.com/2015/02/cia-to-expand-cyber-espionage-capabilities/> accessed:16.10.2016.

[1192] Czech MOD, 'White Paper on Defence' (2011) 107 <www.army.cz/assets/en/ministry-of-defence/whitepaperondefence2011_1.pdf> accessed:14.05.2017.

[1193] Ibid.

[1194] Ibid (footnote 12).

[1195] DPMC (n.108) 3.

[1196] Reuters and Anshel Pfeffer, 'How Cyberwarfare Has Made MI a Combat Arm to the IDF', *Haaretz* (16.12.2009) <www.haaretz.com/how-cyberwarfare-has-made-mi-a-combat-arm-of-the-idf-1.2051> accessed:16.10.2016.

[1197] Associated Press, 'Flame computer virus strikes Middle East, Israel speculation continues', *CBS News* (29.05.2012) <www.cbsnews.com/news/flame-computer-virus-strikes-middle-east-israel-speculation-continues/> accessed:16.04.2015.

Slovakia promotes 'the development of intelligence, surveillance and reconnaissance capabilities' and their land forces benefit from 'intelligence and electronic warfare equipment'.[1198]

The Netherlands needs '[r]obust and independent intelligence',[1199] while the 'DISS uses the following sources for its analyses […] Cyber (computer network exploitation): intelligence collected from networked computer systems'.[1200] Moreover, '[t]raditional interception methods such as SIGINT are no longer sufficient to exploit relevant new forms of digital communication. CNE operations allow DISS to acquire direct access to digital documents in accordance with its statutory powers'.[1201]

Bulgaria affirms that its services 'support and develop capabilities for the acquisition of strategic intelligence by using […] technological means'.[1202] In Croatia, '[c]yberterrorism and other cyber aspects of national security are dealt with by a small number of the competent bodies within the security and intelligence system […]'.[1203] Australia works within the framework of its traditional defence and intelligence and broader national security relationships to counter cyber threats'.[1204] Saudi Arabia addresses 'IS threats and exploitation attempts at the national level' through a 'national Security Operations Center', 'which would collect and disseminate threat and intelligence information'.[1205]

[1198] Slovakian MOD, 'The White Paper on Defence' (n.932) [52], [74].

[1199] Dutch Government, 'International Security Strategy' (2013) 16 <www.government.nl/binaries/government/documents/policy-notes/2013/06/21/international-security-strategy/ivs-engels.pdf> accessed:01.11.2017.

[1200] MIVD, '2014 Annual Report' (n.741) 9.

[1201] MIVD, '2013 Annual Report' (2014) 21 <www.government.nl/binaries/government/documents/annual-reports/2014/06/30/annual-report-2013-netherlands-defence-intelligence-and-security-service/web-jaarverslag-2013-mivd-eng.pdf> accessed:01.11.2017.

[1202] Bulgarian Government, 'White Paper on Defence and the Armed Forces of the Republic of Bulgaria' (2010) 44 <www.mod.bg/en/doc/misc/20101130_WP_EN.pdf> accessed:12.10.2016.

[1203] Croatia (n.933) 9.

[1204] Australian Department of Defence, *Defence White Paper 2013* (Commonwealth of Australia 2013) [2.89].

[1205] Saudi MCIT (n.123) 13.

China confesses that they have made 'significant progress […] in building information systems for reconnaissance and intelligence'.[1206] Poland will use 'reconnaissance and intelligence activities'.[1207]

This theory has previously been supported by some authors. According to Baker 'international law neither endorses nor prohibits espionage, but rather preserves the practice as a tool by which to facilitate international cooperation'.[1208] Ariail, Hitz and Silver note that there is 'information on subjects which are significant national security concerns', and '[m]any consider that the possession of these types of information contributes to national security and the ultimate goals of world peace and order. It can reduce the risks of international conflict and permit international measures to reduce or limit arms'.[1209]

Spying is thus not inconsistent with the UN's object and purposes; on the contrary, it helps reducing uncertainty. Ironically, the communications of diplomats were systematically intercepted by the USA during San Francisco conference.[1210] Moreover, the meta-principles cherished by doctrine are not systematically supported by states.

3. Conclusion

JAB is originally physically-centred, with the sole resort to armed force allowing self-defence in return. Yet, this traditional and accepted definition has proved to

---

[1206] Ministry of National Defence of the PRC, 'China's National Defense in 2010' (2011) part III <http://eng.mod.gov.cn/Database/WhitePapers/2011-04/02/content_4442745_4.htm> accessed:25.08.2016.

[1207] National Security Bureau, 'National Security Strategy of the Republic of Poland' (National Security Bureau 2014) 31.

[1208] Christopher Baker, 'Tolerance of International Espionage: A Functional Approach' (2004) 19(5) Am.U.Int'l.L.Rev. 1091, 1092.

[1209] Daniel Silver, 'Intelligence and Counterintelligence', in John Norton Moore and Robert Turner (eds), *National Security Law* (C.A.P. 2005) 937.

[1210] Nicky Hager, 'Au coeur du renseignement américain', *Le Monde Diplomatique* (November 2001) <www.monde-diplomatique.fr/2001/11/HAGER/8141> accessed:26.10.2016.

hardly fit the particularities of cyberspace. As a consequence, authors have proposed to adapt the existing rules, through three main meta-principles: the consequentialist and target-based approaches, as well as analogy. Two trends exist regarding the consequentialist approach: either they focus on the effects in the virtual world, or in the physical space. In both cases, it is the damage criterion that allegedly distinguishes cyber-spying and cyber-attacks. This approach is gaining ground in states' opinion, as seven of them–the USA, Switzerland, the Netherlands, Belgium, Hungary, France and the UK–resort to it. However, seven–including the Netherlands–acknowledge that further reflexion is required. Only Switzerland and the USA adopt the analogical approach. While states confess that operations targeting critical infrastructures could have dramatic consequences, they do not validate the target-based approach. For the time being, the evolution of the instrument-based approach thus remains *de lege ferenda*.

The UN Charter has always been silent regarding espionage, in both its physical and digital forms. Applying the VCLT actually helps reinforcing this conclusion: cyber-espionage is unphysical, is not a weapon and is not at odds with political independence. Moreover, states are eager to take advantage of this ambiguity, and consider spying as essential for their survival. Espionage is continually less of a taboo subject.

IV – JUS IN BELLO

The regulation of wartime spying has its roots in both the 'law of Geneva' and the 'law of The Hague', which constitute IHL (or JIB). On the one hand, Geneva Conventions 'protect people who do not take part in the fighting (civilians, medics, aid workers) and those who can no longer fight (wounded, sick and shipwrecked troops, prisoners of war)'.[1211] On the other hand, the Hague Conventions aim at 'protecting combatants and non-combatants by restraining the methods and means of combat'.[1212] Two types of conventions are analysed in this chapter, starting with the rules regulating conduct between belligerents, or those who help belligerents: The Hague Conventions II and IV on the Laws and Customs of War on Land (Hague II and Hague IV), and Additional Protocol I to the Geneva Conventions. Then, the rules of interest are those regulating conduct towards a neutral power. They are contained in the Convention relative to the Rights and Duties of Neutral Powers and Persons in case of War on Land (Hague V), and the Convention concerning the Rights and Duties of Neutral Powers in Naval War (Hague XIII).

Three remarks should be made. First, wartime spying is not illegal, and this element is confirmed by national war manuals.[1213] Yet, the captured spy may be denied the prisoner-of-war (POW) status and face an unhappy fate. History is full of these unfortunate men.[1214] Second, these conventions have originally been drafted for specific domains: land and sea. Whether and how they may be adapted to cyberspace are difficult questions. Third, some rules invoked by doctrine regarding the behaviour of foreign powers are not analysed in the 'status of law'. Such is the case for The Hague Air Rules, which have never been ratified.

1211 'The Geneva Conventions of 1949 and their Additional Protocols' (*ICRC,* 2014) <www.icrc.org/en/document/geneva-conventions-1949-additional-protocols> accessed:13.03.2017.

1212 François Bugnion, 'Droit de Genève et droit de La Haye' (2001) 83 I.R.R.C. 901, 905.

1213 Such is the case for Belgium, Colombia, Ecuador, Israel, Madagascar, the Netherlands, New Zealand, Nigeria, South Africa, and Switzerland. See 'Practice Relating to Rule 107. Spies' (*ICRC*) <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule107_sectionb> accessed:13.06.2017.

1214 (1940) III-IV(12) Keesings, 4186; 1941 IV(11) Keesings, 4887; (1942) IV(12) Keesings, 5335; (1945) V(3) Keesings, 7063; (1940) III-IV(10) Keesings, 4279; (1944) V(10) Keesings, 6789.

Due to the lack of subsequent state practice and articles similar to Hague V, Hague XIII will not be analysed in a specific part. These bodies of rules are analysed in both the status of doctrine (1) and the status of law (2). The chapter ends with a conclusion (3).

1. Status of doctrine

The rules concerning belligerents (1.1) and the rules involving a neutral state (1.2) are alternatively tackled.

1.1. The rules concerning belligerents

The regulation of espionage has long been viewed through the mere prism of the law of war. Various treaties and manuals defined and imposed sanctions on spies, including Hague II, Hague IV, the Geneva Convention IV [1215] and Protocol I. In the framework of an international armed conflict, the state that sends spies does not commit a war crime. Paradoxically, if the agent is caught, he may be denied the status of POW,[1216] face a fair trial, and then be punished.[1217]

Authors are quasi-unanimous on the use of analogical reasoning to justify that wartime cyber-espionage is legal. As McGavran notes, '[c]urrently, the law of war applies to cyber-attacks by analogy only'.[1218]
Beard affirms that hostile cyber-acts 'are better described as merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage'. [1219] Cyber-espionage thus belongs to information-gathering

---

[1215] Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War (Adopted:12.08.1949–EIF:21.10.1950) 7 UNTS 287.

[1216] Hague II, art.30; Hague IV, art.30.

[1217] Geneva Convention IV (1949) art.5.

[1218] Wolfgang McGavran, 'Intended Consequences: Regulating Cyber Attacks' (2009) 12 Tul.J.Tech.&.Intell.Prop. 259, 269.

[1219] Beard (n.594) 40.

activities that 'enjoy explicit protection under the *jus in bello*'.[1220] He also thinks that the IHL regime 'was never intended to apply to every type of damaging action',[1221] and describes them as 'legal phantom in IHL'.[1222] According to Aldrich, '[s]ome IW operations may constitute little more than the sophisticated use of technology to spy on an adversary. Spying has always been held permissible under international law and the law of armed conflict [...]'.[1223] Fleck similarly thinks that 'intelligence gathering is not *per se* a violation of international humanitarian law […]'.[1224] Melnitzky suggests that 'the use of traditional military force against cyber-espionage would most likely violate the principal of *jus in bello*'.[1225] Solis also points that espionage is not a violation of the law of armed conflicts (LOAC).[1226] Schaap mentions that 'the lawfulness of espionage during armed conflict' is recognized.[1227] According to Kirchner, '[w]hile espionage might be illegal, indeed a crime under most national legal systems, it is not always illegal under International Humanitarian Law, at least not if it is done by state actors'.[1228] His reasoning continues as follows: 'those who are legally permitted to be combatants might, under Article 46 of Protocol I to the Geneva Conventions, in some cases also engage in espionage when they are identifiable as members of the armed forces of a party to an armed conflict, e.g. if they wear uniforms while engaging in espionage or if the espionage is undertaken by a member of the armed forces who is based ("resident") in an occupied territory. The latter option is no longer technically necessary when it comes to espionage through the Internet and simply requires those manning the computers to wear

---

[1220] Ibid. 127.

[1221] Ibid 123.

[1222] Ibid 114.

[1223] Richard Aldrich, 'How do you know you are at War in the Information Age' (2000) 22 Hous.J.Int'l.L. 223, 252.

[1224] Fleck (n.790) 698.

[1225] Melnitzky (n.997) 539.

[1226] Gary Solis, 'Cyber Warfare', 22.

[1227] Schaap (n.159) 140

[1228] Kirchner (n.1042) 372.

uniforms while doing so'.[1229] Joyner and Lotrionte also suggests that, '[a]s a source of customary international law, state practice seems to sympathise with permitting some IW activities'.[1230] Consequently, 'espionage, universally criminal under domestic laws, does not *ipso facto* violate international law. In this context, IW conducted as espionage activity might be considered lawful. Furthermore, ruses have long been part of warfare and their legitimacy is explicitly recognised in the laws of war. Just as the original ancient Trojan Horse was legal, so too would the use of some "Trojan Horse" pieces of software be permissible in times of armed conflict between two states'.[1231] Jolley thinks that '[e]spionage, being more akin to traditional information gathering, e.g., spying. The use of information systems and the Internet to conduct non-kinetic espionage is lawful under the current international treaties and norms'.[1232]

The Tallinn Manual 1.0 is also of the view that '[c]yber espionage and other forms of information gathering directed at an adversary during an armed conflict do not violate the law of armed conflict'.[1233] Yet, 'a member of the armed forces who has engaged in cyber-espionage in enemy-controlled territory loses the right to be a prisoner of war and may be treated as a spy if captured before re-joining the armed forces to which he or she belongs'.[1234] Similar provisions appear in Rule 89 of Tallinn Manual 2.0.[1235] However, both fail to address the thorny issue of extra-territoriality. Tallinn Manual 1.0 even specifies that '[c]yber-espionage must be distinguished from CNE, which is a doctrinal, as distinct from an international law, concept. CNE often occurs from beyond enemy territory, using remote access operations'.[1236]

[1229] Ibid 372-3.

[1230] Joyner and Lotrionte (n.1033) 859.

[1231] Ibid.

[1232] Jason Jolley, 'Article 2(4) and Cyber Warfare: How do Old Rules Control the Brave New World?' (2013) 2(1) International Law Research 1, 2.

[1233] Schmitt, *Tallinn Manual* (n.52) 192.

[1234] Ibid 193.

[1235] Schmitt, *Tallinn Manual 2.0* (n.53) 409-12.

[1236] Schmitt, *Tallinn Manual* (n.52) 193.

Few scholars have suggested a different solution or mentioned the global practice of states.

Hollis first notices that '[a]t present, there are no specific rules for IO, nor is there any sign of a more general revision to accommodate IO. Thus, [...] the law of war governs IO by analogy'.[1237] He nevertheless considers that 'perhaps the conventional wisdom on the viability of IO law by analogy is simply wrong'.[1238]

Beard underlines that, 'due to the unusual properties of information itself, there are serious problems and perils in relying on such analogies to extend the IHL framework to most events in cyberspace'.[1239] He then underlines that 'current state practice reflects this more complex reality, since no state has actually invoked and applied IHL rules or the *jus ad bellum* to any hostile cyber act standing alone (nor actually engaged in cyberwar)'.[1240] He finally concludes that '[t]he nature of hostile cyber acts–in which information in systems and networks must first be accessed by "persuasion"–makes these acts highly unusual candidates for regulation under either the *jus ad bellum* or *jus in bello*'.[1241]

Analogical reasoning is essential to authors comparing the rules concerning belligerents to cyber-espionage. This form of reasoning is, however, also useful to those authors engaged in doctrinal analysis of the rules involving a neutral state.

1.2. The rules involving a neutral state

Provisions of The Hague Conventions on neutrality raise various interpretations as to whether spying is prohibited on neutral territory. Some arguments are

---

[1237] Duncan Hollis, 'Why States need an International Law for Importation Operations' (2007) 11 Lewis&Clark L.Rev. 1023, 1037. Here, 'IO' is the abbreviation of 'Information Operations'.

[1238] Ibid 1053.

[1239] Beard (n.594) 70-1.

[1240] Ibid.

[1241] Ibid 95-6.

based on articles 1, 2, and 3 of Hague V, article 5 of Hague XIII, and The Hague Air Rules (A), while others are based on article 8 of Hague V, and articles 7 and 10 of Hague XIII (B).

A. Arguments based on articles 1, 2, and 3 of Hague V, article 5 of Hague XIII, and The Hague Air Rules

According to Hague V and XIII, belligerents are forbidden 'to erect wireless telegraphy stations or any apparatus for the purpose of communicating with the belligerent forces on land or sea' in neutral territory,[1242] ports, and seas.[1243] They cannot '[u]se any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages'. Moreover, the non-ratified Hague Air Rules affirm that the neutral state must prevent aerial and sea observation in its jurisdiction.[1244] These rules have never been adopted, but their transformation in CIL is disputed.[1245]

Disagreements arise regarding cyber-spying. As Blank notes, whether it may be considered as direct participation in hostilities is 'more complicated'.[1246] Gaul refers to the provisions of The Hague Air Rules: '[t]he premise is easily extended to the digital battlefield […] If physical surveillance is disallowed, so too is digital surveillance. Therefore, a belligerent's use of neutral Internet infrastructure to conduct intelligence gathering on enemy forces will violate the principle of neutrality'.[1247] Heintschel von Heinegg relies on articles 1, 2, and 3 of Hague V

[1242] Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, (Adopted:18.10.1907–EIF:26.01.1910) art.3.

[1243] Hague XIII, art.5.

[1244] Hague Air Rules, art.XLVII.

[1245] For two contradictory views, see: Roscini (n.961) 247; Natalino Ronzitti, 'The Codification of Law of Air Warfare, in Natalino Ronzitti and Gabriella Venturini (eds), *The Law of Air Warfare: Contemporary Issues* (Eleven International Publishing 2006) 7-8.

[1246] Blank (n.970) 430.

[1247] Allison Gaul, 'Neutrality in the Digital Battle Space: Applications of the Principle of Neutrality in Information Warfare' (2013) 29 Syracuse J.O.S.T. 51, 93.

and articles 1, 2, and 5 of Hague XIII. According to him, '[i]t follows from the foregoing that cyber infrastructure located within the territory of a neutral State is protected against harmful interference by the belligerents'.[1248] However, 'mere intrusion into neutral cyber infrastructure is not covered by this prohibition, because international law does not prohibit espionage'.[1249] According to Woltag, '[i]t is […] reasonable to argue that the routing of CNA through neutral networks is a legitimate use thereof'.[1250] Bothe affirms that 'it is a non-neutral service for a neutral State to place at the disposal of a party to the conflict telecommunication installations not available to it under normal conditions (for instance its own military telecommunication infrastructure) or if it creates, or acquiesces in the creation of, new telecommunication infrastructure for the particular purposes of a party to the conflict'.[1251] Rules 91 and 92 of the Tallinn Manual suggest that '[t]he exercise of belligerent rights by cyber means' is prohibited, when 'directed against neutral cyber infrastructure' or 'in neutral territory'.[1252]

Roscini establishes a corpus of provisions drawn from The Hague Conventions, as well as British, German, and HPCR manuals.[1253] He considers that 'belligerents must "abstain, in neutral territory or neutral waters, from *any act* which would, if knowingly permitted by any Power, constitute a violation of neutrality'[1254] and should not commit '*any act of hostility*',[1255] '*hostilities*',[1256] or '*any hostile actions'*,[1257] in '*neutral territory*'. He refers to similar provisions from the 'UK *Manual of the Law of Armed Conflict'*,[1258] 'section 1108 of the German Military

[1248] Heintschel von Heinegg (n.159) 145-6.

[1249] Ibid.

[1250] Johann-Christoph Woltag, 'Cyber Warfare' (2010) M.P.E.P.I.L., [18].

[1251] Michael Bothe, 'Neutrality, Concept and General Rules' (2015) M.P.E.P.I.L., [51].

[1252] Schmitt, *Tallinn Manual* (n.52) 251.

[1253] Roscini (n.961) 254-5.

[1254] Ibid 255. Roscini refers to Hague XIII, art.1.

[1255] Ibid. Roscini refers to Hague XIII, art.2.

[1256] Ibid. Roscini refers to the HPCR Manual, rule 166.

[1257] Ibid. Roscini refers to the HPCR Manual, rule 167(a).

Manual'[1259] and 'Rule 171(d) of the HPCR Manual'.[1260] according to him, '[t]he references in the above documents to acts of hostilities, military operations, hostile actions, and any activity that contributes to the "warfighting effort" suggest that cyber-exploitation is also prohibited on neutral's territory, at least when it aims to obtain tactical intelligence'.[1261] Article 47 of The Hague Air Rules and Rule 171(b) of the HPCR Manual allegedly confirm his theory.[1262]

He then tackles a second issue: 'the neutrals' duty not to tolerate certain belligerent activities on their territory', which is 'absolute on land' but of 'due diligence' in 'maritime neutrality'.[1263] He underlines that '[t]his lower standard is due to the different characteristics of the respective domains of warfare'.[1264] He thus suggests that, '[b]ecause of its evanescent characteristics and the difficulty of exercising jurisdiction over it, the situation seems to have more in common with the maritime and air domain than with land warfare. In the cyber domain too, then, the neutral's duty not to allow certain activities on their territory should be an obligation of conduct, not of result'.[1265]

As to the routing of cyber-operations through a neutral territory, he mentions that 'neutral states have only an obligation to use the means at their disposal to prevent violations of their neutrality'.[1266] He highlights that, '[u]nlike the situation of cyber operations originating from neutral cyber infrastructure, it is difficult to see how a neutral state could have the means to prevent routing of data and malware through its territory, or even in most cases be aware of it'.[1267]

[1258] Ibid.

[1259] Ibid

[1260] Ibid.

[1261] Ibid.

[1262] Ibid.

[1263] Ibid 257.

[1264] Ibid.

[1265] Ibid.

[1266] Ibid 260.

[1267] Ibid.

The doctrinal conclusions reached are thus diverse with respect to these articles, and are actually more homogenous when it comes to article 8 of Hague V, and articles 7 and 10 of Hague XIII.

B. Arguments based on article 8 of Hague V, and articles 7 and 10 of Hague XIII

According to article 8 of The Hague Convention V, '[a] neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals'. Restrictions must just 'be impartially applied by it to both belligerents'. According to articles 7 and 10 of Hague XIII, neutrality 'is not affected by the mere passage through its territorial waters of war-ships or prizes belonging to belligerents', while the state is not required 'to prevent the export or transport, on behalf of one or other of the belligerents, of arms, munitions of war, or […] of anything which can be of use to an army or a fleet'.

Kish and Turns refer to article 8 of Hague V, and think that '[t]he Convention thus essentially allows the belligerent use of neutral communications systems for espionage. Consequently neutrality restricts, but does not prohibit, belligerent espionage on neutral territory'.[1268] According to Hostettler and Danai, '[i]t might be seen as a problem that the existing law of neutrality is mostly applied as customary law, which means that the rules are not clearly elaborated'.[1269] However, they suggest that '[o]ld rules must be interpreted by analogy: where Hague Conventions mention wireless telegraphy, we have to interpret that these rules would apply to modern communication technology as it stands today and as it will develop tomorrow'.[1270] Nevertheless, the Internet 'is posing new problems', because it 'may be used for military purposes and its infrastructure is partly also based in neutral territory'.[1271] Bothe also notices that rules of Hague

[1268] Kish and Turns (n.66) 125.

[1269] Olivia Danai and Peter Hostettler, 'Neutrality in Land Warfare' (2015) M.P.E.P.I.L., [23].

[1270] Ibid.

[1271] Ibid [24].

Convention V 'do not address modern problems of telecommunication with the necessary clarity, but they contain principles that remain valid and applicable today'.[1272] 'A neutral State is not obliged to bar the use' of 'data communication infrastructure' by 'parties to a conflict even if that use is of a military nature'.[1273]

Doctrine, thus, appears to be based on the analogy between cyber-espionage and existing concepts of JIB. However, the application of the VCLT rules reveals a different status of law.

2. Status of law

The rules concerning belligerents (2.1) and the rules involving a neutral state (2.2) are to be alternatively tackled.

2.1. The rules concerning belligerents

Applying JIB to cyber-espionage is complicated by two aspects. First, a textual interpretation does not support its application to cyber-espionage (A), while subsequent state practice does not support the entire application of JIB in cyberspace (B). A conclusive note ends this section (C).

A. A textual interpretation does not support the application of jus in bello to cyber-espionage

The terms used in Hague II (1889) and Hague IV (1907) are defined (a) and the same task is then carried out for the terms of Additional Protocol I (1977) (b). However, this research reveals that they are not directly applicable to cyber-espionage, and focus on territory and land (c).

[1272] Bothe (n.1251) [50].

[1273] Ibid.

a. Hague II (1889) and Hague IV (1907)

Article 29 of Hague II (1899) and Hague IV (1907) tackle spying in a similar fashion. In the 1899 version, '[a]n individual can only be considered a spy if, acting clandestinely, or on false pretences, he obtains, or seeks to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party. Thus, soldiers not in disguise who have penetrated into the zone of operations of a hostile army to obtain information are not considered spies'. In the 1907 version, '[a] person can only be considered a spy when, acting clandestinely or on false pretences, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party. Thus, soldiers not wearing a disguise who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, are not considered spies'. They both mention that soldiers or civilians carrying out their mission 'openly'–delivering 'dispatches' and maintaining 'communications'–are not spies.

The term 'false pretences' means 'pretending that a certain condition or circumstance was true'.[1274] 'Clandestine' means '[s]ecret or concealed, esp. for illegal or unauthorized purposes'.[1275] Disguise is defined as an '[a]pparel worn to conceal one's identity',[1276] while uniform is defined as '[a] distinctive dress of uniform cut, materials, and colour worn by all the members of a particular naval, military, or other force to which it is recognized as properly belonging and peculiar'.[1277] 'Information' may mean '[k]nowledge communicated concerning some particular fact, subject, or event; that of which one is apprised or told; intelligence, news'.[1278] It originates from the provisions that spies may be soldiers

[1274] 'on/under false pretenses' (Merriam-Webster) <www.merriam-webster.com/dictionary/false%20pretenses> accessed:15.05.2017.

[1275] Black's (n.863) 'clandestine'.

[1276] Ibid 'disguise'.

[1277] 'uniform' (O.E.D-Online, O.U.P. 2017).

[1278] 'information' (Oxford Living Dictionary) <en.oxforddictionaries.com/definition/information> accessed:14.05.2017.

('[o]ne who serves in an army for pay', 'takes part in military service or warfare')[1279] or civilians ('[a] person not serving in the military').[1280]

The context of article 29 of Hague II and Hague IV is the following: article 1 mentions that 'Contracting Powers shall issue instructions to their armed land forces which shall be in conformity with the Regulations respecting the laws and customs of war on land, annexed to the present Convention'. References to territories are recurrent in the annexed regulations: they appear in articles 2, 8, 42, 44, 45, 48, and 49. It goes the same way for concepts that may only be conceived of in the context of a territory: 'horses' (article 4), 'town, fortress, camp' (article 5), 'towns', 'villages', and 'buildings' (article 25). Moreover, Contracting Parties intended to regulate each domain with separate instruments. In 1899, instead of automatically applying Hague II to other fields, instruments were tailor-made for maritime (Hague III) and aerial warfare (Declaration IV-1). The same was done eight years later, as some conventions were designed for the sea (VI, VII, VIII, IX, X, XI) and one for airspace (XIV).

The titles of Hague II (1899) and Hague IV (1907) reveal their identical purpose: defining the 'Regulations concerning the Laws and Customs of War on Land'. Land is '[a]n immovable and indestructible three-dimensional area consisting of a portion of the earth's surface, the space above and below the surface, and everything growing on or permanently affixed to it'.[1281]

It is, thus, obvious that the concept of wartime spy, as defined in Hague II (1899) and Hague IV (1907), is only applicable to land, and is intrinsically territorial. It hardly extends to cyberspace. Similar reasoning applies to the forms of spies defined in the Additional Protocol I

[1279] 'soldier' (O.E.D-Online, O.U.P. 2017).

[1280] Black's (n.863) 'civilian'.

[1281] Ibid 'land'.

b. Additional Protocol I (1977)

Additional Protocol I to the Geneva Conventions (1977) is a '[p]rotocol additional to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflicts'. There are actually four 'Geneva Conventions of 12 August 1949': Convention (I) on Wounded and Sick in Armed Forces in the Field, Convention (II) on Wounded, Sick and Shipwrecked of the Armed Forces at Sea, Convention (III) on Prisoners of War, and Convention (IV) on Civilians. While some provisions of the Additional Protocol are general in nature, and apply to any battlefield (articles 12, 18, 37-41, part IV etc.), others are specific to land (article 21) or maritime (article 22, 23 etc.) warfare.

Article 46 of the Additional Protocol I deals with '[s]pies'. This article is placed in Part III, Section II, which tackles 'Combatant and Prisoner-Of-War Status'. Article 46 has similarities with the provisions of Hague law, and three different categories of spies may be identified in this article.

A first category is '[a] member of the armed forces of a Party to the conflict who, on behalf of that Party and in territory controlled by an adverse Party, gathers or attempts to gather information'. Such activity does not constitute espionage 'if, while so acting, he is in the uniform of his armed forces'.
The geographical scope of this first category is 'a territory controlled by an adverse party'. Both gathering and the attempt to gather information are punished. Whether the operation was successful or not is thus of little importance. As the type of information is not mentioned, the terms must thus be understood as any information. Spies do not wear any uniform, which was previously defined.[1282]

A second category is '[a] member of the armed forces of a Party to the conflict who is a resident of territory occupied by an adverse Party and who, on behalf of the Party on which he depends, gathers or attempts to gather information of

[1282] 'uniform' (n.1277).

military value within that territory'. Such activity does not constitute espionage 'unless he does so through an act of false pretences or deliberately in a clandestine manner'. He must be 'captured while engaging in espionage'.

The geographical scope changes for this second category. It is now 'a territory occupied by an adverse party' which is at stake. An 'occupied territory' refers to a '[t]erritory that is under the effective control and authority of a belligerent armed force'.[1283] As sovereignty 'over the territory' is not transferred 'to the occupying power', 'international law must regulate the interrelationships between the occupying force, the ousted government, and the local inhabitants for the duration of the occupation'.[1284] Another change concerns the quality of the spy: he is a 'resident' of this occupied territory. A resident is '[a] person who resides permanently in a place; a permanent or settled inhabitant of a town, district, etc.'.[1285] Moreover, the type of information is specified: 'information of military value', i.e. information '[o]f, relating to, or involving the armed forces', or 'war'.[1286] There is no reference to uniform, but to 'false pretences' or 'a clandestine manner', as in The Hague Conventions. Information gathering must, however, be deliberate, i.e. '[c]onsciously and intentionally'.[1287] This nuance may be easily explained: 'residents who are members of armed forces "will almost necessarily in their everyday life come across information of value to the armed forces to which they belong, and this should not make them spies or serve as a pretext for denying them protection as prisoners of war"'.[1288]

A third category is '[a] member of the armed forces of a Party to the conflict who is not a resident of territory occupied by an adverse Party and who has

---

[1283] Black's (n.863) 'territory'.

[1284] Eyal Benvenisti, 'Occupation, Belligerent' (2009) M.P.E.P.I.L., [1].

[1285] Black's (n.863) 'resident'.

[1286] Black's (n.863) 'military'.

[1287] 'deliberately' (Oxford English Dictionary) <en.oxforddictionaries.com/definition/deliberately> accessed:16.05.2017.

[1288] Jean De Preux, 'article 46–Spies', in ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12.08.1949* (Kluwer 1987) 569.

engaged in espionage in that territory'. He must be captured 'before he has rejoined the armed forces to which he belongs'.
This third category of spy still acts on occupied territory, but he 'is not a resident' and engages in 'espionage'. The difference between 'espionage' and the clandestine gathering or attempt to gather information is unclear; the latter could be a suitable definition of the former.

c. The centrality of territory and land in The Hague and Geneva rules

For both of them, a central notion is either land or territory. The textual interpretation carried out previously seems to indicate that territory cannot be anything other than physical. As cyberspace is not a physical concept, The Hague and Geneva rules seem hardly applicable to it. An analysis of the subsequent state practice confirms this conclusion.

B. Subsequent state practice does not support the entire application of jus in bello in cyberspace

This lack of support may be found in two aspects of JIB, both substantial (a) and geographical (b).

a. State practice on the substantial aspect of *jus in bello*

This practice is heterogeneous, and the following conduct may be identified: some states support a global implementation of *jus in bello* in cyberspace (i), others define minimal standards to respect (ii), or acknowledge the impossibility to apply some concepts (iii). A few states acknowledge the lack of consensus surrounding the transposition of *jus in bello* to cyberspace (iv), while many of them prioritize the definition of rules of engagements (v), and some even demand new rules (vi).

i. States supporting a global implementation of *jus in bello* in cyberspace

Spying is expressly authorized by the law of war, and doctrine resorts to analogical reasoning. Should states recognize that IHL is applicable in cyberspace–and without excluding some provisions or expressing doubts–there would be less uncertainty regarding the applicability of their provisions to cyber-espionage.

Eight states and various institutions of the EU consider existing IHL as applicable in cyberspace. The USA considers that the law of war applies,[1289] and expressly quotes distinction, discrimination, and proportionality.[1290] The Dutch government and intelligence services both agree 'that applying the rules of international humanitarian law (*jus in bello*) to hostilities in cyberspace is "technically feasible and legally necessary"'.[1291] However, 'armed attacks in cyberspace only fall under international humanitarian law if they are carried out in the context of an armed conflict by the parties to that conflict', which 'constitutes an important distinction with regard to other cyber-attacks'.[1292] The 'principles of distinction, proportionality and the taking of precautionary measures' must also be respected.[1293] Croatian '[n]ational interest and all the necessary activities will be pursued according to the principles, values and obligations based on […] international humanitarian law'.[1294] Chile makes a similar statement regarding its own 'planning, conduct and execution of operations in cyberspace'.[1295] Belgium claims 'the right to respond immediately with a counter cyber-attack in accordance with the provisions of the law of armed conflict'.[1296] According to various EU institutions, '[i]f armed conflicts

[1289] DoD/OGC, 'Law of War Manual' (n.1073) 994-999.

[1290] UNGA, 'Developments' (15.07.2011) (n.141) 19.

[1291] Dutch Government, 'Government response to the AIV/CAVV' (n.1082) 5.

[1292] Ibid.

[1293] AIV/CAVV (n.213) 36.

[1294] Croatia (n.933) 23.

[1295] Chilean MND, 'Aprueba' (n.103) 4.

[1296] L.R&S, art.11(2).

extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights law will apply to the case at hand'.[1297] Australia,[1298] Canada[1299] and the UK also acknowledge such applicability.[1300]

Three states demand more reflection on the topic. Switzerland affirms that 'in principle, international humanitarian law is applicable to combat actions', but acknowledges that 'many legal questions have still to be answered', which requires 'a comprehensive analysis of technical and practical aspects'.[1301] 'Japan is of the view that existing international law, including [...] international humanitarian law, naturally applies to acts in cyberspace',[1302] but asks for further work on the topic.[1303] Spain describes the applicability of the LOAC in cyberspace as a 'major problem'.[1304]

In contrast, some States have chosen to define minimal standards to be respected in cyberspace.

ii. States defining minimal standards to respect

The Russian armed forces 'are guided' by 'international humanitarian law' in the 'global information space'.[1305] However, IHL is understood as 'limiting the indiscriminate use of the information weapons; establishing a special protection

---

[1297] European Commission (n.97) 16.

[1298] UNGA, 'Developments' (30.06.2014) (n.95) 2.

[1299] Canada, 'Developments' (n.91) [2].

[1300] FCO (n.930) 7-8.

[1301] Caflisch, Pratique Suisse 2009 (n.689) 564.

[1302] ISPC, 'International Strategy' (n.929) [4.3.2].

[1303] UNGA, 'Developments' (19.07.2016) (n.93) 11-12.

[1304] Spanish Government, 'Informe Anual de Seguridad Nacional' (2013) 38 <www.dsn.gob.es/sites/dsn/files/Informe_Seguridad_Nacional%202013.pdf> accessed:29.10.2017.

[1305] Russian MOD (n.85) [2.1].

for the information objects that are potentially harmful sources of man-made disasters; prohibiting treacherous methods of information warfare'. [1306] According to the AIV and the CAVV, only '[c]yber attacks that are more than sporadic, isolated armed incidents and that (could) result in loss of life, injury, destruction or prolonged damage to physical objects may be qualified as armed conflict within the meaning of the humanitarian law of war'. [1307] Qualified as such is a cyber-attack that 'causes destruction or prolonged and serious damage to computer systems that manage critical military or civil infrastructure, or seriously compromises the state's ability to perform essential public functions and hence causes serious and long-lasting damage to the economic or financial stability of the state and its population'.[1308]

Conversely, some states acknowledge the impossibility of applying some concepts in cyberspace.

iii. States acknowledging the impossibility of applying some concepts

As revealed previously, The Hague and Geneva rules contain precise requirements regarding uniform and control. While supporting the application of JIB in cyberspace, the USA expresses doubts about the uniform requirement. In fact, '[i]f a computer network attack is launched from a location far from its target, it may be of no practical significance whether the "combatant" is wearing a uniform'.[1309] Tallinn Manual 1.0 and 2.0 both acknowledge that 'there is no legal notion of occupation of cyberspace'.[1310] Furthermore, 'cyber-operations cannot alone suffice to establish or maintain the degree of authority over territory necessary to constitute an occupation'.[1311]

[1306] Ibid.

[1307] AIV/CAVV (n.213) 24.

[1308] Ibid.

[1309] DoD/OGC, 'An Assessment' (n.676) 8.

[1310] Schmitt, *Tallinn Manual* (n.52) 239; Schmitt, *Tallinn Manual 2.0* (n.53) 543.

[1311] Schmitt, *Tallinn Manual* (n.52) 239; Schmitt, *Tallinn Manual 2.0* (n.53) 543.

Moreover, some states acknowledge the lack of consensus surrounding the application of JIB in cyberspace.

iv. States acknowledging the lack of consensus surrounding the application of *jus in bello* in cyberspace

While urging on a consensus about the application of the LOAC, states are usually aware that their own interpretation is everything but binding. Canada mentions that 'there is no guarantee that any future adversary will abide by, or interpret international laws regarding conflict in a similar manner to how the CAF [Canadian Armed Forces] or any of Canada's traditional allies might'.[1312] Japan thinks that 'the international community has yet to form a consensus on the definition and status of cyber-attacks under international law including the recognition of cyber-attacks as armed attacks'.[1313] After ascertaining the lack of international treaties on cyberspace and mentioning that cyber-incidents are only handled 'in a fragmented manner', Finland notes that '[t]here has been more international legal debate on this complex topic in recent years' which 'will probably result in new legal interpretations on the assessment of cyber incidents at the state level or in IO'.[1314] However, 'these interpretations will not be legally binding on states, but, they will indicate the objectives which the states participating in the arrangements are prepared to adopt'.[1315]

Germany confesses that states sail on troubled waters, and are left to deal with situations on a case-by-case basis. 'Since the basic provisions of LOAC (1949

[1312] DND, *The Future Security Environment 2013-2040* (n.116) 109.

[1313] Japanese MOD, 'Defence of Japan 2012' (2012) 93 (footnote 2) <www.mod.go.jp/e/publ/w_paper/pdf/2012/14_Part1_Chapter2_Sec2.pdf> accessed:15.05.2017;
Japanese MOD, 'Defence of Japan 2013' (2013) 82 (footnote 2) <www.mod.go.jp/e/publ/w_paper/pdf/2013/17_Part1_Chapter2_Sec1.pdf> accessed:15.05.2017.

[1314] DEFMIN (n.106) 33.

[1315] Ibid.

Geneva Convention, 1977 Additional Protocols) were laid down at a time when military cyber-operations were only just emerging, no explicit rules for such cases were contained in these provisions. There may thus be problems of definition or interpretation in individual cases (e.g. definition of an attack, distinction between civilian and military objectives, determination of territories of the Parties to the conflict in cyberspace). In every individual case, the situation will thus have to be carefully assessed'.[1316]

As underlined by Finland, '[n]o rules of engagement exist for cyber-operations'.[1317] Analysing practice reveals that defining rules of engagement (ROE) is actually their priority.

v. States prioritizing the definition of rules of engagement

As affirmed by O'Donnell and Kraska, '[w]hile theories and approaches that emerge from academia are useful to national decision-makers contending with these issues, they may be of limited value to operational commanders [...] the legal and policy research surrounding CNA often raises more questions than it answers'.[1318] A deeper study actually reveals that states promote ROE, which is– by far–their main concern. 'ROE are issued by competent authorities and assist in the delineation of the circumstances and limitations within which military forces may be employed to achieve their objectives'.[1319] They 'appear in a variety of forms in national military doctrines, including execute orders, deployment orders, operational plans, or standing directives. Whatever their form, they provide authorisation for and/or limits on, among other things, the use of force, the positioning and posturing of forces, and the employment of certain specific

[1316] Federal MOD, 'Law of Armed Conflict Manual' (2013) ZDv 15/2, [486] <www.bmvg.de/resource/blob/16630/ae27428ce99dfa6bbd8897c269e7d214/b-02-02-10-download-manual--law-of-armed-conflict-data.pdf> accessed:14.05.2017.

[1317] DEFMIN (n.106) 33.

[1318] James Kraska and Brian O'Donnell, 'International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement' (2002) 76 I.L.S. 395, 398.

[1319] IIHL, *Sanremo Handbook on Rules of Engagement* (IIHL 2009) [3].

capabilities'. [1320] 'Conventional national rules of engagement have a dual purpose': expressing 'policy objectives (to delineate how force could be used to further national policy and to preclude actions that could be contrary to national policy)' and ensuring 'that actions do not offend international law'.[1321] They "convert" humanitarian rules into operational rules.[1322]

Australia underlines that '[t]he conduct of Info Actys [information activities] often involves complex legal and policy questions' but 'must comply with [...] the rules of engagement'.[1323] Canada is even more explicit. It mentions that 'the Army would not want to bomb a hospital' and would similarly 'not want to manipulate the cyber environment in such a way that a hospital's power supply is wiped out by an unintended downstream effect'.[1324] As a consequence, '[i]f an offensive cyber-operation is launched against a legitimate military target, it must be considered as being no different than a traditional EW [electronic warfare] operation and would follow appropriate ROE and national policies'.[1325] It then repeats this need, as '[c]omplete integration of new technological means will continuously require the Rules of Engagement'.[1326] France underlines the need to elaborate 'proper rules of engagement, taking account [of] legal consideration linked to this new environment'.[1327] The USA affirms that 'when we do take action–defensive or otherwise, conventionally or in cyberspace–we operate under rules of engagement that comply with international and domestic law'.[1328]

[1320] Ibid.

[1321] Hugh Stanton Watson, 'Armed Conflict and Humanitarian Intervention–International Standard Rules of Engagement' (2000) Austl.Int'l.L.J. 151, 173.

[1322] Ibid.

[1323] Australian Defence Force, 'Operation Series–Information Activities' (2013) 3.13, [3.8] <www.defence.gov.au/FOI/Docs/Disclosures/330_1314_Document.pdf> accessed:03.05.2017.

[1324] Canadian Army Land Warfare Centre (n.937) 5-31.

[1325] Ibid.

[1326] DND, *The Future Security Environment 2013-2040* (n.116) 135.

[1327] Commission du livre blanc (n.119) 53.

[1328] Ash Carter, 'Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity' (2015) <http://archive.defense.gov/speeches/speech.aspx?SpeechID=1935> accessed:22.11.2017.

Moreover, 'cyberspace operations are executed with a clear mission and under clear authorities'.[1329] Yet, '[a]s with all of the activities that DoD pursues in the physical world, cyberspace operations are executed with a clear mission and under clear authorities, and they are governed by all applicable domestic and international legal frameworks […]'. [1330] Japan thinks that the lack of consensus surrounding the application of IHL makes 'it difficult to apply the existing ROE of armed forces in response to cyber-attacks'.[1331]

While some states ask for the definitions of ROE in cyberspace, others demand new rules.

vi. States demanding new rules

China has never acknowledged the extension of the LOAC to cyberspace.[1332] As a matter of fact, it 'supports the protection of civilians and the limitations of suffering during war–a key basis for LOAC–but appears to prefer the development of a separate cyber-specific regime to limit suffering and protect civilians during hostilities'.[1333] Russia also plans 'to promote formulation and adoption by Member States of the United Nations of international regulation concerning the use of principles and standards of international humanitarian law in the use of information and communication technologies'.[1334] Paradoxically,

---

[1329] DOD Cyberspace Policy Report, 'A Report to Congress' (n.1134) 1.

[1330] Ibid 1.

[1331] Japanese MOD, 'Defence of Japan 2013' (n.1313) 82 (footnote 2); Japanese MOD, 'Defence of Japan 2012' (n.1313) 93 (footnote 2).

[1332] DoD, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012' (2012) 9 <www.defense.gov/Portals/1/Documents/pubs/2012_CMPR_Final.pdf> accessed:05.09.2016.

[1333] Kimberly Hsu and Craig Murray, 'China International Law in Cyberspace' (2015) 6 <www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf>

[1334] Security Council of the Russian Federation, 'Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020' (2013) [12-d] <www.ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf> accessed:22.08.2016.

Canada acknowledges the applicability of IHL to cyberspace, but adds that '[t]here is probably already a need to revisit the existing provisions in [...] the law of conflicts, and agreements such as the Geneva Convention'.[1335]

The diversity of state practice regarding the application of the substance of the JIB to cyberspace has been revealed. However, analysing the geographical aspect of JIB is of equal importance.

b. States' practice on the geographical aspect of jus in bello

This state practice is interesting, as states tend to define cyberspace as a different domain from territory (i). Moreover, Canada provides guidelines on the distinction of environments (ii).

i. States defining cyberspace as a different domain

States are almost unanimous regarding the different nature of cyberspace. Most of them qualify cyberspace as a 'fifth domain', rather than 'land' or 'territory'. This subsequent practice is thus essential to differentiate cyberspace from the traditional battlefield.

'[F]rom a military perspective, environments include maritime, land, air and space, and cyberspace' in the British Army.[1336] The USA develops a similar approach.[1337] France describes cyberspace as 'a new field of action',[1338] 'an area of confrontation as such' and identifies 'five environments (earth, air, sea, outer space and cyberspace)'.[1339] Germany defines 'an overall objective': the 'ability of the *Bundeswehr* as a whole to deliver effects in all domains–land, air, sea, cyber

[1335] Canadian Army Land Warfare Centre (n.937) 2-37, 2-38.

[1336] MoD, 'Land Operations' (n.1185) G-2.

[1337] DoD, 'Summary of the 2018 National Defense Strategy' (2018) 3.

[1338] Commission du livre blanc (n.119) 53.

[1339] Commission du livre blanc, *French White Paper* (n.699) 43, 82.

and information, and space'.[1340] Australia defines a 'domain' as follows: '[w]ithin the operational environment, a medium with discrete characteristics in which, or through which, military activity takes place'.[1341] It underlines that 'domains are physical (maritime, land, air and space) and non-physical (information, including cyberspace and the electromagnetic spectrum, and human)'.[1342] The Czech Republic defines cyberspace as 'a very specific environment that has no geographic borders and in which the distance between the source of threat and the potential target becomes relative'.[1343] According to India, 'space is a medium like land, sea, air and cyber through which various activities are likely to expand in the future'.[1344] Slovakia affirms that '[c]yberspace has become a new operational domain of conducting combat activity'.[1345] Lithuania thinks that '[f]uture conflicts will take place in both physical and virtual domains: land, air, sea, space, and cyberspace'.[1346] According to Slovenia, '[i]n addition to land, sea and air, the future theatre of war will also include cyberspace and outer space'.[1347] Norway defines four combat domains: cognitive, information, social, and physical. The second one includes cyber, while the fourth one 'covers the traditional arenas for military operations: land, sea, air and space'.[1348] Cyberspace

---

[1340] Federal MOD, 'White Paper on German Security Policy and the Future of the Bundeswehr' (2016) 102 <www.bundeswehr.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NzE3MzM1Njc2NDYyMzMyMDIwMjAyMDIw/2016%20White%20Paper.pdf> accessed:12.10.2016.

[1341] Australian Defence Force (n.1323) Glossary and Terms.

[1342] Ibid.

[1343] Czech MFA, 'Security Strategy of the Czech Republic 2015' (2015) 13 <www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf> accessed:14.05.2017.

[1344] Indian MOD, 'Joint Doctrine Indian Armed Forces' (2017) 26 <http://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf> accessed:15.05.2017.

[1345] Slovakian MOD, 'White Paper on Defence' (n.1135) [44].

[1346] Lithuanian MND, 'The World 2030' (2013) 38 <https://kam.lt/download/35262/gl-111_world%202030_elektroninis.pdf> accessed:15.05.2017.

[1347] Slovenian National Assembly, *Resolution on the National Security Strategy of the Republic of Slovenia* (Ministry of Defence 2010) [4.2.7].

[1348] Norwegian Defence Command and Staff College, *Norwegian Armed Forces Joint Operational Doctrine* (The Defence Staff 2007) [0408]-[0413].

is also qualified as 'a new area, in which various conflicts of different nature, national and international, occur'.[1349] Cyberspace is defined by Israel as 'another area of combat',[1350] along 'four dimensions (land, sea, air, and cyber)'.[1351] Mexico also considers cyberspace as another 'dimension of operation'.[1352] Canada even predicts that the identification of new dimensions is unlikely to stop: '[t]he discovery of new spatial dimensions beyond the traditional three dimensions of the physical plane (up/down, left/right, and in/out) will fundamentally change our perception of physical space'. [1353] Slovakia shares this idea, as '[u]nconventional domains and spaces (informational, electromagnetic, cybernetic, cosmic and nano-technological) will be drawn towards the centre of gravity of military activities, depending on the speed of technological advance of specific security actors'.[1354] According to Guatemala, 'besides the domestic and foreign physical areas, a new dimensionless area exists for purposes of war: cyberspace'. [1355] Chile suggests that 'concepts such as terrestrial battlefield, maritime area and airspace have evolved over the last years to the point of integration in a unique battlespace that […] also includes the electromagnetic spectrum and the recent notion of cyberspace'.[1356]

Interestingly, the Netherlands considers cyberspace as a 'fifth domain for military action' but denies 'that it is a distinct "space" that has no relationship to

---

[1349] Chilean MND, 'Ciberdefensa' <www.defensa.cl/temas-de-contenido/ciberdefensa/> accessed:06.01.2018.

[1350] Belfer Center, *Deterring Terror–How Israel Confronts the Next Generation of Threats* (Belfer Center 2016) 44.

[1351] Ibid 12.

[1352] Presidencia, 'Programa Sectorial de Defensa Nacional 2013-2018' (2013) [1.6.5] <www.sedena.gob.mx/archivos/psdn_2013_2018.pdf> accessed:18.05.2017.

[1353] Canadian Army Land Warfare Centre (n.937) 5-10.

[1354] Slovakian MOD, 'White Paper on Defence' (n.1135) [44].

[1355] Guatemalan MOD (n.172) 12.

[1356] Chilean MND, 'Libro de la Defensa Nacional de Chile' (2010) Part 4, 176 <www.defensa.cl/media/2010_libro_de_la_defensa_4_Parte_Politica_Militar.pdf> accessed:20.09.2017.

time, place or human action'.[1357] It is, in fact, 'nothing more or less than the sum of all ICT equipment and services'.[1358] '[C]yberspace can be regarded as a fifth theatre of operations–albeit one with specific characteristics–that interacts with the other four domains of military operation: land, sea, air and space. Operations in the fifth domain can therefore act as a force multiplier in the other domains'.[1359] Then, '[a]ctivity in the other domains, incidentally, is now barely even possible without the use of digital equipment'.[1360] According to the Netherlands, '[w]ars were originally fought only on land and at sea. At the beginning of World War I, aerial warfare added a third domain. A fourth–space–acquired operational significance in the 1980s with the development of anti-satellite missiles and the Strategic Defence Initiative ("Star Wars"). With the development and spread of the internet and the digitisation of society in general, we can also talk of a fifth domain, the only one to have been created by man'.[1361]

In sum, cyberspace is a fifth domain, and separated from land, sea, airspace and outer-space. To help distinguishing environments, Canada provides interesting guidelines, which are worth studying.

ii. Canadian guidelines on the distinction of environments

Canada has adopted a pragmatic approach to define how environments have to be distinguished from one another: 'an operating environment may simply be thought of as the milieu in which military activities are conducted. Operating environments may be distinguished from one another based on the technology used by military personnel to operate in them'.[1362] The doctrine then goes further: '[t]he traditional environments of land, air, and maritime are distinct and

[1357] AIV/CAVV (n.213) 12.

[1358] Ibid.

[1359] Ibid.

[1360] Ibid.

[1361] Ibid.

[1362] Canadian Army Land Warfare Centre (n.937) 5-3.

will continue to be distinct in the future. The division exists because different technologies–and therefore unique supporting equipment, skill sets, and training–are required to physically operate within these distinct environments. Sometimes the lines between operating environments can blur. The physical land environment, for example, may include water (swamps, streams, rivers, and landlocked bodies of water). Those features, however, differ significantly from blue water oceans. Blue water requires distinct technologies–both surface and subsurface–in which to operate. Land forces are ill suited to navigating maritime shipping lanes, and naval ships are similarly undesirable for swamp or riverine operations. Thus, land and maritime must still be treated as distinct physical operating environments'.[1363] The same reasoning is then applied to airspace. It is even specified that '[a]rmy brigade groups or naval task groups may be structured to include helicopters in their respective orders of battle, but that is a characteristic of joint operations rather than an example of merging physical environments'.[1364]

Cyber is then tackled: '[t]he use of distinct technologies to delineate physical operating environments opens up other possibilities for environments beyond land, air, and maritime. As distinct physical components, only space and cyber need be added to round out an all-inclusive model of the physical plane'.[1365] However, the manual considers that cyber is an aspect of the electromagnetic environment; '[t]herefore, there are precisely five environments: land, air, maritime, space, and EM. The technologies required to operate in each are distinct, and each environment requires its own unique supporting equipment, skill sets, and training'.[1366]

A warning is then issued: '[t]hinking merely in terms of how space and cyber support the land, air, or maritime environments creates the potential for vulnerabilities and lost opportunities. For example, if we think of cyber only as the glue that links Command with the other operational functions, we risk marginalizing the cyber component of the physical plane, turning it into a mere

[1363] Ibid 5-2.

[1364] Ibid 5-3.

[1365] Ibid.

[1366] Ibid 5-7.

synonym for CIS–the so-called zeros and ones that only signallers should be concerned with. Thus we would miss the full range of force enhancement capabilities that cyber offers'.[1367]

C. Conclusion

Most authors resort to analogy to prove that cyber-espionage is authorized by the LOAC. However, neither a textual interpretation of The Hague and Geneva rules, nor an analysis of subsequent state practice allows one to deduce that the rules on wartime spying are applicable to wartime cyber-espionage. JIB applicability in cyberspace is still ambiguous, and states are mainly left to decide for themselves. Moreover–and as mentioned by the Swedish Defence Commission–'[t]here are [...] particular difficulties in maintaining a clear distinction between situations of peace and armed conflict in cyberspace'.[1368] Yet, the framework of an international armed conflict is an essential condition for JIB to apply. In contrast, some rules involving a neutral State are more successful in cyberspace.

2.2. The rules involving a neutral state

According to Heintschel Von Heinegg, 'if cyberspace is considered to be a new "fifth dimension," a "global common" that "defies measurement in any physical dimension or time space continuum"', it could be 'difficult to maintain that the law of neutrality applies. However, should it be acknowledged that cyberspace "requires a physical architecture to exist," many of the difficulties can be overcome'.[1369] Yet, cyberspace is actually a fifth domain and it is necessary to assess Hague V provisions on a case-by-case basis. Among them, four are regularly mentioned by doctrine–articles 1 (A), 2 (B), 5 (D), 8 (E)–while article 3 (C) appears in state practice.

[1367] Ibid 5-12.

[1368] Sweden, 'Submission by Sweden to UNGA resolution 68/243' (n.96) 6.

[1369] Heintschel von Heinegg (n.159) 143.

A. Article 1 of Hague V

Article 1 of Hague V mentions that '[t]he territory of neutral Powers is inviolable'.[1370] As demonstrated previously–and absent contradictory state practice–cyber-espionage cannot be considered a violation of sovereignty, even if directed by a belligerent against a neutral State.[1371]

The little state practice available actually focuses on cyber-attacks, and how inflicting damage to a neutral state is prohibited.

The Netherlands affirms that, '[i]n a digital context, cyber-attacks on objects or information systems in neutral territory are therefore prohibited'.[1372]

The Swiss position is clear: 'it is usually considered that cyberspace's virtual space is not subject to the rule according to which a neutral state has to prevent belligerents from accessing its territory'.[1373] Conversely, 'belligerents do not breach neutrality when their data go through neutral computer-networks during combat operations'.[1374] However, '[n]eutral state territory must be saved from combats' possible side-effects', and '[b]elligerents are thus theoretically forbidden from inflicting damage to neutral states' networks when combating through computer networks'.[1375] This conclusion results from the following reasoning: '[i]f cyberspace was considered as belonging to a State–such as airspace–the neutral State would be compelled to block belligerent's access to its computer networks. Conversely, belligerents would have to renounce to use them in a malicious way'.[1376] However, 'contrary to airplanes, data are not

[1370] A similar provision exists in article 1 of Hague XIII, preventing belligerents from committing 'in neutral territory or neutral waters', 'any act which would […] constitute a violation of neutrality'.

[1371] See Chapter I-I.

[1372] AIV/CAVV (n.213) 26.

[1373] Caflisch, Pratique Suisse 2009 (n.689) 564-5.

[1374] Ibid 565.

[1375] Ibid.

[1376] Ibid.

controlled when moving to their target. It is often impossible to determine which route takes internationally-exchanged data. It is possible to close airspace to specific airplanes but it is by far less obvious to do so for computer-networks' data'.[1377] Moreover, 'some of these data transit through satellites, which are based in outer-space, and thus escape neutrality's application scope'.[1378]

The Judge Advocate General's Legal Center and School (TJAGLCS) is linked to the US Army, but its handbook 'is not an official representation of U.S. policy regarding the binding application of various sources of law'.[1379] Yet, it interestingly mentions that '[i]t is well settled that creating cyberspace "effects" or striking a cyberspace "target" in a neutral state is a violation of that state's sovereignty unless consent is given or an exception applies'.[1380]

The Swiss position is the most reasonable, and the functioning of the Internet explains it again. Indeed, belligerents' data could perfectly be on a server located on the territory of a neutral power, but it is hard to know it. Moreover, data is constantly moving. Such is the case with cloud-computing. The following is particularly interesting: 'VM migration means moving a VM from one physical server to another and continuing the operation of VM in the latter. It may be often necessary to perform workload migration [...] An organisation can move its workload to data centers located at areas with lower power and infrastructure cost [...] For example, at night, the cooling cost of a server will be less as temperature is cooler than day time. During peak time of the day, electricity usage rate may be higher than off peak time. When it is night in a country, it may be day in some other countries. Cloud data can be moved to a cloud data center somewhere in the world which is observing night time in rotation on a 24-hour basis'.[1381]

[1377] Ibid 564.

[1378] Ibid.

[1379] TJAGLCS, 'Information Operations and Cyberspace Operations' (2015) i. <www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf> accessed:23.05.2017.

[1380] Ibid 139.

As cyber-espionage does not constitute an infringement of territorial integrity, spying on a neutral state is not contrary to article 1. This complex transposition of a land regime may also be found in the application of article 2.

B. Article 2 of Hague V

According to article 2 of Hague V, '[b]elligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power'.[1382]

At first glance, these terms seem to point to something intrinsically physical, designed to carry out kinetic actions or satisfy troops' needs. 'Troop' means '[a] body of soldiers' and 'troops', '[a]rmed forces collectively'.[1383] A convoy is usually understood as '[a] group of vehicles or vessels traveling together for safety, esp. with armed escorts'.[1384] Munitions include '[m]ilitary equipment of any kind, as weaponry, ammunition, stores, etc'.[1385]

As to supplies, their definition is the following: '[m]eans of provision or relief; stores available for distribution'.[1386] The application of the concepts mentioned in article 2 makes little sense in cyberspace, as they seem intrinsically physical.

Switzerland nevertheless adopts a more dynamic interpretation, but specific to military networks: '[a] neutral state is not allowed to support belligerents with troops or weapons. If such prohibition is applied to military CNO carried out during an armed conflict, this means that a neutral state cannot accept that belligerents use its military networks. Theoretically, military networks are

---

[1381] Al Bento, *Cloud Computing Service and Deployment Models: Layers and Management* (IGI Global 2012) 43.

[1382] The provisions of Hague XIII are a bit different: the supply of 'of war-ships, ammunition, or war material' is forbidden by article 6, while–as suggested by article 7–the neutral power is not bound to prevent their 'export or transit'.

[1383] 'troops' (O.E.D-Online, O.U.P. 2018).

[1384] Black's (n.863) 'convoy'.

[1385] 'munition' (O.E.D-Online, O.U.P. 2017).

[1386] Black's (n.863) 'supplies'.

protected and are not openly accessible'.[1387] Its interpretation is actually closer to the provisions of article 3, which is now analysed.

C. Article 3 of Hague V

Belligerents are forbidden to '[e]rect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea' and to '[u]se any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages'.[1388]

The formula 'other apparatus for the purpose of communicating with belligerent forces' is broad enough to resort to an evolutionary interpretation, which could also incorporate the Internet. It is thus possible to affirm that erecting ICT structures on the territory of a neutral state to communicate with belligerents, as well as the use of such structures–when they are not 'opened for the service of public message'–is prohibited. However, the condition of an existing 'war on land' is maintained.

Article 3 is applicable to the Internet. However, this clarity does not appear for the application of article 5.

D. Article 5 of Hague V

A form of *due diligence* may be found in article 5 of Hague V (1907). It reads as follows: '[a] neutral Power must not allow any of the acts referred to in Articles 2 to 4 to occur on its territory. It is not called upon to punish acts in violation of its neutrality unless the said acts have been committed on its own territory'.[1389]

[1387] Caflisch, Pratique Suisse 2009 (n.689) 565.

[1388] There is a similar prohibition in article 5 of Hague XIII, as they cannot 'use neutral ports and waters as a base of naval operations against their adversaries, and in particular to erect wireless telegraphy stations or any apparatus for the purpose of communicating with the belligerent forces on land or sea'.

It must be noted that article 4 makes little sense in cyberspace, as it says that '[c]orps of combatants cannot be formed nor recruiting agencies opened on the territory of a neutral Power to assist the belligerents'.

The Netherlands is the only state to acknowledge the application of *due diligence* in cyberspace, but does so without any reference to Hague V. The AIV thinks that '[w]here possible, it prevents belligerent parties from using computers or computer systems located in neutral territory and from attacking computer networks or information systems in neutral territory. A neutral state may prevent a belligerent party from using computers and information systems located in its territory or jurisdiction.[1390] Then, '[n]eutral states can take measures to prevent the transmission of military data in their territory and scan or delete data in the internet domain they control using software to identify certain data files containing malware or other cyberweapons of one of the belligerent parties. If an attack uses computer systems in the territory of a neutral state, that state can protect its neutrality by taking measures to identify the origin of the attack and take corrective action provided it does not breach other legal obligations related to respect for human rights'.[1391] 'In an armed conflict involving third parties, the Netherlands can protect its neutrality by impeding the use by such parties of infrastructure and systems (e.g. botnets) on Dutch territory. Constant vigilance, as well as sound intelligence and a permanent scanning capability, are required here'.[1392] Ultimately, the Dutch interpretation thus promotes more espionage.

Contrary to the ambiguity surrounding article 5, article 8 is a good candidate for a transposition in cyberspace.

[1389] Similarly, a neutral government 'is bound to employ the means at its disposal' to 'prevent the fitting out or arming of any vessel within its jurisdiction' that is intended to fight, as well as their 'departure from its jurisdiction' (art.8 of Hague XIII).

[1390] AIV, 'Cyber Warfare–Conclusions and recommendations' (*AIV*, 21.03.2012) [22] <https://aiv-advies.nl/6ct/publications/advisory-reports/cyber-warfare> accessed:20.05.2017.

[1391] AIV/CAVV (n.213) 26.

[1392] Dutch Government, 'Government response to the AIV/CAVV' (n.1082) 6.

E. Article 8 of Hague V

By mentioning that '[a] neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals', article 8 corresponds to cyberspace specificities and could be easily transposed. As mentioned previously, the Internet relies on 'a universal language network, called the TCP/IP protocol'.[1393] Thanks to these protocols, data packets are sent between computers and then reassembled once they reach the addressee. 'When a node receives a packet it stores it, determines the best route to its destination, and sends it to the next node on that path. If there was a problem with a node (or if it had been destroyed) packets would simply be routed around it'.[1394] The main priority of route control is speed,[1395] and packets can thus go through different states' infrastructure. Contrary to the Dutch solution proposed above, it is nearly impossible for a state to know what type of information–including cyber-attacks or cyber-espionage–goes through these infrastructures. As a consequence, it would be feasible, fair and logical for both belligerents and neutral states to apply article 8 to cyberspace. However, the transposition of this article is not a silver bullet: it has been previously highlighted that the existence of a war on land is a condition to apply the convention, and Hague V cannot give a definitive solution to cyber-spying.

[1393] Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (O.U.P. 2006) 23.

[1394] 'Paul Baran and the Origins of the Internet' (*RAND*) <www.rand.org/about/history/baran.html> accessed:27.03.2017.

[1395] 'Route Control' (*Technopedia*) <www.techopedia.com/definition/2532/route-control accessed> 26.03.2017.

Many recent military manuals evoke neutrality on land and sea but ignore cyberspace. Such is the case for Canada,[1396] France,[1397] Germany,[1398] and the UK.[1399]

As to the TJAGLCS, it fails to answer '[t]he more difficult question': 'whether the mere passage of code through a state's borders ("cyber overflight') is also a violation, even if effects are not being created in the neutral states during passage. This issue is still hotly debated and the U.S. position is classified'.[1400] It is just mentioned that–with respect to articles 8 and 9 of Hague V–'[a] limited exception exists for communications relay systems', 'so long as such facilities are provided equally to both belligerents'.[1401] The issue remains unclear in the most recent edition of the handbook.[1402] However, a clear position is given by the DOD, as rule 8 'was developed because it was viewed as impractical for neutral States to censor or screen their publicly available communications infrastructure for belligerent traffic. Thus, for example, it would not be prohibited for a belligerent State to route information through cyber infrastructure in a neutral State that is open for the service of public messages, and that neutral State would have no obligation to forbid such traffic. This rule would appear to be applicable even if the information that is being routed through neutral communications infrastructure may be characterized as a cyber weapon or otherwise could cause

---

1396 Chief of Defence Staff, 'Law of Armed Conflict at the Operational and Tactical Levels' (2001) B-GJ-005-104/FP-021 <www.fichl.org/fileadmin/_migrated/content_uploads/Canadian_LOAC_Manual_2001_English.pdf> accessed:14.05.2017.

1397 Ministère de la Défense, 'Manuel du Droit des Conflits Armés' (2012) <www.cicde.defense.gouv.fr/IMG/pdf/20130226_np_cicde_manuel-dca.pdf> accessed:15.05.2017.

1398 BDVg, 'Law of Armed Conflict–Manual' (2013) ZDv 15/2 <www.bmvg.de/resource/blob/16630/ae27428ce99dfa6bbd8897c269e7d214/b-02-02-10-download-manual--law-of-armed-conflict-data.pdf> accessed:15.05.2017.

1399 MOD, 'The Joint Service Manual of the Law of Armed Conflict' (2004) JSP 383.

1400 TJAGLCS (n.1379) 139-40.

1401 Ibid 140.

1402 TJAGLCS, 'Operational Law Handbook', (17th edn, 2017) <www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2017.pdf> accessed:15.06.2018.

destructive effects in a belligerent State (but no destructive effects within the neutral State or States)'.[1403]

Switzerland also thinks that 'by transposing article 8 of The Hague Convention', 'the neutral state is not obliged to bar access of its computer-networks to belligerents in wartime'.[1404] This is however only valid for 'networks open to the public', as military networks must not be open to belligerents and should be protected'.[1405] The Netherlands similarly affirms that '[i]f a neutral state cannot reasonably prevent the transmission of malicious data through the part of the internet in its jurisdiction, its neutrality is not violated or lost. The situation is comparable to that of a radio or telephone message transmitted through part of the global communication network located in neutral territory, which is not considered a violation of neutrality by either the belligerent party or the neutral state'.[1406]

3. Conclusion

Arguments about spying between belligerents are usually constructed in the same manner: (1) spying is a form of intelligence gathering; (2) cyber-espionage is also a form of intelligence gathering; (3) spying is authorized by the law of armed conflicts; (4) cyber-espionage is thus also authorized by the law of armed-conflict.

There is more diversity in the arguments surrounding neutral states. As to the application of The Hague Air Rules, the reasoning is usually as follows: (1) spying is a form of intelligence gathering; (2) cyber-espionage is also a form of intelligence gathering; (3) spying is prohibited by The Hague Air Rules; (4) cyber-

---

[1403] DoD/OGC, 'Law of War Manual' (n.1073) [16.4.1].

[1404] Caflisch, Pratique Suisse 2009 (n.689) 565.

[1405] Ibid.

[1406] AIV/CAVV (n.213) 26.

spying is thus also prohibited by The Hague Air Rules. Regarding the application of articles 1, 2, and 3 of Hague V, and article 5 of Hague XIII, the following reasoning is applied: (1) neutral territory is inviolable; (2) activities affecting cyber-infrastructures are a violation of neutrality; (3) cyber-espionage does not affect cyber-infrastructures; (4) cyber-espionage is not a violation of neutrality. As to article 8 of Hague V, the reasoning is as follows: (1) wireless telegraphy is a means of communication; (2) cyberspace is also a means of communication; (3) a neutral state is not obliged to prevent belligerents from using wireless telegraphy; (4) a neutral state is thus not obliged to prevent belligerents from using cyberspace.

Analogical reasoning transpires from these writings. The construction of analogy is theoretically the following: '(1) Some fact pattern A has a certain characteristic X, or characteristics X, Y, and Z; (2) Fact pattern B differs from A in some respects but shares characteristics X, or characteristics X, Y, and Z; (3) The law treats A in a certain way; (4) Because B shares certain characteristics with A, the law should treat B the same way'.[1407] This foundation is well accepted by doctrine, while some critiques,[1408] proposals to refine,[1409] or new constructions[1410] exist for other aspects of the analogical reasoning.

'The whole point of argument by analogy in law is that a rule can contribute to a decision on facts to which it is not directly applicable'.[1411] '[I]n order for an

[1407] Cass Sunstein, 'On Analogical Reasoning' (1992-3) 106 Harv.L.Rev. 741, 745; see also Scott Brewer, 'Exemplary Reasoning: Semantics, Pragmatics, and the Rational Force of Legal Argument by Analogy' (1996) 109(5) Harv.L.Rev. 923, 950.

[1408] About the lack of clarity of analogy's criteria, see John Farrar, 'Reasoning by Analogy in the Law' (1997) 9(2) Bond L.R. 149; For the need of a legal theory, see Ronald Dworkin, 'In Praise of Theory' (1997) 29 Ariz.St.L.J. 353; On the different types and nature of analogy (inductive, deductive etc.), see Trudy Govier, 'Analogies and Missing Premises' (1989) 11(3) Informal Logic 141; As to whether analogy is a way of stating or reaching a conclusion, see Frances Kamm, 'Theory and Analogy in Law' (1997) Ariz.St.L.J. 405.

[1409] Martin Golding, *Legal Reasoning* (Broadview Press 2001) 45-6.

[1410] Luís Duarte d'Almeida and Claudio Michelon, 'The Structure of Arguments by Analogy in Law' (2017) Edinburgh School of Law Research Paper No.06/2017, 18-19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2948558> accessed:21.11.2017.

[1411] Neil MacCormick, *Legal Reasoning and Legal Theory* (Clarendon Press 1978) 155. See also Silja Vöneky, 'Analogy in International Law' (2008) M.P.E.P.I.L., [1].

argument by analogy to be compelling [...] there must be sufficient warrant to believe that the presence in an "analogized" item of some particular characteristic or characteristics allows one to infer the presence in that item of some particular other characteristic'.[1412] According to Juthe, good analogical reasoning is where 'the contents of the premises and the conclusion are adequately related, that the premises provide adequate evidence for the conclusion and that the premises are true, probably or otherwise reliable'.[1413] Then, '[t]he premise that states the analogy is […] the crucial premise for argument by analogy'.[1414] Moreover, '[t]wo objects are analogous if and only if there is a one-to-one correspondence between the elements of the objects'.[1415]

Authors have accepted the legitimacy of analogy with respect to cyber-espionage, and assume it works. Unfortunately, the problem with these examples of analogical reasoning is that they rely on a wrong presumption: that cyberspace and land are similar.

This idea is rejected by states. The military have long acknowledged that cyberspace is something different, a 'fifth' environment, domain or space. Even if more governments acknowledge that public international law is applicable in cyberspace, they are far from affirming that JIB has to be transposed *en bloc*. States are actually highly selective has to what is applicable, and know what is needed: ROE. Thus, there is a patchwork of unilateral acknowledgement to respect this or that aspect of IHL, without a coherent or binding framework. As to the rules involving a neutral state, they have only been apprehended by neutral states themselves and the USA. They seem to agree that article 1 prohibits cyber-attacks having an 'effect' on a neutral territory. The Netherlands has a conflicting position, supporting the transposition of both articles 5 and 8; yet, applying these articles to the same activities has contrary effects.

[1412] Brewer (n.1407) 165.

[1413] André Juthe, 'Argument by Analogy' (2005) 19(1) Argumentation 1, 4.

[1414] Ibid 5.

[1415] Ibid.

While doctrinal works usually resort to analogy to reach the conclusion that cyber-espionage is not prohibited, this thesis has a different approach. By applying the VCLT rules of interpretation, it reveals that the relevant provisions in The Hague Conventions and Additional Protocol I only apply to land espionage. This thesis thus deems it necessary–by looking into state practice–to determine whether cyberspace is similar to land. In such a case, JIB would be automatically applicable. However, the contrary happens: states do not consider that cyberspace and land are similar, rendering JIB inapplicable in cyberspace. Wartime cyber-espionage is thus characterized by an absence of law.

SECOND PART – THE RULES DISCONNECTED FROM TERRITORIAL INTEGRITY

I – THE VIENNA CONVENTION ON DIPLOMATIC RELATIONS

Diplomacy and espionage have always been intrinsically correlated. Indeed, '[t]he foreign agents, cloaked with prosecutorial immunities extended to diplomats, may engage in clandestine activities far beyond the scope of their diplomatic duties and yet, remain protected by the defense of diplomatic immunity in the event their espionage activities should be unearthed'.[1416] 'If apprehended, they need not fear prosecution due to the protection accorded them through diplomatic immunity'.[1417] Moreover, '[c]onfidentiality and secrecy are necessary requisites for effective diplomatic relations; hence, the perfect guise for espionage'.[1418] In return, the hosting state used to spy on the communications within the embassy. 'It so happens that I have here today a concrete example of Soviet espionage so that you can see for yourself', said Cabot Lodge before the UNSC.[1419] He then 'reached down and pulled out from under the table a wooden Great Seal of the United States, which had been presented to the U.S. embassy in Moscow by the Soviet-American Friendship Society', and contained a bugging device.[1420] Whether organized by embassies or directed against them, traditional diplomatic espionage relied on the physical presence of a foreign agent on the territory concerned. Yet–and while espionage was a widespread practice at the time of its drafting–the VCDR does not expressly tackle this activity,[1421] and provisions respecting the sending and receiving states have to be interpreted. Status of doctrine (1) and status of law (2) with respect to both of these aspects is thus analysed. A conclusion finally ends this chapter (3).

[1416] Joseph Caccamo, 'A Comparison and Analysis of Immunities Defenses Raised by Soviet Nationals Indicted under United States Espionage Laws' (1980) 6 Brook.J.Int'l.L. 259, 261.

[1417] Karen Jennings, 'Espionage: Anything goes' (1987) 14 Pepp.L.Rev. 647, 651.

[1418] Caccamo (n.1416) 261.

[1419] David Bosco, *Five to Rule Them All: The UN Security Council and the Making of the Modern World* (O.U.P. 2009) 91.

[1420] Ibid.

[1421] See Ashley Deeks, 'An International Legal Framework for Surveillance' (2015) 55(2) Va.J.Int'l.L. 290, 313; Lafouasse, *L'Espionnage* (n.66) 334

1. Status of doctrine

As two sides of the same coin, the arguments surrounding espionage by embassies (1.1) and espionage on embassies (1.2) have to be alternatively tackled.

1.1. Espionage by embassies

Three approaches with respect to the VCDR are identifiable in doctrinal writings. A first approach consists in applying articles 3 and 41(1), usually to demonstrate the illegality of espionage by embassies (A). A second approach relies on the silence of the VCDR on the widespread practice of spying, and affirms that this is actually a legal activity (B). A third type of opinion considers that the VCDR actually lets espionage in a grey zone (C).

A. Arguments based on articles 3 and 41(1) of the VCDR

According to article 3(1) (d), '[t]he functions of a diplomatic mission consist, *inter alia*, in […] Ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State'. Then, article 41(1) mentions that 'it is the duty of all persons enjoying such privileges and immunities to respect the laws and regulations of the receiving State'. These articles are usually harnessed by scholars to demonstrate the illegality of traditional espionage by embassies (a), as well as electronic surveillance and cyber-espionage (b).

a. Traditional espionage

Ward affirms that '[w]hile the diplomat is authorized to collect information by lawful means, espionage clearly is not within this category. We are [...] in the presence of a treaty violation by the diplomatic officer, under the express

direction and approval of the sending State'.[1422] Lafouasse suggests that the terms 'lawful means' include an obligation to comply with the receiving state's legislation, and, 'among other things, this obligation aims spying activities [...]'.[1423]

b. Electronic surveillance and cyber-espionage

According to Duquet and Wouters, '[t]he Convention does not expressly deal with [...] secret intelligence gathering by foreign diplomats in the receiving State'.[1424] However, article 41(1) obliges diplomats 'to respect the laws and regulations of the receiving State'.[1425] 'As a result, acquiring information cannot take place through a violation of the law of the host State and may only be ascertained by "all lawful means" [...] Such means are often defined in local laws, such as espionage legislation, by which diplomats must abide'.[1426] Forcese thinks that '[u]sing a diplomatic mission as an electronic communications listening post might easily be an unlawful activity prohibited by the Convention'.[1427] Talmon affirms that the terms 'lawful means […] does not cover spying on the government of the receiving State'.[1428] Peters also asserts that this provision 'refers to the domestic law of the host state', before adding that '[m]ost states criminalise both the spying out of state secrets [...] and spying on private communication'.[1429] As a consequence, it is a possible breach of the law of diplomacy.[1430] Tallinn Manual 2.0 also considers that 'a sending State may not

[1422] Nathaniel Ward, 'Espionage and the Forfeiture of Diplomatic Immunity' (1977) 11(4) Int.Lawyer 657, 666.

[1423] Lafouasse, *L'Espionnage* (n.66) 321.

[1424] Sanderjin Duquet and Jan Wouters, 'Diplomacy, Secrecy and the Law' (2015) Leuven Centre for Global Governance Studies, Working Paper No.151, 9 <https://ghum.kuleuven.be/ggs/publications/working_papers/2015/151duquetwouters> accessed:15.09.2016.

[1425] Ibid.

[1426] Ibid.

[1427] Forcese (n.66) 200.

[1428] Talmon, 'Tapping' (n.793).

[1429] Peters (n.583).

[1430] Ibid.

use the premises of its diplomatic mission to engage in cyber espionage against the receiving State'.[1431] A 'majority' of the experts also think that it is not permissible, 'for a sending State to use the premises of its diplomatic mission or consular post, without the consent of the receiving State, as a base to engage in cyber espionage directed at a third State, whether that espionage occurs against the third State's organs located in the receiving State or beyond it'.[1432]

However, some scholars combine the treaty's silence on the specific issue of espionage and its widespread practice to affirm that espionage is a lawful activity.

B. Arguments based on widespread practice

The VCDR does not expressly tackle spying. Some scholars thus rely on this gap and the widespread practice of espionage (a), electronic surveillance and cyber-espionage (b), to demonstrate that they are legal.

a. Traditional espionage

As of 1973, McDougal, Lasswell and Reisman already thought that, '[a]lthough they are not mentioned in the Vienna Convention or in the major texts, these intelligence activities are accepted as a correlative purpose of diplomatic activity and are tolerated with a high degree of latitude'.[1433] They then added that '[e]xpulsions of diplomats for intelligence activities have usually been motivated by clear breaches of domestic espionage laws […] The normative frame provided by such laws are the outer limits of diplomatic intelligence gathering'.[1434] According to Grzybowski, '[t]he first conclusion which comes to mind in the light of such confrontation of the Convention with the practice of

---

[1431] Schmitt, *Tallinn Manual 2.0* (n.53) 229.

[1432] Ibid.

[1433] McDougal, Lasswell, Reisman (n.581) 380-1.

[1434] Ibid.

States is that reciprocity in the regime of diplomacy plays a much larger role than is accorded to it in formal law'.[1435] He adds that '[i]t is also clear that the Convention is not a complete code of law, in the sense that it contains no answer to situations in which the interests of international relations come into conflict with vital national interests of a great power'.[1436] Murty evokes 'the departure of the person associated with the diplomatic mission who is caught while engaged in espionage activity', saying 'it is preferable to secure' it 'without much publicity, or to trade him off against one's own national caught in the other state in a similar fashion'.[1437]

b. Electronic surveillance and cyber-espionage

According to Deeks, spying 'is so widespread that it is inappropriate to interpret VCDR Article 41 as prohibiting such activity. States manifestly have not interpreted the VCDR that way. Further, even though spying was widespread at the time states negotiated the VCDR, states did not explicitly address spying in the treaty'.[1438] Sharp notes that the VCDR 'explicitly recognizes the well-established right of nations to engage in espionage during peacetime, and the practice of states has specifically recognized a right to engage in such clandestine intelligence collection activities as an inherent part of foreign relations and policy'.[1439]

In contrast, some authors think that diplomatic espionage lies in a grey zone, as it is neither expressly authorized nor forbidden by the VCDR.

[1435] Kazimierz Grzybowski, 'The Regime of Diplomacy and the Tehran Hostages' (1981) 30 I.C.L.Q. 42, 57.

[1436] Ibid.

[1437] Bhagevatula Satyanarayana Murty, *The International Law of Diplomacy: The Diplomatic Instrument and World Public Order* (New Haven Press 1989) 505.

[1438] Deeks (n.1421) 313.

[1439] Sharp (n.598) 123.

C. Arguments based on the existence of a grey zone

Chesterman lengthily studies the VCDR in his works, and quotes articles 3(1)(d), 7, 11, 27 and 41(1) as relevant regarding espionage. He affirms that '[t]he norms in place [...] both implicitly accept limited intelligence gathering as an inevitable element of diplomacy and explicitly grant an absolute discretion to terminate that relationship at will'.[1440] According to Murty, it is only '[i]f electronic surveillance seriously threatens the security of the receiving state' that 'it is likely to demand the closure of the mission'.[1441] He notes that '[a] high degree of tolerance is necessary to preserve the institution of the diplomatic mission itself'.[1442] Delahunty suggests that diplomacy 'resembles, and occasionally overlaps with, espionage'.[1443] He concludes that 'intelligence-gathering […] tends to conduct to peace', as it seeks reducing and eliminating 'the uncertainty on the part of two States about each other's intentions (or capabilities for harm) that gives rise to the spiral of fear, mistrust and armament'.[1444]

Nahlik thinks that 'this is a highly "dialectical", often controversial, subject'. As 'collecting information for one's government' is 'one of the main functions of any diplomatic agent', '[t]he frontier between [...] "legal" and "illegal" means, is in many cases very difficult to draw'.[1445] As 'whenever a country expels a couple of diplomats for spying, the other country would reply by an analogous measure', there is 'a whole chain of measures and counter-measures, sometimes not easy to disentangle'.[1446] As this problem had not been tackled during the drafting of Vienna Convention–in spite of a well-known practice–Lafouasse also suggests

---

[1440] Chesterman (n.566) 1089.

[1441] Murty (n.1437) 506.

[1442] Ibid.

[1443] Robert Delahunty, 'Herbert Butterfield, Christianity, and International Law' (2009) 86 U.Det. Mercy L.Rev. 615, 642-3.

[1444] Ibid.

[1445] Stanislaw Nahlik, 'Developments of Diplomatic Law–Selected Problems' (1990) 222 Recueil des Cours 187, 340.

[1446] Ibid.

that participating states deliberately avoided creating any binding norm in this field'.[1447]

Kish, Turns and Witiw both refer to the *Hostages* case. According to Kish, 'the Court acknowledges the complexity of the regulation of diplomatic observation in article 3(1) (d) of the Convention, and consequently the marginal overlap of diplomacy and espionage'.[1448] Witiw adds that 'even if the alleged criminal activity of the United States in Iran were established', the ICJ 'was unable to accept that the activities constituted a justification for Iran's conduct'.[1449]

While espionage by embassies is a serious concern for the hosting state, embassies themselves may be spied on. The doctrinal arguments on this aspect should thus be displayed.

1.2. Espionage on embassies

Scholars draw various conclusions regarding espionage on embassies. Those affirming that it is illegal usually rely on the inviolabilities of the mission (article 22), archives and documents (article 24) and official correspondence (article 27(2)) (A). Others, thinking it is legal, invoke states' widespread practice of espionage (B). Finally, some of them demonstrate the existence of a grey zone (C).

A. Arguments based on articles 22, 24, 27(2) of the VCDR

Forcese refers to the inviolability of diplomatic premises (article 22), archives, documents and official correspondence (articles 24 and 27(2)). '[W]hile spying on diplomats may be commonplace, it is no less a violation of the Convention', and 'states that intercept communications occurring in diplomatic missions or

[1447] Lafouasse, *L'Espionnage* (n.66) 334

[1448] Kish and Turns (n.66) 57.

[1449] Eric-Paul Witiw, 'Persona Non Grata: Expelling Diplomats who abuse their Privileges' (1988) 9 N.Y.L.Sch.J.Int'l.&Comp. 345, 354.

the personal premises of diplomats violate international law'.[1450] Indeed, 'it is [...] difficult to see how spying on diplomats [...] can be squared with the actual rules found in the Convention, unless one accepts the doubtful proposition that interception of communications is permitted in an effort to separate official correspondence from correspondence not properly related to the mission's functions'.[1451] Quigley is of the same opinion.[1452] Tallinn Manual 2.0 mentions that the 'International Group of Experts agreed that "inviolability" means that these materials are free from […] cyber espionage […]'.[1453]

As in the debate surrounding the legality of espionage by embassies, arguments based on widespread practice may be found.

B. Arguments based on widespread practice

According to Smith, the Congress was once satisfied that electronic espionage 'was such a widely accepted practice of states that, although not specifically authorized by the Vienna Convention, one could hardly argue [it] violated the Convention, since everybody was doing it'.[1454] He then supports the idea that '[...] espionage activities are consistent with, or at least tolerated by, international law [...]'.[1455]

In addition, some arguments remain based on the existence of a grey zone.

[1450] Forcese (n.66) 196-7

[1451] Ibid.

[1452] Peter Beaumont, Martin Bright and Ed Vulliamy, 'UN launches inquiry into American spying', *Guardian* (09.03.2003) <www.theguardian.com/world/2003/mar/09/iraq.unitednations1> accessed:19.04.2017.

[1453] Schmitt, *Tallinn Manual 2.0* (n.53) 219.

[1454] Jeffrey Smith, 'State Intelligence Gathering and International Law–Keynote addres' (2007) 28 Mich.J.Int'l.L. 543, 545.

[1455] Ibid.

C. Arguments based on the existence of a grey zone

Murty affirms that 'the sending state will decide to close the mission if the electronic surveillance of the receiving government seriously undermines the utility of the mission'.[1456]

In sum, authors reach different conclusions regarding the legality of spying by and on embassies. Establishing the status of law thanks to the VCLT rules will help determining who has the most convincing arguments.

2. Status of law

Espionage by embassies (2.1) and on embassies (2.2) has to be alternatively tackled.

2.1. Espionage by embassies

The VCDR does not expressly tackle espionage by embassies. However, some articles allow a protection of the receiving state, on different stages of the mission's life. Articles 7 and 11 display the modalities of members' appointment, and regulate the mission's size. They deal with accreditations, and thus, the beginning of the mission (A). Articles 3 and 41 lay out the mission's functions, and the diplomats' duties. They correspond to the mission's performing and thus, embassy's daily life (B).

A. The accreditation of the mission

'[T]he sending State may freely appoint the members of the staff of the mission', except for 'military, naval or air attachés'.[1457] This exception actually allows the

[1456] Murty (n.1437) 506.

[1457] VCDR, art.7.

receiving State to indirectly limit espionage. As a CIA's document mentions, '[t]he attaché system is recognized [...] as an effective collection arm'.[1458]

Article 11 has a similar goal, and entitles the receiving state to limit the size of the mission and to 'refuse to accept officials of a particular category'.
Some events illustrate the link between a high number of diplomats and the risks of espionage. In 1971, Foreign Secretary Douglas-Home wrote to his Soviet counterpart, Gromyko: '[y]ou are no doubt aware that the total number of Soviet officials on the staff of Soviet diplomatic, commercial and other organizations has now risen to more than 500 and you are presumably able to ascertain what proportion of these are intelligence officers'.[1459] In the absence of a reply, his Under-Secretary Greenhill wrote to Soviet Chargé d'Affaires Ippolitov. 'The staffs of the Soviet Embassy and the Soviet trade delegation [...] far outnumber the British officials working in the Soviet Union [...] H.M. Government have tolerated the growth of these establishments. They have not sought to bargain increases in the Soviet establishment in this country against increases in the British establishment in the U.S.S.R. [...] Evidence has, however, been accumulating that this tolerance has been systematically abused'.[1460]

Some safeguards also exist after the accreditation of the mission, i.e. when the mission is performed.

B. The performing of the mission

The VCDR proposes a balanced solution by acknowledging that intelligence-gathering is a function of the diplomatic mission (a), and by setting up safeguards to prevent abuse of such function (b).

[1458] Peter Dorondo, 'The Military Attachés' (2008) 4(3) Studies Archive Indexes.

[1459] Ivor Roberts, *Satow's Diplomatic Practice* (O.U.P. 2009) 212.

[1460] Ibid.

a. Intelligence-gathering is a function of the diplomatic mission

Intelligence-gathering is inherently linked to diplomatic missions, as revealed by VCDR articles 3(1) (b) and 3(1) (d). The mission must indeed protect, 'in the receiving State the interests of the sending State and of its nationals, within the limits permitted by international law', while '[a]scertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the Sending State'. A recent statement of the Irish Department of Foreign Affairs confirms this: 'Ireland's network of Embassies and Consulates is uniquely placed to advance our political and economic interests in developed and emerging markets and to raise our cultural profile overseas. Our diplomatic network is well-positioned to provide advance warning of regulatory trends in our major markets, and is a valuable source of contacts and market intelligence for Irish business entering the global marketplace'.[1461] States are aware that foreign intelligence officers are based in embassies, and examples are given by Finland and Lithuania. 'Intelligence operations in Finland are primarily managed from embassies, consulates and commercial missions […] A diplomatic position is a typical "cover" for an intelligence officer'.[1462] Moreover, '[o]ne third of Russian diplomats accredited in Lithuania are intelligence officers or are related to intelligence services'.[1463] Yet, safeguards exist to prevent this kind of misuse.

b. Safeguards are set up by the VCDR to prevent abuses

These safeguards are of three types, and call on domestic law (i), or international law (ii). A political solution is the third one: the declaration *persona non grata* (iii).

[1461] 'Department of Foreign Affairs Statement of Strategy 2008-10' (2008) 3 Irish Y.B.I.L., 280.

[1462] SUPO (n.739) 13.

[1463] State Security Department, 'Lithuanian Threat Assessment 2014' (2015) 4 <www.vsd.lt/senoji/Files/Documents/635664369272603750.pdf> accessed:15.05.2017.

i. Legal safeguards relying on domestic law

Article 41(1) clearly refers to the domestic law of the receiving state. Indeed, 'it is the duty of all persons enjoying such privileges and immunities to respect the laws and regulations of the receiving State'.

The case of article 3(1) (d) is more obscure. 'Ascertaining [...] conditions and developments in the receiving State' and their 'reporting' must be done 'by all lawful means'. It is not expressly defined whether such 'lawful means' refer to international or domestic law. The issue is of importance: as spying is prohibited by the domestic law of a majority of states, a reference to national law would render diplomatic espionage quasi-systematically unlawful at the national stage.
Subsequent state practice answers the question. Diplomats are actually expected to comply with the receiving state's domestic law, while 'lawful means' is not invoked in the light of international law.
Swiss position is clear: '"[l]awful means" should not be only examined in the light of the legislation of the sending state', but '[i]t has to be essentially interpreted in the light of the receiving state's legislation'.[1464]
Japan and the Netherlands also head the same way, but in a subtler fashion. It is indeed by reference to their domestic law that they used to denounce instances of diplomatic spying.
In 1973, at the Japanese MFA, the Deputy Director-General of the Treaties Bureau had to determine whether installing a wire-tapping device was equivalent to police activities within the jurisdiction of Japan. He expressed doubts about it, and affirmed that '[t]here is no general prohibition for members of a foreign embassy in Japan to engage in the collection of information of a general character of research activities'.[1465] Then, '[t]he problem is whether such use of a tapping device is illegal under the Japanese laws'.[1466] He thus determined that

[1464] Lucius Caflisch, 'La Pratique Suisse en Matière de Droit International Public 2004' (2005) 15 R.S.D.I.E. 713, 754; see also Lucius Caflisch, 'La Pratique Suisse en Matière de Droit International Public 1992' (1993) 3 R.S.D.I.E. 669, 723-25.

[1465] Shigeru Oda and Hisashi Owada, 'Annual Review of Japanese Practice in International Law XII (1973)' (1982) 25 J.A.I.L. 73, 137.

[1466] Ibid.

it was probably not 'a criminal act under the Japanese laws', 'rather [...] a tort in civil law for which a legal remedy could be sought'.[1467] He concluded: '[i]n international law, diplomats are naturally under the obligation to observe the laws and regulations of the receiving state. If, therefore, a member of an embassy in Japan were to engage in some activity of information collection or inquiry through the use of the tapping device, it would probably be an improper activity'.[1468] In 2008, the Tokyo Police suspected Russian agents of violating the National Public Security Service Law, and the Japanese Government subsequently protested.[1469]

According to the Netherlands, 'it is a principle of public international law that the host country should put nothing in the way of a diplomat which would hinder him from complete freedom to exercise his functions and should remove any existing hindrances. There are of course limits; for instance, when a diplomat obviously abuses his position'.[1470] This includes 'cases in which espionage activities lead to expulsion'.[1471] Thus, 'it goes without saying that foreign diplomats should conform entirely to the rules of Dutch law and public policy and not to what is permissible in their own countries'.[1472]

Some references to international law are made in the VCDR. However, they fail to confront cyber-espionage.

[1467] Ibid.

[1468] Ibid.

[1469] Shuichi Furuya and Satsuki Konaka, 'Chronology of Japanese Foreign Affairs in 2008' (2009) 52 Japanese Y.B.I.L. 704, 704.

[1470] Ko Swan Sik, 'Netherlands State Practice for the Parliamentary Year 1969–1970' (1971) Netherlands Y.B.I.L. 136, 170.

[1471] Ibid.

[1472] Ibid 171.

ii. Legal safeguards relying on international law

Diplomats 'have a duty not to interfere in the internal affairs of that State'.[1473] Then, it is 'within the limits permitted by international law' that sending state's interests must be protected.[1474] However, as espionage is not generally prohibited in international law, the latter provision seems of little help to combat spying.

Only Brazil and Germany think that the use of diplomatic premises for purposes of electronic and cyber-espionage breaches the VCDR. Brazil affirms that '[t]his situation would clearly represent an abuse of the protection granted to such premises since the Vienna Convention determined that they cannot be used for purposes other than those of diplomatic and consular activities'.[1475] Following revelations of eavesdropping from the British embassy in Berlin, the German MFA said that the 'interception of communications from the premises of a diplomatic mission would be behaviour contrary to international law'.[1476]

Actually, the solution to intelligence activities carried out by diplomats does not necessarily appeals to law, but lies in the political realm of declarations *persona non grata* (PNG).

iii. Declarations *persona non grata*

Diplomats cannot be put on trial due to their immunities. Besides, Canada expressly mentions that the 'intent to put the embassy personnel on trial for espionage is an obvious breach of international law, as they benefit from

[1473] VCDR, art.41(1).

[1474] VCDR, art.3(1)(b).

[1475] 'Sixth Committee 15th meeting, 69th General Assembly' (*UN Web TV,* 14.10.2014) <http://webtv.un.org/watch/sixth-committee-14th-meeting-69th-general-assembly/3849676513001> accessed:13.09.2016.

[1476]Julian Borger, Philip Oltermann and Nicholas Watt, 'Germany calls in British ambassador over spy claims', *BBC* (05.11.2013) <www.bbc.com/news/world-europe-24824633> accessed:19.09.2017.

jurisdictional immunity on behalf of the Convention'.[1477] However, article 9 allows the receiving state to declare a diplomat PNG 'at any time and without having to explain its decision'.[1478]

States regularly declare diplomats PNG in espionage-related cases,[1479] and refer to various behaviours:[1480] 'activities incompatible with the status',[1481] 'illegal activity',[1482] 'espionage',[1483] 'violation of embassy security'.[1484] Following the migration of espionage on the Internet, PNG declarations are still valid. After the allegations of Russian hacking during the American elections, '[t]he State Department' declared '35 Russian intelligence operatives' PNG.[1485]

The decision to declare diplomats PNG and its modalities are deeply political and is a case-by-case assessment. For instance, France expelled 47 Soviet diplomats in the wake of Vetrov's revelations about Soviet spying activities, but refused to make a nominal list public, considering their expulsion as sufficiently satisfactory.[1486] A secret etiquette could even have emerged. Guisnel affirms that 'according to the applicable regulations between friendly states' services, such espionage cases are not to be solved publicly, especially among allies'.[1487]

[1477] L Legault, 'Canadian Practice in International Law during 1979 as Reflected Mainly in Public Correspondence and Statements of the Department of External Affairs' (1980) 18 Canadian Y.B.I.L. 301, 307.

[1478] VCDR, art.9(1).

[1479] (2014) 60(4) Keesings, 53287. See also: (1954) IX(12) Keesings, 13772; (1986) 32(7) Keesings, 34505; (2002) 48(11) Keesings, 45086.

[1480] According to Navarette, States resort to 'euphemisms' to qualify espionage, 'in order to prevent the formation *opinio juris*'. See Navarette (n.708) 7.

[1481] 1982) 28(10 Keesings, 31784; (2001) 47(3) Keesings, 44072; (2013) 59(5) Keesings, 52686.

[1482] (2010) 56(12) Keesings, 49994.

[1483] (1974) 20(3) Keesings, 26389.

[1484] (1988) 34(6) Keesings, 35991.

[1485] The White House, 'Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment' (29.12.2016) <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity> accessed:9.05.2017.

[1486] Jean Charpentier, 'Pratique Française du Droit International–1983' (1983) 29 A.F.D.I. 850, 919.

[1487] Jean Guisnel, *Guerres dans le Cyberespace–Services Secrets et Internet* (La Découverte 2013) 274.

The ICJ had the opportunity to study the VCDR and the Vienna Convention on Consular Relations (VCCR)[1488] in the *Hostages* Case. First, the ICJ referred to the diplomatic and consular personnel's duties to respect the receiving state's legislation and non-interference,[1489] as well as the impossibility for the diplomatic and consular premises to be used in a manner incompatible with their mission.[1490] According to the Court, '[t]he Vienna Conventions of 1961 and 1963 contain express provisions to meet the case when members of an embassy staff, under the cover of diplomatic privileges and immunities, engage in such abuses of their functions as espionage or interference in the internal affairs of the receiving State'.[1491] The ICJ then turned to articles 9(1) VCDR and 23(4) VCCR, which both allow declarations PNG. According to the Court, they 'take account of the difficulty that may be experienced in practice of proving such abuses in every case or, indeed, of determining exactly when exercise of the diplomatic function [...] of "ascertaining by all lawful means conditions and developments in the receiving State" may be considered as involving such acts as "espionage" or "interference in internal affairs"'.[1492] The Court further noted that states could even choose to break off diplomatic relations.[1493] The ICJ concluded that '[t]he rules of diplomatic law, in short, constitute a self-contained *régime* which, on the one hand, lays down the receiving State's obligations regarding the facilities, privileges and immunities to be accorded to diplomatic missions and, on the other, foresees their possible abuse by members of the mission and specifies the

---

[1488] Vienna Convention on Consular Relations ('VCCR') (adopted:24.04.1963–EIF:19.03.1967) 596 UNTS 261

[1489] As mentioned in articles 41(1) VCDR and 55(1) VCCR.

[1490] As mentioned in articled 41(3) VCDR and 55(2) VCCR. *United States Diplomatic and Consular Staff in Tehran* (*USA v Iran*) (Judgment) [1980] ICJ Rep 3, [84].

[1491] Ibid.

[1492] Ibid [85].

[1493] Ibid.

means at the disposal of the receiving State to counter any such abuse. These means are, by their nature, entirely efficacious […]'.[1494]

The case of IOs' members is darker, and state practice is not homogeneous. For instance, an American court affirmed 'that unlawful espionage is not a function of the defendant as an employee of the United Nations'.[1495] As a consequence, 'defendant's status as an employee of the United Nations conferred upon him no privilege or immunity which should constitute an obstacle to his apprehension, trial or conviction'.[1496] 'By analogy', 'the VCDR is to be applied to permanent missions of IOs in Geneva and to their members [...] If the security of Switzerland is in danger, the domestic or external security clause contained in host agreements […] can be applied by analogy to deport a member of a permanent mission […] This clause will essentially apply to instances of espionage and terrorism'.[1497]

In sum, international law does not prohibit espionage by embassies, but provides means to combat him, including resort to domestic law and political measures. Fortunately, it has a better fate when it comes to espionage on embassies.

2.2. Espionage on embassies

Two types of inviolability have to be analysed: the inviolability of the mission premises (A) and of the official correspondence, documents and archives (B).

[1494] Ibid [86].

[1495] SDNY District Court, *United States v Coplon* (1949) 84 FSupp 472, 474.

[1496] Ibid 474-5.

[1497] Lucius Caflisch, 'La Pratique Suisse en Matière de Droit International Public 1993' (1994) 4 R.S.D.I.E. 597, 616.

A. The inviolability of the mission premises

According to article 22(1), '[t]he premises of the mission shall be inviolable. The agents of the receiving State may not enter them, except with the consent of the head of the mission'. It then obliges the receiving states 'to take all appropriate steps to protect the premises of the mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity'.

It seems obvious that breaking into an embassy to install listening device goes against the inviolability of the mission's premises. However, article 22(1) is insufficient to prevent eavesdropping or cyber-espionage. Premises may indeed be defined as '[a] house or building together with its grounds, outhouses, etc., *esp.* a building or part of a building that houses a business'.[1498] They thus name an area that is part of a property, and physical in essence. The French text helps confirming such interpretation. 'Premises' translates into 'locaux', which is systematically linked to a building: '[p]ièces, partie de bâtiment servant de siège aux activités d'une profession'.[1499] The whole paragraph then moves in this direction. 'The agents of the receiving State' are prevented from 'entering' them. 'To enter' is similarly linked to a physical space, meaning to '[t]o come or go into; esp., to go onto (real property) by right of entry so as to take possession'.[1500] 'These premises should thus be protected 'against any intrusion or damage'. 'Intrusion' means '[a] person's entering without permission', but also '[i]n an action for invasion of privacy, a highly offensive invasion of another person's seclusion or private life'.[1501] But again, the French text confirms that the sole physical trespass is to be tackled by the article, preventing these premises from being 'envahis' ('invaded'). 'Damage' is originally physical, referring to the '[l]oss

[1498] 'premises' (O.E.D-Online, O.U.P. 2018)

[1499] 'locaux' (Larousse) <www.larousse.fr/dictionnaires/francais/locaux/47585?q=locaux#47510> accessed:16.09.2017. '

[1500] Black's (n.863) 'enter'.

[1501] Black's (n.863) 'intrusion'.

or injury to person or property; esp., physical harm that is done to something or to part of someone's body', even if it may mean '[b]y extension, any bad effect on something'.[1502]

Switzerland confirms this interpretation, as 'the goal' of this provision is 'to prevent the hosting State from penetrating these premises without an express authorization, in order to prevent any attempt of interference in the domestic affairs of the beneficiary'.[1503] Yet, an interesting and contradictory precedent exists regarding an equivalent article in the VCCR.[1504] In 1990, the German Supreme Court ruled that surveillance of phone connections emanating from consular premises infringed article 31 VCCR and was thus generally deemed illegal.[1505] This decision was criticized by some authors,[1506] and remains isolated.

It is then difficult to qualify the mere collection of information as 'disturbance of the peace of the mission or impairment of its dignity'. Subsequent practice indeed confirms that preventing the excesses of protest movements is the provision's main goal. For instance, the Australian MFA invoked these grounds to order the removal of white crosses raised by Timorese outside the Indonesian Embassy in Canberra. The latter went to the Court. According to Judge French, '[n]either State practice nor the writings of jurists or judicial decisions have exposed an exhaustive definition of the peace and dignity in respect of which a diplomatic mission is entitled to the protection of the receiving State'.[1507] However, he listed some examples of breaches: 'the prolonged broadcast [...] of loud speeches or music', '[s]ustaining chanting of slogans or the organised passing and repassing of people outside the premises in such a way as to

---

[1502] Black's (n.863) 'damage'.

[1503] Lucius Caflisch, 'La Pratique Suisse en Matière de Droit International Public 2006' (2007) 17 R.S.D.I.E. 743, 781.

[1504] VCCR, art.31(3).

[1505] Bundesgerichtshof (04.04.1990) 3 StB 5/90.

[1506] Jörg Polakiewicz, 'Die völkerrechtliche Zulässigkeit der Überwachung des Telefonverkehrs von Konsulaten ausländischer Staaten' (1990) 50 Z.a.ö.R.V. 761, 770.

[1507] Federal Court of Australia (FCA), *Minister of Foreign Affairs and Trade; the Commissioner of the Australian Federal Police and the Commonwealth of Australia v Geraldo Magno and Ines Almeida, Re* (1992) FCA 566.

compromise or deter access to them', '[o]ffensive or insulting behaviours', '[t]he burning of flag', 'the mock execution of its leader in effigy', 'the depositing of some offensive substance and perhaps also the dumping of farm commodities' in the vicinity of the diplomatic premises.[1508] The British Foreign Affairs Committee confirms this, as 'the UK's duty to protect the peace of diplomatic missions cannot be interpreted so widely that no demonstration are allowed outside them [...] the essential requirements are that the work of the mission should not be disrupted, that mission staff are not put in fear, and that there is free access for both staff and visitors'.[1509]

Article 22(3) then affirms that '[t]he premises of the mission, their furnishings and other property thereon and the means of transport of the mission shall be immune from search, requisition, attachment or execution'.
'Premises' have previously been defined,[1510] while 'furnishing' means '[f]urniture, fittings, and other decorative accessories such as curtains and carpets, for a house or room'.[1511] As to 'other property'–'[a] (usually material) thing belonging to a person, group of persons, etc.; a possession; (as a mass noun) that which one owns; possessions collectively; a person's goods, wealth, etc'[1512]–there could be more room for interpretation. However, the French text translates 'property' into 'objets'. The term 'objets' means '[c]hose solide considérée comme un tout, fabriquée par l'homme et destinée à un certain usage'.[1513] They are thus intrinsically physical and exclude virtual data and communications.

[1508] Ibid.

[1509] Jason Reed and Ethan Jee-Sheok Shin, 'Statue wars reveal contested history of Japan's "comfort women"', *The Huffington Post* (02.07.2017) <www.huffingtonpost.com/the-conversation-global/statue-wars-reveal-contes_b_14635786.html?guccounter=1> accessed:18.09.2017.

[1510] 'premises' (n.1498).

[1511] 'furnishing' (English Oxford Dictionaries) <https://en.oxforddictionaries.com/definition/furnishing> accessed:16.09.2017.

[1512] 'property' (O.E.D-Online, O.U.P. 2017).

[1513] 'objet' (Larousse) <www.larousse.fr/dictionnaires/francais/objet/55366?q=objet#54989> accessed:16.09.2017.

The inviolability of the mission premises is thus irrelevant to cyber-espionage, contrary to the inviolability of official correspondence.

B. The inviolability of the official correspondence, documents and archives

According to article 27(1), '[t]he receiving State shall permit and protect free communication on the part of the mission for all official purposes. In communicating with the Government and the other missions and consulates of the sending State, wherever situated, the mission may employ all appropriate means, including diplomatic couriers and messages in code or cipher. However, the mission may install and use a wireless transmitter only with the consent of the receiving State'.

Such provision is of little help against espionage. 'Free' indeed means '[n]ot impeded, restrained, or restricted in actions, activity, or movement'.[1514] Espionage does not go against this principle. Should there be an end to such freedom, spying would in fact be hindered. As to the restriction on wireless transmitter, it was actually conceived as a restriction to the diplomats' action, not as a burden to the receiving state. As a matter of fact, 'the fear remained that transmitters might be used for propaganda or for intervention in that State's internal affairs'.[1515]

Article 24 mentions that 'the archives and documents of the mission shall be inviolable at any time and wherever they may be'. While the VCDR was made for a continuing period, it turns out that its terms are generic, thus allowing an evolutionary interpretation. Archives may indeed be defined as '[a] historical record or document so preserved',[1516] '[c]ollected and preserved public, historical, or institutional papers and records',[1517] or '[a]ny systematic

---

[1514] 'free' (O.E.D-Online, O.U.P. 2017).

[1515] Eileen Denza (ed), *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations* (4th edn, O.U.P. 2016) 180.

[1516] 'archives' (O.E.D-Online, O.U.P. 2017).

[1517] Black's (n.863) 'archive'.

compilation of materials, esp. writings, in physical or electronic form'.[1518] 'Documents' may refer to '[s]omething written, inscribed, etc., which furnishes evidence or information upon any subject, as a manuscript, title-deed, tomb-stone, coin, picture, etc' or '[a] collection of data in digital form that is considered a single item and typically has a unique filename by which it can be stored, retrieved, or transmitted (as a file, a spreadsheet, or a graphic)'.[1519] Moreover– and as explained below–this interpretation is supported by subsequent practice. In compliance with article 24, spying on archives and documents of the mission is thus prohibited.

According to article 27(2), '[t]he official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the missions and its functions'. However, 'correspondence' is an ambiguous term. In French, 'correspondance' means 'communication par échange de lettres, de messages'.[1520] 'Message' is a broad term, and may describe any information transmitted to someone.[1521] In English, however, many definitions focus on the notion of 'letter'. 'Correspondence' is thus defined as '[i]ntercourse or communication by letters',[1522] while 'correspondent' means '[t]he writer of a letter or letters'.[1523] A problem with the term 'letter' is that definitions usually exclude electronic and vocal communications: '[a] written communication that is usu. enclosed in an envelope, sealed, stamped, and delivered (esp., an official

[1518] Ibid.

[1519] 'document' (Oxford English Dictionary) <en.oxforddictionaries.com/definition/document> accessed:23.05.2017.

[1520] 'correspondance' (Larousse) <www.larousse.fr/dictionnaires/francais/correspondance/19439?q=correspondance#19326> accessed:10.09.2016.

[1521] 'message' (Larousse) <www.larousse.fr/dictionnaires/francais/message/50766?q=message#50659> accessed:27.02.2017.

[1522] 'letter' (O.E.D-Online, O.U.P. 2018).

[1523] Black's (n.863) 'correspondent'.

written communication)',[1524] '[a] written text on paper, parchment, etc., and related senses'.[1525]

Subsequent practice is thus decisive here.

On the one hand, the American Foreign Intelligence Surveillance Act (FISA) gives the modalities to 'authorize electronic surveillance', in order 'to acquire foreign intelligence information'.[1526] It must be directed at 'the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers',[1527] or 'the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power'.[1528] It is also possible to direct electronic surveillance at 'facilities or places' that are 'used' or 'about to be used' by 'a foreign power or an agent of a foreign power'.[1529] It seems that the adoption of this instrument was prompted by classified sources, including a memorandum written by Antonin Scalia at the Office of Legal Counsel (OLC), and dated 24 December 1975. These classified sources would deem the wiretapping and eavesdropping of embassies permissible,[1530] and list acts of spying directed towards the U.S. embassies, suggesting it is common practice and does not violate the VCDR.[1531]

On the other hand, a majority of states consider that cyber-espionage is a violation of the VCDR. First, the FISA itself was hotly debated at the US Congress, and many people considered that surveillance of embassies was at

[1524] Black's (n.863) 'letter'.

[1525] 'letter' (O.E.D-Online, O.U.P. 2018).

[1526] 50 USC §1802(a)(1).

[1527] 50 USC §1802(a)(1)(A)(i).

[1528] 50 USC §1802(a)(1)(A)(ii).

[1529] 50 USC §1804(a)(3)(A)-(B).

[1530] Scott (n.787) fn 15.

[1531] Deeks (n.1421) 313; Forcese (n.66) 197; Smith (n.1454) 545.

odds with the VCDR, such as Representative Drinan,[1532] Senator Tunney,[1533] Jerry Berman (Legislative Counsel) and John Shattuck (American Civil Liberties Union).[1534] Second, Switzerland thinks that the goal of the 'inviolability of agents, goods, archives, documents, correspondence or diplomatic bag' is to prevent the hosting State from 'claiming the right to monitor the information available' to the personnel.[1535] Third, the activities of the NSA shed light on the problem's extent, and raised unanimous reactions. The European Parliament condemned spying on EU representations as it 'would imply a serious violation of the Vienna Convention on Diplomatic Relations'.[1536] At the UNGA in 2014, Costa Rica affirmed that 'CELAC wish to express its concern over surveillance and interception of communication (including extraterritorially) may have on diplomatic and consular archives, documents and communication'.[1537] Brazil similarly thinks that 'although communication methods' are 'no longer dependent on physical support and could circulate through technologically sophisticated channels', it remains 'beyond doubt that diplomatic and consular communications, archives and documents should be protected both online and offline'.[1538] UNGA Resolution 69/121 notes that 'diplomatic and consular

---

[1532] United States, *Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary House of Representatives, Ninety-Fourth Congress, Second Session 94 Congress on Foreign Intelligence Surveillance Act, April 12, May 5 and June 2, 1976, Serial No.65* (GPO 1977) 100-01. <https://babel.hathitrust.org/cgi/pt?id=mdp.39015005012367;view=1up;seq=3> accessed:10.09.2016.

[1533] Ibid 112.

[1534] USA, *Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary House of Representatives, Ninety-Fourth Congress, Second session on H.R. 7308 Foreign Intelligence Surveillance Act, June 22, 28 and 29, 1978, Serial No.48* (GPO 1978) 153 <https://babel.hathitrust.org/cgi/pt?id=mdp.39015005012292;view=1up;seq=3> accessed:10.09.2016..

[1535] Lucius Caflisch, 'La Pratique Suisse en Matière de Droit International Public 2006' (2007) 17 R.S.D.I.E. 743, 781.

[1536] European Parliament (n.669) [2].

[1537] PMUN Costa Rica, 'Consideration of effective measures to enhance the protection, security and safety of diplomatic and consular missions and representatives' (2014) <www.un.int/costarica/statements_speeches/consideration-effective-measures-enhance-protection-security-and-safety> accessed:13.09.2016.

[1538] 'International Trade Law Body Highlights Finalized Texts on Secured Transactions, Arbitration, Online Dispute Resolution, as Sixth Committee Takes Up Report', UN meeting coverage GA/L/3523 (10.10.2016)

missions may maintain archives and documents in various forms, that official correspondence may take a variety of forms and that diplomatic and consular missions may use a variety of means of communication'.[1539] Then, the resolution recalls 'that the archives and documents of diplomatic and consular missions shall be inviolable at any time and wherever they may be and that the official correspondence of diplomatic and consular missions shall be inviolable'.[1540]
In compliance with article 31(3) (b), the 'subsequent practice in the application of the treaty' establishes 'the agreement of the parties regarding its interpretation': article 27(2) prohibits spying on vocal and electronic communications 'relating to the missions and its functions', while the embassy's digital documents and archives remain inviolable under article 24.

3. Conclusion

The dematerialization of espionage has had two consequences: it has increased the flow of contestations based on the VCDR–states used to rarely refer to international law when protesting against spying activities and expelling diplomats–and article 22 is now deprived of its relevance. Yet, cyber-espionage on embassies remains prohibited by the VCDR, as it constitutes a breach of the inviolability of archives, documents and official correspondence. Articles 24 and 27(2) of the Convention protect digital and vocal forms of official correspondence, as well as electronic archives and documents of the diplomatic mission. This interpretation is confirmed by subsequent practice. International law is however silent when it comes to cyber-espionage by embassies, as the VCDR delegates to Parties the power to take measures against spies, without prohibiting espionage by itself.

<www.un.org/press/en/2016/gal3523.doc.htm> accessed:19.09.2017.

[1539] UNGA Res 69/121 (18.12.2014) [Consideration of effective measures to enhance the protection, security and safety of diplomatic and consular missions and representatives]

[1540] Ibid.

II – THE AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS

According to French Rear-Admiral Coustillière, 'industrial spying has always existed'.[1541] Many examples may indeed be found in history: China lost the secret of silk-making when a princess hid silkworms in her hat and brought them abroad, and of porcelain, when 'a visiting French Jesuit memorized the process' and described it in letters.[1542] In 1813, Lowell–'who is credited […] with having a photographic memory–similarly memorized the secret of British looms, and brought it to the USA.[1543] At the time, the physical presence of the spy on the design and conception places was thus required, and economic espionage was a risky activity. States have since taken steps to protect intellectual property, and TRIPS is an example. Yet, the prohibition of economic cyber-espionage is not expressly mentioned in this instrument, and competitive intelligence is a common practice in the business sphere. Today, '[a]ll organizations collect and make use of some kind of information about their competitors and other organizations, whether through market scanning, industry profiling, or simply debriefing of managers recruited from competitors', and this is 'very much a standard aspect of conventional market research and competitor benchmarking, and make for effective competitive behavior'.[1544] In parallel, the paradoxical behaviour of intelligence agencies has been highlighted by Pierre Marion, the former director of the DGSE: '[w]e are military allies, but economic competitors. Therefore, industrial espionage, even among friends, is a normal action of an intelligence agency'.[1545]

[1541] AN, 'Audition du contre-amiral Arnaud Coustillière' (12.06.2013) CR No.79, 9 <www.assemblee-nationale.fr/14/pdf/cr-cdef/12-13/c1213079.pdf> accessed:02.11.2017.

[1542] Robert Van Arnam, 'Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection' (2001) 27 N.C.J.Int'l.L.&Com.Reg. 95, 97.

[1543] John Fialka, 'While America Sleeps' (1997) 21(1) The Wilson Quarterly 48, 50-1.

[1544] Andrew Crane, 'In the company of spies: when competitive intelligence gathering becomes industrial espionage' (2005) 48 Business Horizons 233, 234.

[1545] Lathrop (n.913) 130.

Three TRIPS articles are of potential interest regarding cyber-espionage: articles 3(1), 39 and 73. They respectively oblige states to ensure national treatment, to protect undisclosed information, and provide them with security exceptions. The doctrinal arguments based on TRIPS in general, and on these specific articles are first evoked (1). Then, a textual interpretation of these articles is carried out in the status of law (2). Finally, a conclusion is set up (3).

1. Status of doctrine

Doctrine adopts two main positions with respect to TRIPS. Either it directly applies some of its provisions to cyber-espionage (1.1), or it resorts to unofficial means of interpretation (1.2).

1.1. Arguments based on the direct application of TRIPS articles

As suggested previously, three TRIPS articles are usually invoked by doctrine when tackling the legality of economic espionage: articles 3 (national treatment) (A), 39 (the protection of undisclosed information) (B), and 73 (the national security exception) (C).

A. Arguments based on national treatment (article 3)

Fidler thinks that this provision is not relevant to the regulation of economic cyber-spying. 'As a general matter of law, IP [Intellectual Property] rights are granted and protected on a territorial basis by national governments'.[1546] Then, '[n]othing in the WTO generally or TRIPS specifically mandates that [...] any other WTO member protect commercially valuable information found in the territories of other countries'.[1547] Indeed, 'TRIPS does not require WTO

[1546] David Fidler, 'Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage' (*ArmsControlLaw,* 11.02.2013) <https://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/> accessed:03.05.2017.

[1547] Ibid.

members to prohibit their nationals or companies from engaging in corporate espionage inside foreign nations, nor does TRIPS regulate government-led economic espionage within other countries.[1548] He adds that 'WTO rules create obligations for WTO members to fulfil within their territories and do not generally impose duties that apply outside those limits'. [1549] Then, 'WTO members that covertly obtain intellectual property of nationals of other WTO members operating in their territories could violate WTO obligations to protect such property'.[1550] The problem with espionage is that it 'involves governments obtaining information from private-sector companies located outside their territories'.[1551]

On the contrary, Parajon-Skinner responds to Fidler, and thinks that '[t]his assumption may prove too much'.[1552] 'That the harm is done in cyber space seems a poor reason to limit application of the TRIPS Agreement, which was, in any event, negotiated before the rise' of cyber-threats.[1553] She then refers to the preamble of the TRIPS, and affirms that '[i]n short, to remain relevant, the WTO Agreements must consider the possibility of cyber violation'.[1554] Malawer wonders: '[w]hat if the member state directs its efforts to secure information abroad, and then turn it over to its domestic firms? Is this a loophole?'[1555] He answers: '[n]ot in this case. As is apparent in snooping on foreign firms within the member state, the protected information is being used to benefit local firms'. [1556] In other words, 'it is providing treatment to foreign firms doing

[1548] Ibid.

[1549] Fidler, 'Economic Cyber Espionage and International Law' (n.835).

[1550] Ibid.

[1551] Ibid.

[1552] Parajon-Skinner (n.591) 1197.

[1553] Ibid.

[1554] Ibid.

[1555] Stuart Malawer, 'Chinese Economic Cyber Espionage: U.S. Litigation in the WTO and Other Diplomatic Remedies' (2015) 16 Geo.J.Int'l.L. 158, 161.

[1556] Ibid.

business within the member state that is less favorable than it provides to its own national firms'.[1557] Lotrionte similarly thinks that 'China, in providing government-sponsored commercial intelligence based on stolen IP to its own firms, is giving its own nationals a more favorable treatment, arguably in violation of its obligation under TRIPS'.[1558]

There are two opposing visions regarding the impact of national treatment on cyber-espionage. In contrast, authors are more consensual about article 39.

B. Arguments based on the protection of undisclosed information (article 39)

According to Blood, 'two provisions in Article 39 undercut its effectiveness in protecting trade secrets from economic espionage'.[1559] On the one hand, '[i]n specifically referencing the Paris Convention's Article 10bis', article 39(1) 'leaves itself open to being construed to afford no more protections against unfair competition than those accorded by the Paris Convention'.[1560] On the other hand, 'by providing specific examples of activities "contrary to honest commercial practices", and by failing to specifically include the unlawful taking of proprietary information', article 39(2) and its footnote 10 'may implicitly suggest to its signatories that the protection of trade secrets is of but ancillary importance in the overall scheme of intellectual property rights protection'.[1561] According to Danielson, 'TRIPS does not specifically address economic espionage. Since that proprietary information theft is not among its enumerated activities, "contrary to honest commercial practices" may imply that trade secret protection is an ancillary concern in TRIPS' overall IP protection scheme'.[1562]

[1557] Ibid.

[1558] Lotrionte (n.797) 527.

[1559] Christopher Blood, 'Holding Foreign Nations Civilly Accountable for Their Economic Espionage Practices' (2002) 42(2) I.D.E.A. 227, 235.

[1560] Ibid.

[1561] Ibid.

[1562] Mark Danielson, 'Economic espionage: a framework for a workable solution' (2008) 10(2) Minn.J.L.Sci.&Tech. 503, 520.

Strawbridge similarly thinks that '[...] TRIPS Article 39 does not appear to be an effective safeguard against cyber economic espionage perpetrated by foreign governments'.[1563] Indeed, 'the language of TRIPS Article 39.2 appears to imply a jurisdictional limitation–i.e. WTO Members must afford this "possibility" only to natural and legal persons who are operating within their territory [...]'.[1564] Moreover, 'the use of the word "possibility" suggests that this obligation relates to the establishment of a cause of action; such persons must have the "possibility" of protecting their trade secrets through judicial proceedings'.[1565] His final argument is that '[w]here WTO Members wanted to impose a TRIPS obligation directly on the government, they did so in explicit terms'.[1566]

Most authors thus conclude that no prohibition of cyber-espionage stems from article 39. The debate surrounding security exceptions is however more disputed.

C. Arguments based on the security exceptions (article 73)

The scope of this provision raises disagreements. According to Brenner, '[t]he practical difficulties of implementing even limited espionage protections under the WTO […] begin with the need to put a boundary on the national security exception to the TRIPS rules'.[1567] Moreover, 'the Chinese and Russians do not recognize a distinction between national and economic security'.[1568]

Considering that 'China and other nations are violating their international commitments by tolerating IP theft' and 'by establishing state programs to steal

---

[1563] James Strawbridge, 'The Big Bluff–Obama, Cyber Economic Espionage, and the Threat of WTO Espionage' (2016) 47 Geo.J.Int'l.L. 833, 859.

[1564] Ibid 858.

[1565] Ibid 858-9.

[1566] Ibid 859.

[1567] Joel Brenner, 'The New Industrial Espionage', *The American Interest* (10.12.2014) <www.the-american-interest.com/2014/12/10/the-new-industrial-espionage/> accessed:15.02.2016.

[1568] Ibid.

IP',[1569] Lewis affirms that the national security exception 'provides the vehicle for the United States and its allies to move outside the constraints of the WTO to address cyber-espionage'.[1570] It would indeed be 'a significant reinterpretation of this exception to use it to justify a vigorous response (or to threaten a vigorous response) to cyber-espionage'.[1571] According to Malawer, 'China could hardly claim that cyber-theft of commercial information is part of its "essential security interests" and that this is a "time of war or other emergency in international relations"'.[1572]

There is no consensus regarding the capacity of these articles in combating cyber-espionage. Some authors thus turn to unofficial means of interpretation to support the illegality of economic cyber-espionage.

1.2. Arguments based on the application of unofficial means of interpretation

Applying unofficial means of interpretation–i.e., means not favoured by the VCLT–is another method used by scholars to tackle spying. The first one consists in taking into account the whole corpus of TRIPS–without selecting a single provision for purpose of interpretation–to deduce that espionage is unlawful (A). The second one relies on Dispute Settlement Body (DSB) case-law: as the latter found that CIL applied to the WTO rules, their provisions could allegedly be interpreted in the light of the principle of non-intervention to prohibit spying (B). Finally, the letter and spirit of the WTO agreements and TRIPS allegedly go against economic cyber-espionage (C).

[1569] James Lewis, *Conflicts and Negotiations in Cyberspace* (CSIS 2013) 44.

[1570] Ibid 50.

[1571] Ibid.

[1572] Malawer, 'Chinese Economic Cyber Espionage' (n.1555) 162.

A. Arguments based on TRIPS' whole corpus

Various conventions aim at protecting intellectual property. Paris Convention–which is now incorporated in TRIPS–imposes national treatment (article 2) and protection against unfair competition (article 10bis). TRIPS additionally prevents the disclosure of secret information of commercial value,[1573] and protects industrial designs,[1574] copyrights,[1575] and patents.[1576]

According to Parajon-Skinner, '[t]ogether, these rights and enforcement principles suggest two things relevant to economic cyber-espionage. First, the rules require member states to protect innovative economic activity that is not necessarily developed or owned by the state itself, but rather by private economic actors. Second, member states are bound to protect one another's intellectual property and refrain from any activity that impedes those rights […] WTO appears as an obvious forum, but has never been used'.[1577]

Relying on the whole corpus allows her to conclude that economic cyber-espionage is illegal. Authors reach a similar conclusion in interpreting TRIPS in the light of sovereignty and non-intervention.

B. Arguments based on the interpretation of the WTO rules and TRIPS in the light of sovereignty and non-intervention

Whether the WTO creates a self-contained regime has sometimes been disputed.[1578] Self-contained regimes comprise 'not only rules that regulate a

---

[1573] TRIPS, art.39.

[1574] TRIPS, arts.25-26.

[1575] TRIPS, arts.9-14.

[1576] TRIPS, arts.27-34.

[1577] Parajon-Skinner (n.591) 1196.

[1578] Joost Pauwelyn, 'The Role of Public International Law in the WTO: How far can we go?' (2001) 95 A.J.I.L. 535, 535-78.

particular field or factual relations laying down the rights and duties of the actors within the regime (primary rules), but also a set of rules that provide for means and mechanisms to enforce compliance, to settle disputes, to modify or amend the undertakings, and to react to breaches (secondary rules), with the intention to replace and through this to exclude the application of general international law, at least to a certain extent'.[1579]

According to article 23 of the Dispute Settlement Understanding (DSU), members are required to 'have recourse to, and abide by, the rules and procedures' of the DSU when they 'seek the redress of a violation of obligations or other nullification or impairment of benefits under the covered agreements or an impediment to the attainment of any objective of the covered agreements'.[1580]

However, the WTO rules are not isolated from the whole corpus of international law. Firstly, article 3.2 DSU affirms that they are to be clarified 'in accordance with customary rules of interpretation of public international law'. Secondly, DSB Panels have taken into account existing international law and rules of treaty interpretation in various cases. In the *Gasoline* case, the panel noted: 'the General Agreement is not to be read in clinical isolation from public international law'.[1581] It then applied 'the basic principle of interpretation that the words of a treaty, like the General Agreement, are to be given their ordinary meaning, in their context and in the light of the treaty's object and purpose'.[1582] According to a subsequent case, 'to the extent there is no conflict or inconsistency, or an expression in a covered WTO agreement that implies differently, we are of the view that the customary rules of international law apply to the WTO treaties and

[1579] Eckart Klein, 'Self-Contained Regime' (2006) M.P.E.P.I.L., [1].

[1580] Understanding on the Rules and Procedures Governing the Settlement of Disputes (Annex 2 of Marrakesh Agreement Establishing the World Trade Organization) 1869 UNTS 401, art.23.

[1581] *US–Gasoline* (20.05.1996) WT/DS2/9, 17.

[1582] Ibid.

to the process of treaty formation under the WTO'.[1583] In the *Hormones* case, the panel referred to the principle of good faith.[1584]

Parajon-Skinner mentions that '[t]he WTO agreements' silence on the issue of cyber trade violations presents a classic situation in which customary principles should be consulted to interpret the agreements' scope and applicability in this domain'.[1585] She then says that '[n]o TRIPS provision has explicitly (and entirely) contracted out of the fundamental tenants of state sovereignty and state responsibility. Nor is TRIPS inconsistent with these general principles'.[1586] As a consequence–and in light of WTO case-law–'[t]he economic corollaries of sovereignty and non-intervention–in addition to the well-recognized requirement to comply with one's treaty obligations in good faith–should therefore give rise to a cognizable claim that economic cyber-espionage violates TRIPS'.[1587] Lotrionte refers to both the *Gasoline* case and article 31(2) (c) of the VCLT.[1588] She subsequently suggests that '[i]t may be that while the WTO rules say nothing about economic espionage, the customary norm of non-intervention will lend interpretive value to the WTO rules to find that such state behavior is not acceptable under the WTO regime'.[1589]

Interpreting TRIPS in the light of DSU and DSB case-law allows doctrine to assert that espionage is illegal. A similar conclusion is reached by authors when they rely on the letter and spirit of the WTO agreements.

[1583] *Korea–Measures affecting Government Procurement* (01.05.2000) WT/DS163/R [7.96].

[1584] *Canada–Continued Suspension of Obligations in the EC–Hormones Dispute* (31.03.2008) WT/DS321/R, paras 7.310-7.323; *United States–Continued Suspension of Obligations in the EC–Hormones Dispute* (31.03.2008) WT/DS320/R, [7.310]-[7.323].

[1585] Parajon-Skinner (n.591) 1199-200.

[1586] Ibid 1200.

[1587] Ibid.

[1588] Lotrionte (n.797) 529.

[1589] Ibid.

C. Arguments based on the letter and spirit of the WTO agreements and TRIPS

According to Lotrionte, '[e]ven though there is no express economic espionage prohibition in the WTO rules or the TRIPS agreement, the letter and spirit of the agreements indicate that theft of trade secrets are prohibited'.[1590] As TRIPS was drafted before the emergence of Internet, Brenner says that it does 'not deal with cross-border enforcement challenges'.[1591] He nevertheless refers to articles 26 and 39(2), and affirms that 'TRIPS already enshrines principles of fair play and honest dealing that are inconsistent with cross-border IP theft "for commercial purposes"'.[1592]

In other words, doctrine resorts to a diversity of interpretative tools and disagrees on the legal regime of economic cyber-espionage. Resorting to the VCLT rules of interpretation nevertheless demonstrates that economic cyber-espionage is not prohibited by TRIPS and the WTO rules.

2. Status of law

The provisions related to national treatment (2.1), the protection of undisclosed information (2.2) and the security exceptions (2.3) could be of relevance to cyber-espionage, and have to be alternatively analysed.

2.1. National treatment (article 3)

Article 3 provides that '[e]ach Member shall accord to the nationals of other Members' treatment no less favourable than that it accords to its own nationals with regard to the protection of intellectual property [...]'.

Even though the TRIPS' preamble acknowledges 'the need to promote effective

[1590] Lotrionte (n.797) 527.

[1591] Brenner (n.1567).

[1592] Ibid.

and adequate protection of intellectual property rights', a textual interpretation of 'accord[ing] to the nationals of other Members treatment no less favourable than that it accords to its own nationals' does not actually reveal a potential extraterritorial application. National treatment may be defined as '[t]he policy or practice of a country that accords the citizens of other countries the same intellectual-property protection as it gives its own citizens, no formal treaty of reciprocity being in place'.[1593] Members thus have a positive obligation of according national treatment, not to abstain from spying. Then, the WTO's website itself confirms that, in compliance with national treatment, '[i]mported and locally-produced goods should be treated equally–at least after the foreign goods have entered the market. The same should apply to foreign and domestic services, and to foreign and local trademarks, copyrights and patents'.[1594] The focus is thus on the very territory of the Member. Then, when entering the market, a product is usually no longer a secret. Rather, it becomes protected by 'trademarks, copyrights and patents'. 'Trade secret' and 'to enter the market' are thus antagonistic notions, and renders the provision irrelevant to spying.

The subsequent claims made by states before the DSB confirm that article 3 has no extraterritorial scope, as the cases based on articles 3 and 3.1 were prompted by the following claims. According to the USA, EC regulation 2081/92 'limit[ed] the access of nationals of other Members to the EC GI [geographical indications] procedures and protections provided under the Regulation'.[1595] The EC affirmed: 'the registration or renewal in the United States of a trademark previously abandoned by a trademark owner whose business and assets have been confiscated under Cuban law is no longer permitted'.[1596] Japanese legislation would not protect sound recordings for a sufficient time.[1597] The EC was unhappy with section 337 of the US Tariff Act, which dealt with 'unfair

[1593] Black's (n.863) 'national treatment'.

[1594] WTO, 'Principles of the Trading System' <www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm> accessed:16.05.2017.

[1595] *EC–Trademarks and Geographical Indications* (10.04.2003) WT/DS174/1/Add.1.

[1596] *US–Section 211 Appropriations Act* (15.07.1999) WT/DS176/1.

[1597] *Japan–Measures concerning Sound Recordings* (04.06.1996) WT/DS42/1.

practices in import trade'.[1598] Ukraine contended that Australian requirements on tobacco packaging failed to provide 'equal competitive opportunities to imported tobacco products and foreign trademark right holders as compared to like domestic tobacco products and trademark right holders'.[1599] They were also challenged by Honduras, [1600] the Dominican Republic, [1601] Cuba, [1602] and Indonesia[1603] on the basis of article 3, but no real justification was provided. The USA affirmed that an Indonesian 'exemption from customs duties and luxury taxes on imports of "national vehicles"' was illegal. Indeed, 'their effect [was] to displace or impede imports of motor vehicles and motor vehicle parts and components from the United States, and to cause significant price undercutting by the subsidized products compared with products from another Member in Indonesia'. [1604] According to the USA, Chinese copyright laws 'provide[d] different pre-distribution and pre-authorization review processes' for the 'works, performances […] and sound recordings' of 'Chinese nationals' and 'foreign nationals'.[1605] The former allegedly received 'more favourable protection'.[1606] The broadcast and access of television content 'over which Qatari nationals [held] copyrights and related broadcasting rights' and their use 'in the territory' of Saudi Arabia,[1607] Bahrain,[1608] and the United Arab Emirates[1609] was allegedly restricted.

1598 *United States–Section 337 of the Tariff Act of 1930 and Amendments Thereto* (18.01.2000) WT/DS186/1.

1599 *Australia–Tobacco Plain Packaging (Ukraine)* (15.03.2012) WT/DS434/1.

1600 *Australia–Tobacco Plain Packaging (Honduras)* (10.04.2012) WT/DS435/1.

1601 *Australia–Tobacco Plain Packaging (Dominican Republic)* (23.07.2012) WT/DS441/1.

1602 *Australia–Tobacco Plain Packaging (Cuba)* (07.05.2013) WT/DS458/1

1603 *Australia–Tobacco Plain Packaging (Indonesia)* (20.09.2013) WT/DS467/1

1604 *Indonesia–Autos* (15.10.1996) WT/DS59/1

1605 *China–Intellectual Property Rights* (16.04.2007) WT/DS362/1.

1606 Ibid.

1607 *Saudi Arabia–Measures Relating to Trade in Goods and Services, and Trade-Related Aspects of Intellectual Property Right* (01.08.2017) WT/DS528/1, [7].

1608 *Bahrain–Measures Relating to Trade in Goods and Services, and Trade-Related Aspects of Intellectual Property Right* (04.08.2017) WT/DS527/1.

As a consequence, national treatment does not prevent extraterritorial spying. Similarly, the rule of protection of undisclosed information proves to be ineffective.

2.2. Protection of undisclosed information (article 39)

This thesis asserts that, under article 39, states are not obliged to refrain from spying. Their burden is actually mentioned in article 39(1): '[i]n the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3'. The provision mentioned–Article 10bis of the Paris Convention–says that '[t]he countries of the Union are bound to assure to nationals of such countries effective protection against unfair competition'.

According to article 39(2), '[n]atural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices […]'. Yet, the formula 'a manner contrary to honest commercial practice' does not call for an external definition. As Blood noted, footnote 10 already sets minimum standards for this.[1610] Thus, it 'shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition'.

The next step is to determine whether governments might be considered 'third parties', and would thus be prevented from acquiring 'undisclosed information'

[1609] *United Arab Emirates–Measures Relating to Trade in Goods and Services, and Trade-Related Aspects of Intellectual Property Rights* (12.10.2017) WT/DS526/2, [8].

[1610] Blood (n.1559) 235.

(i.e. spying). This is highly unlikely. Firstly, a textual interpretation does not really allow one to deduce that 'third parties' include Member states. Context is decisive here. All along the TRIPS, states are referred to as 'Members' or 'governments', while 'third parties' clearly denominate non-state actors. Article 31 is a convincing example: '[w]here the law of a Member allows for other use of the subject matter of a patent without the authorization of the right holder, including use by the government or third parties authorized by the government, the following provisions shall be respected [...]'. Article 30 also says that '[m]embers may provide limited exceptions to the exclusive rights conferred by a patent [...] taking account of the legitimate interests of third parties'.

Pursuant to article 39, states thus have a positive obligation: to give private persons the means to protect undisclosed information from 'others'. States are not required to abstain from spying abroad. Article 39(3) similarly expresses a positive obligation: states have to protect the undisclosed information submitted to them against unfair commercial use and divulgation. No negative obligation– such as abstaining from spying–stems from it. This is in line with TRIPS' object and purpose, which is that states adopt efficient domestic mechanisms. This results from both the preamble and article 1. States express their desire 'to reduce distortions and impediments to international trade', to take 'into account the need to promote effective and adequate protection of intellectual property rights', and to ensure that the measures taken 'do not themselves become barriers to legitimate trade'.[1611] To this end, they recognize 'the need for new rules and disciplines concerning [...] (c) the provision of effective and appropriate means for the enforcement of trade-related intellectual property rights, taking into account differences in national legal systems'.[1612] In this context, 'Members shall be free to determine the appropriate method of implementing the provisions of this Agreement within their own legal system and practice'.[1613]

[1611] TRIPS, preamble.

[1612] Ibid.

[1613] TRIPS, art.1.

Moreover, nothing in subsequent practice allows one to affirm that such provisions may prohibit extraterritorial cyber-spying. The WTO itself confirms that '[n]o jurisprudence or decision of a competent WTO body' exists regarding article 39'.[1614] Yet, some initiatives have been taken by American Congressmen to draw the WTO's attention to Chinese cyber-espionage. Representatives Levin and Rangel wrote a letter to US Trade Representative Marantis on 29 March 2013, stating that 'IP-thefts by China […] appear to be a straightforward violation of the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights'.[1615] On 22 May 2014, Senator Schumer wrote to Michael Froman, the new US Trade Representative. He urged him 'to initiate a case at the [...] WTO against China for state-backed cyber-espionage against American businesses and workers', as '[...] TRIPS requires each WTO member to protect trade secrets and Chinese policies that sanction cyber-espionage are in clear violation of that agreement'.[1616] But such efforts have remained dead letter, and no panel has ever been seized.

There is a recent trend in reaching non-binding agreement with respect to trade secrets. It started with Xi Jinping's visit in America in 2015. According to a statement, '[t]he United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors'.[1617] Two months later, a similar formula was used by the

---

[1614] WTO, 'Interpretation and Application of Article 39' <www.wto.org/english/res_e/booksp_e/analytic_index_e/trips_03_e.htm#article39> accessed:03.05.2017.

[1615] US House Committee on Ways and Means, 'Levin, Rangel to USTR: Consider Designating China "Priority Foreign Country" for Alleged Trade Secrets Theft' (28.03.2013) <https://democrats-waysandmeans.house.gov/media-center/press-releases/levin-rangel-ustr-consider-designating-china-priority-foreign-country> accessed:11.11.2016.

[1616] GPO, 'Schumer calls on U.S. Trade Rep to file WTO Suit in Response to Chinese Cyber-Attacks' (22.05.2014).
Accessed:via Factiva <https://global.factiva.com> accessed:11.11.2016.;
'U.S. Indictment On Chinese Cyber Theft Largely A Strong Political Warning', Inside U.S. Trade (23.05.2014).
Accessed:via Factiva <https://global.factiva.com> accessed:11.11.2016

[1617] The White House, 'President Xi Jinping's State Visit to the United States' (25.09.2015)

G20 Leader's Communiqué in Antalya: 'no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors'. The latter sentence has since been replicated by the G7,[1618] and by the US–Nordic Leaders' Summit.[1619] Perhaps more importantly, it received the support of more than fifty states,[1620] in the framework of the *Paris Call of 12 November 2018 for Trust and Security in Cyberspace.*[1621] American Congressmen asked the President to promote this objective in multilateral relations.[1622] However, none of these instruments is binding, and their efficiency is debated. A report by FireEye estimates that, between 2013 and 2016, the Chinese threat 'is less voluminous but more focused, calculated, and still successful in compromising corporate networks'.[1623] It does not view 'Xi-Obama agreement as a watershed moment', but as 'one point amongst dramatic changes that had been taking place for years'.[1624] The evolutions are allegedly linked to 'President Xi's military and political initiatives, the widespread exposure of Chinese cyber-operations, and mounting pressure from the U.S. Government'.[1625]

<obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> accessed:05.10.2016.

[1618] G7, 'G7 declaration on responsible states behavior in cyberspace' (2017) [12] <www.g7italy.it/sites/default/files/documents/Declaration_on_cyberspace_0.pdf> accessed:22.12.2017.

[1619] 'US–Nordic Leaders' Summit, Joint Statement' (n.731).

[1620] Gouvernement, 'List of Supporters of the Paris Call for Trust and Security in Cyberspace' (*France Diplomatie*, 2018) <www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in#sommaire_4> accessed:13.11.2018.

[1621] Gouvernement, 'Paris Call for Trust and Security in Cyberspace' (*France Diplomatie*, 12.11.2018) <www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf> accessed:13.11.2018

[1622] HoR, 'A bill to support US international cyber diplomacy' (introduced by Mr Royce) (2017) 115th Congress, 1st session, section 3(5)(A).

[1623] FireEye, *Redline drawn: China recalculates its Use of Cyber Espionage* (FireEye Incorporated 2016) 15.

[1624] Ibid.

[1625] Ibid.

It results from the above that 'Members' have to enforce intellectual property rights on their own territories but are not prevented from spying abroad. Moreover, cultural differences help demonstrating that article 73's security exceptions are unable to discourage economic cyber-espionage.

2.3. Security exceptions (article 73)

According to article 73(a), '[n]othing in this Agreement shall be construed [...] to require a Member to furnish any information the disclosure of which it considers contrary to its essential security interests'. As a consequence, a state suspected of spying may perfectly remain silent when held to account. Then, a Member is not prevented 'from taking any action which it considers necessary for the protection of its essential security interests'.[1626] They include measures related to 'fissionable materials or the materials from which they are derived',[1627] 'the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment'.[1628] Measures 'taken in time of war or other emergency in international relations' are also included,[1629] and nothing prevents a Member from taking 'any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security'.[1630]

As evoked previously, some scholars challenge the fact that IP theft could be considered as an essential security interest. A problem with this approach is that it totally ignores different economic cultures. China is opposed to the American vision, that promotes a legal regime distinguishing between economic and

---

[1626] TRIPS, art.73(b).

[1627] TRIPS, art.73(b)(i).

[1628] TRIPS, art.73(b)(ii).

[1629] TRIPS, art.73(b)(iii).

[1630] TRIPS, art.73(c).

political-military spying. Such an attempt is indeed ill perceived: 'by dividing cyberespionage into "bad" and "good" activities, Washington is trying to dictate the rules for global cyberdomain, which is a public space'.[1631] In the Russian and Chinese views, 'all state-sponsored espionage is by definition conducted in the national interest'.[1632] The distinction 'between the public and private sectors is either non-existent or blurred', as 'public and private actions are expected to support national policy'.[1633] Yet, this cultural difference was at the epicentre of American justification when ECHELON was discovered. The former CIA director denounced the 'dirigisme' of European states, which led them to 'bribe'.[1634]

3. Conclusion

Whether carried out through a physical or a cyber-intrusion, economic espionage is left unregulated by TRIPS. Article 3 does not restrict extraterritorial conducts, while article 39 does not place states under a negative obligation: they are not prevented from spying. Two trends confirm this finding. First, many states' protests are made without any express reference to the WTO rules. In 2011, US NCSC's report to the Congress denounced cyber-activities carried out by China and Russia. Mike Rogers, the Intelligence Committee's Chairman, said: '[t]his once again underscores the need for America's allies across Asia and Europe to join forces to pressure Beijing to end this illegal behaviour'.[1635] Following revelations on US spying on national oil companies, Venezuelan President Maduro called it 'a violation of international law'.[1636] After revelations on

[1631] David Sanger, 'Differences on Cybertheft complicate China Talks', *NYT* (10.07.2013) <www.nytimes.com/2013/07/11/world/asia/differences-on-cybertheft-complicate-china-talks.html?ref=technology> accessed:03.05.2017.

[1632] Brenner (n.1567).

[1633] Ibid.

[1634] James Woolsey, 'Why We Spy on Our Allies', *Wall Street Journal* (17.03.2000) <www.wsj.com/articles/SB953268243116572 69> accessed:07.02.2018.

[1635] Zakaria Tabassum, 'U.S. blames China, Russia for cyber-espionage', *Reuters* (03.11.2011) <www.reuters.com/article/us-usa-cyber-china-idUSTRE7A23FX20111103> accessed:06.09.2015.

[1636] Eyanir Chinea and Girish Gupta, 'Venezuela president orders investigation after report on U.S. spying', *Reuters* (18.11.2015)

ECHELON, the French Minister of Justice failed to refer to any legal terms, mentioning 'a misappropriation for purposes of economic espionage and business intelligence'.[1637] She rather referred to concrete measures to be adopted.[1638] Second, states have settled for non-binding instruments, and nothing actually indicates that they want to create any rules in the field.

<www.reuters.com/article/us-venezuela-usa-idUSKCN0T80AB20151119> accessed:11.11.2016.

[1637] AN, '1ere séance du 23 février 2000' (n.734).

[1638] Ibid.

THIRD PART – A SPECIAL CUSTOMARY LAW ON CYBER-ESPIONAGE

The application of existing rules–both conventional and customary–to cyber-espionage is unsatisfactory, as they offer sparse and unequal protection against such activities. As a consequence, there is a great temptation in looking for new customary rules, which would prohibit espionage *per se*. Yet, espionage has always existed, in both peacetime and wartime, on the land, on the seas, and in the air. England, France and Russia already had intelligence organizations in the 1600's,[1639] and history brims with famous spies: Mata Hari, Richard Sorge, the Rosenberg, Kim Philby, Jonathan Pollard etc. While US Secretary of State Stimson thought that espionage was unethical–and declared in 1929 that 'gentlemen do not read each other's mail',[1640] '[s]ince the beginning of World War II, intelligence and counterintelligence have been major governmental concerns for the United States'.[1641] Moreover, the territorial disconnection of espionage is not a new phenomenon. It already happened with satellites in the 60's. When the Samos programme started, it was supposed to 'carry photographic and TV equipment that permits perception of surface objects equivalent to what the human eye sees from one hundred feet. This should [have been] enough to pick up troop concentrations, airfields, missile sites, and much other useful information'.[1642] The UNGA finally ended up adopting an untitled resolution, '[p]rinciples relating to remote sensing of the Earth from space'.[1643] According to Klaousen, 'owing to the Christian spiritual heritage, Westerners are probably the only ones to worry that much about the effective integration of moral principles in the right conduct [...] They are also the only ones who believe

---

[1639] David McElreath and others, *Introduction to Homeland Security* (2nde edn, CRC Press 2013) 297.

[1640] Olga Khazan, 'Gentlemen Reading Each Other's Mail: A Brief History of Diplomatic Spying', *The Atlantic* (17.06.2013) <www.theatlantic.com/international/archive/2013/06/gentlemen-reading-each-others-mail-a-brief-history-of-diplomatic-spying/276940/> accessed:22.03.2018.

[1641] Shreve Ariail, Frederic Hitz and Daniel Silver, 'Intelligence and Counterintelligence', in Norton Moore and Turner (n.1209) 935.

[1642] Richard Falk, 'Space Espionage and World Order: A Consideration of the Samos-Program' in Stanger (n.569) 46. See also: Luc Frieden, 'Newsgathering by Satellites: A New Challenge to International and National Law at the Dawn of the Twenty-First Century' (1988-9) 25 Stan.J.Int'l.L. 103; Herbert Scoville, 'Is Espionage Necessary for Our Security' (1976) 54 Foreign Affairs 482, 484-6.

[1643] UNGA Res 41/65 (3.12.1986) [Principles relating to remote sensing of the Earth from space].

that it is a universal concern'.[1644] It remains to be seen how doctrine (1) and law (2) reflect such complexity. A conclusion is finally available (3).

1. Status of doctrine

Four types of arguments may be found in doctrinal works. First, authors may rely on both general practice and *opinio juris*, in favour or against the prohibition of espionage (1.1). Then, some authors may insist on practice to support the authorisation of espionage (1.2), or on *opinio juris* to defend the opposite position (1.3).

1.1. Arguments based on practice and *opinio juris*

The joint analysis of practice and *opinio juris* has either been used to demonstrate the authorization (A), the prohibition (B), or the silence of customary law regarding espionage (C).

A. Arguments supporting the authorization of espionage

Invocation of CIL had already happened with respect to previous forms of espionage.

Smith affirms that 'virtually every state has an intelligence service that seeks to collect information on potential adversaries', which 'frequently violate the municipal (or domestic) law of other states'.[1645] However, 'because espionage is such a fixture in international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law'.[1646] According to him, '[e]vidence of that is that when intelligence officers are accused of operating under diplomatic cover in an embassy, they are nearly always declared personae non gratae and

[1644] Patrick Klaousen, 'Le moindre mal nécessaire' in Patrick Klaousen and Thierry Pichevin (eds), *Renseignement et Ethique, Le Moindre Mal Nécessaire* (Lavauzelle 2014) 29.

[1645] Smith (n.1454) 544.

[1646] Ibid.

sent home. In exercising the right to "PNG" a diplomat, the receiving state typically says their activities were inconsistent with diplomatic activities'.[1647] He concludes as follows: 'I can recall no instance in which a receiving state has said that these activities violate international law'.[1648] Kish thinks that '[t]he exchange of spies has manifested the mutual admission of espionage as State practice recognized in customary international law'.[1649] Lafouasse,[1650] Cohen-Jonathan and Kovar[1651] all affirm that spying has only been punished by domestic courts. As a consequence, it could not be deduced that such activity is prohibited in CIL. Frieden affirms that '[a]n example of the development of customary international law concerns the overflight of foreign territory by spacecraft. Although this practice was not specifically authorized by the international community, it was carried out in the early 1960s without protest by any government. As a result, overflight by spacecraft is now recognized as legitimate under international law'.[1652] According to Lotrionte, 'given the fact that all states send spies to "clandestinely" collect information within other states, and that most states have passed domestic legislation establishing the some form of legal authority for such clandestine activities, it would seem that there exists *opinio juris* on the practice of espionage'.[1653] Wright thinks that 'this would appear to be a case in which frequent practice has not established a rule of law because the practice is accompanied not by a sense of right but by a sense of wrong'.[1654] Adams, who refers to the fact that spying has existed since ancient times, says: 'History should speak for itself [...] states have shaped the international arena through their conduct, but also through their refusal to craft international law

---

[1647] Ibid.

[1648] Ibid.

[1649] Kish and Turns (n.66) 155.

[1650] Lafouasse, 'L'Espionnage' (n.574) 66.

[1651] Cohen-Jonathan and Kovar (n.567) 253-4.

[1652] Luc Frieden, 'Newsgathering by Satellites: A New Challenge to International and National Law at the Dawn of the Twenty-First Century' (1988-9) 25 Stan.J.Int'l.L. 103, 115.

[1653] Lotrionte (n.797) 487-8.

[1654] Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in Stanger (n.569) 17.

obstructions to their national security interests-particularly when acting for benign defensive purposes'.[1655] He then affirms that 'state custom illustrates that national security activities conducted outside of armed conflict occur, and have historically occurred, with regularity, creating or reflecting the existence of a customary international norm'. [1656] Furthermore, 'international law does not distinguish between apparent or publicly acknowledged state action, and statecraft that may be covert, clandestine, low in visibility, or otherwise unapparent'.[1657]

This trend is now commonplace regarding cyber-espionage. According to Beard, there is no custom with respect to cyber-operations: 'state practice in this area […] reflects conscious neglect, confusion, lack of consensus, and enormous practical and legal difficulties in both determining the origin of hostile cyber actions and in imposing a territorial model on them'.[1658] Joyner thinks that '[a]s a source of customary international law, state practice seems to sympathise with permitting some IW activities. For instance, espionage, universally criminal under domestic laws, does not *ipso facto* violate international law'.[1659]

A joint analysis of practice and *opinio juris* allows some authors to conclude that cyber-espionage is a lawful activity. However, the same tools enable others to support the opposite vision.

B. Arguments supporting the prohibition of espionage

According to Buchan, practice must be public and open, whereas 'state practice committed in secret is irrelevant' and 'cannot be classified as state practice for

[1655] Michael Jefferson Adams, 'Jus Extra Bellum: Reconstructing the Ordinary, Realistic Conditions of Peace' (2014) 5 Harv.Nat'l.Sec.J. 377, 396-7.

[1656] Ibid 401.

[1657] Ibid 402.

[1658] Beard (n.594) 90.

[1659] Christopher Joyner, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12(5) E.J.I.L. 825, 860.

the purpose of customary law formation'.[1660] As Wood's second report mentions that 'it is difficult to see how' confidential practice 'can contribute to the formation or identification of general customary international law',[1661] he affirms that 'States must indeed be given the opportunity "to respond to it positively or negatively"'.[1662] He adds that 'customary international law forms on the basis of specific "instances of State conduct" that form "a web of precedents" from which an observable pattern is identifiable'.[1663] The problem–he notes–is that 'specific instances of espionage are committed in secret' and cannot be accepted as evidence of state practice.[1664] He then tackles *opinio juris*, and affirms that States must 'assert the international legality of their conduct' or 'at least to say it is permissible under IL'.[1665] However, 'when challenged about their espionage activities, states overwhelmingly refuse to admit responsibility for this conduct'.[1666] According to him, 'a further point is relevant here [...] When states discover that they are the victims of espionage, they often protest (and often vociferously) that such conduct is contrary to international law'.[1667] He then analyses the American reaction following the Sony Pictures hacking and affirms that 'a reasonable reading of the US's reaction to the Sony incident is that it regarded such conduct as incompatible with international law'.[1668]

Beside the arguments supporting the prohibition or the authorization of espionage, a third approach appears in doctrine: the silence of international law.

[1660] Russell Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage' in Anna-Maria Osula and Henry Röigas (eds), *International Cyber Norms: Legal, Policy&Industry Perspectives* (NATO CCD COE Publications 2016) 82.

[1661] Wood, 'Second report' (n.423) [47].

[1662] Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage' (n.1660) 82.

[1663] Ibid 83.

[1664] Ibid.

[1665] Ibid.

[1666] Ibid.

[1667] Ibid 84.

[1668] Ibid 85.

C. Arguments based on the silence of customary international law

Some scholars think that CIL has little to say about espionage. After referring to state practice and *opinio juris*, Khalil affirms that '[c]ustomary international law [...] fails to provide the international community with a set a rules governing espionage on foreign states and individuals',[1669] and 'could plausibly support both sides of the surveillance debate'. [1670] Radsan says that 'customary international law, so it seems, has very little to say about espionage'. [1671] Edmondson thinks that '[c]ustomary international rules governing the conduct of states in the aftermath of the discovery of espionage are few'.[1672] Yoo pretends that 'the ICJ appears to be going out of its way to avoid creating *opinio juris* with respect to peacetime espionage'.[1673] Navarette refers to the 'long practice of espionage' and 'the existence of intelligence services, which have a legitimate and open state function'. However, he considers that this practice 'does not go along *opinio juris*'. Espionage is thus 'a political activity *par excellence*'.[1674] According to Chesterman, 'if the vast majority of states both decry it and practice it, state practice and *opinio juris* appear to run in opposite directions'.[1675]

Relying on both practice and *opinio juris* does not allow authors to reach a common conclusion on the legality of cyber-espionage. Some of them thus insist on the fact that practice supports the authorization of espionage.

[1669] Chantal Khalil, 'Thinking Intelligently about Intelligence: A Modal Global Framework protecting Privacy' (2015) 47 Geo.Wash.Int'l.L.Rev. 919, 922.

[1670] Ibid 934.

[1672] Leslie Edmondson, 'Espionage in Transnational Law' (1971-2) 5 Vanderbilt J.Transnatl.L. 434, 445. See also John Radsan, 'The Unresolved Equation of Espionage and International Law' (2007) 28 Mich.J.Int'l.L. 595, 597.

[1673] Christopher Yoo, 'Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures' (2015) University of Pennsylvania Law, Public Law Research Paper No.15-2, 24
<https://ssrn.com/abstract=2596634> accessed:10.10.2016.

[1674] Navarette (n.708) 15-16.

[1675] Chesterman (n.566) 1072.

1.2. Arguments based on practice to support the authorization of espionage

Many authors essentially rely on practice to reveal that 'everyone does it', thus neutralizing a prohibition of espionage in CIL. Lotrionte affirms that 'despite the occasional outcries for its cessation, states have long engaged in espionage and acknowledged it as a matter of practical reality. Arguably, the long history of espionage by states has given its practice the appearance of lawful activity'.[1676] According to Deeks, 'the widespread and long-standing practice of spying–committed by many states in different regions of the world during time periods that both precede and post-date the UN Charter–undercuts arguments that these customary principles either were intended to prohibit espionage at the time they developed or should be deemed to do so today'.[1677] Williams similarly thinks that '[t]he lack of clarity in treaties and customary norms, combined with a proliferation of state practice, favors the conclusion that international law does not prohibit intelligence collection in the territory of other states'.[1678] As Scott reveals, '[t]he United States is not a party to any treaty or agreement that prohibits surreptitious, non-destructive intelligence collection', and it 'does not violate customary international law'.[1679] 'In fact, customary international law has evolved such that spying has become the long-standing practice of nations. Indeed, while the surreptitious penetration of another nation's territory to collect intelligence in peacetime potentially conflicts with the customary principle of territorial integrity, international law does not specifically prohibit espionage'.[1680] Sharp refers to various means of technical intelligence and affirms that '[c]ustomary international law [...] has long recognized the lawfulness of the use of information in CyberSpace'.[1681] Indeed, 'CyberSpace infrastructures such as

[1676] Lotrionte (n.797) 474.

[1677] Deeks (n.1421) 305.

[1678] Williams (n.572) 1177.

[1679] Scott (n.787) 217.

[1680] Ibid.

[1681] Sharp (n.598) 124.

computers, telecommunication systems, and satellites have been used for intelligence collection since their invention'.[1682]

Focusing on practice enables these authors to support the authorization of espionage. However, studying its counterpart–*opinio juris*–actually allows others to reach the opposite conclusion.

1.3. Arguments based on *opinio juris* to support the prohibition of espionage

According to Shull, 'there is no evidence of *opinio juris* surrounding the conduct of the states that engage in acts of economic cyber-espionage or in the actions of the states that are victim'.[1683] Indeed, '[t]here has never been a public case of a state seeking to justify acts of cyber-espionage as something that is defensible pursuant to international law', and '[s]tates do not feel compelled as a matter of legal obligation to engage in these acts, nor do states feel compelled to remain silent or acquiesce when they fall victim'.[1684] Such position is allegedly reinforced by the fact that '[w]hen these activities are exposed, states are careful to distance themselves from the conduct'.[1685] He finally concludes that '[a]ll of this creates a unique legal position for economic cyber-espionage: it is implicitly prohibited under customary international law, with a normative push to make it explicitly prohibited, all while states use municipal law to prohibit the conduct domestically and transnationally'.[1686]

Doctrine does not reach a consensus regarding the status of cyber-espionage in CIL. However, applying the ILC draft conclusions demonstrates that there are no customary rules on cyber-espionage.

[1682] Ibid 125.

[1683] Shull (n.828) 14-15.

[1684] Ibid.

[1685] Ibid 18.

[1686] Ibid.

2. Status of law

In the introduction, it is demonstrated that two elements have to coexist to ascertain the existence of a new customary rule. The present study thus alternatively analyses state practice (2.1.) and *opinio juris* (2.2.).

2.1. Practice

The ILC made clear that 'legislative acts' (A), 'executive conducts' (B) and 'decisions of national courts' (C) had to be considered as components of practice. These elements, when related to espionage, are thus alternatively analysed.

A. Legislative acts

Two sets of legislative acts have to be analysed, and reveal a first paradox. Criminal laws indeed all prohibit 'espionage' (a), while national security laws authorize 'intelligence activities' (b). The grounds allowing such intelligence collection then have to be reviewed (c).

a. Criminal law prohibiting espionage

Nearly every state tends to prohibit espionage, whether in Europe (i), Asia (ii), Africa (iii), America (iv), or Oceania (v).

i. Europe

Collecting information on behalf of a foreign power, company or organisation, when its divulgation could harm the nation's basic interests, is prohibited by the

French *code pénal* (CP).[1687] Preparatory acts[1688] and its effective transmission are similarly prohibited.[1689]

'Crown servants' or 'government contractors' commit an offense when disclosing any information related to 'defence',[1690] or 'international relations'.[1691] Disclosing information related to 'security or intelligence' is also prohibited for them and the members of the British Secret Intelligence Service (SIS).[1692]

The transmission of information classified in the interest of the Netherlands and its allies,[1693] or originating from a restricted area and relevant to their security is prohibited by the *Wetboek van Strafrecht* (WvS).[1694] Transmitting any object or data from which such information may be derived is similarly prohibited.[1695] Sentences are harsher if the information is delivered to a foreign power, a person or organization based in a foreign country,[1696] and *a fortiori* in wartime.[1697]

The transmission of a state secret to a foreign power or foreign organisation,[1698] its divulgation–with the intent to prejudice Austria,[1699] or not[1700]–and spying on state secrets[1701] are considered as high treason in Austria.

[1687] CP (France) art.411-7.

[1688] Ibid arts.411-7, 411-8.

[1689] Ibid art.411-6.

[1690] Official Secrets Act 1989 (OSA 1989) s2.

[1691] Ibid s3.

[1692] Ibid s1(1)-(3).

[1693] WvS (Netherlands) art.98(1).

[1694] Ibid art.98(2).

[1695] Ibid art.98(1).

[1696] Ibid art.98(a)(1).

[1697] Ibid art.98(a)(2).

[1698] Strafgesetzbuch (Austria) §251(1).

[1699] Ibid §252(2).

[1700] Ibid §253.

[1701] Ibid §254.

The German definition of treason includes communicating state secrets to a foreign power or its intermediaries,[1702] and its divulgation to an unauthorized person or to the public, when done to prejudice Germany or to benefit a foreign power.[1703] Disclosing an element which is not a state secret, but could endanger the external security of Germany is punished as treason.[1704] Spying consists in obtaining a state secret,[1705] and doing so with the intent to disclose it is treasonous espionage.[1706] Revealing a state secret to the public is also forbidden.[1707] An agent of a foreign power who attempts to obtain state secrets,[1708] or someone who demonstrate an interest in doing so, commits an offence.[1709] Extraterritorial criminal jurisdiction exists for any of these offences, and for violation of trade and business secrets, when the company has its seat in Germany or depends on a company having its seat in Germany.[1710]

Revealing a secret, at the expense of Switzerland's interest, to a foreign power or an agent is diplomatic treason.[1711] Diplomatic treason also includes the intentional revelation of such secret to the public[1712] and negligent divulgation.[1713] The attempt and effective divulgation of trade and business secrets to public and private organization, a foreign company or their agents amounts to economic espionage.[1714] Gathering military[1715] or political

---

[1702] Strafgesetzbuch (Germany) §94(1) 1.

[1703] Ibid §94(1) 2.

[1704] Ibid §97a.

[1705] Ibid §96(1)

[1706] Ibid §96(2)

[1707] Ibid §97.

[1708] Ibid §98(1) 1.

[1709] Ibid §98(1) 2.

[1710] Ibid §5.

[1711] CP (Switzerland) art.267(1).

[1712] Ibid art.267(2).

[1713] Ibid art.267(3).

[1714] Ibid art.273.

[1715] Ibid art.274.

intelligence,[1716] and organizing such activities in the interest of a foreign power, to Switzerland's prejudice, are prohibited.

Communicating any object, plan, writing, document and intelligence linked to the territory defence or State safety to the enemy,[1717] or any foreign power,[1718] is prohibited in Belgium. It is similarly forbidden if detrimental to an ally.[1719]

Spanish citizens[1720] and residents[1721] are traitors if they obtain or reveal, to the prejudice of Spain's national security or national defence, classified information, to favour a foreign power, association or organization. The acquisition and revelation of secrets linked to national defence, in absence of a foreign power's involvement remains prohibited.[1722]

Treason,[1723] espionage,[1724] and disclosure of state secrets,[1725] are punished in Russia and Estonia.

Acts of espionage detrimental to the security is prohibited by all these States. Curiously, only Switzerland expressly prohibits acts of economic espionage on behalf of a foreign power, and none of them openly refer to state-sponsored cyber-espionage. Most of these legislations still prevent employees or managers from disclosing their own company's trade and business secrets,[1726] and their acquisition by an external element.[1727] Most of them also refer to cyber-

---

[1716] Ibid art.272.

[1717] CP (Belgium) art.116.

[1718] Ibid art.118.

[1719] Ibid art.117.

[1720] CP (Spain) art.584.

[1721] Ibid art.586.

[1722] Ibid arts.598-603.

[1723] Penal code (PC) (Russia) art.275; PC (Estonia) [232]

[1724] PC (Russia) art.276; PC (Estonia) [234].

[1725] PC (Russia) art.283; PC (Estonia) [241].

[1726] See: CP (Belgium) art.309; PC (Estonia) [377]; WvS (Netherlands) art.273(1)(1).

[1727] See: CP (Spain) art.278.

intrusions,[1728] as should be the case for the forty-six European parties to the Convention on Cybercrime.

As to older practice, espionage was still prohibited in Croatia in 2003,[1729] in Montenegro in 2004,[1730] in Serbia in 2005,[1731] in the Czech Republic,[1732] Hungary,[1733] and Moldova in 2009,[1734] in Bosnia-and-Herzegovina in 2010,[1735] and in Latvia in 2015.[1736] At the same time, Croatia,[1737] Hungary,[1738] and Montenegro,[1739] had forbidden intrusions in computer-systems.

ii. Asia

It is a criminal offence in China to join an espionage organization or to accept a spying mission.[1740] 'Whoever steals, secretly gathers, purchases, or illegally provides state secrets or intelligence for an organization, institution, or personnel outside the country' is to be put on trial.[1741]

[1728] See: CP (France) art.323-1; Strafgesetzbuch (Germany) §202(a), 204; CP (Luxembourg) art.509-1; WvS (Netherlands) arts 138ab, 273(1)-(2); Criminal Code (CC) (Russia) art.272; CP (Switzerland) arts.143-143bis; Computer Misuse Act 1990, ss1-2.

[1729] CC (Croatia) arts.146, 295.

[1730] CC (Montenegro) art.368.

[1731] CC (Serbia) art.315.

[1732] CC (Czech Republic) s316.

[1733] CC (Hungary) ss261-262.

[1734] CC (Moldova) art.338.

[1735] CC (Bosnia-and-Herzegovina) art.163.

[1736] CC (Latvia) s85.

[1737] CC (Croatia) art.223.

[1738] CC (Hungary) s422.

[1739] CC (Montenegro) art.353.

[1740] Criminal Law of the People's Republic of China, art.110.

[1741] Ibid art.111.

Acting 'as a spy for an enemy country' or helping a spy,[1742] divulgating military,[1743] and diplomatic secrets,[1744] are forbidden in South Korea.

'[A]ny person for any purpose prejudicial to the safety or interests of Singapore' commits spying if approaching or entering a prohibited place,[1745] collecting intelligence and official secrets that could be useful to a foreign power or an enemy.[1746]

Trespassing on restricted areas is qualified as espionage in the Philippines, if done with the intent to obtain intelligence.[1747] Disclosing intelligence linked to these areas is also qualified as spying.[1748]

India similarly prohibits trespassing on restricted areas,[1749] and considers as spying the production and collection of intelligence that could be useful to the enemy.[1750]

Turkey punishes the following actions, with harsher penalties when committed in wartime: stealing or using documents related to public security,[1751] political or military spying,[1752] disclosure of information related to public security and political interests of the State,[1753] disclosure of confidential information,[1754] trespass upon military zone,[1755] exploitation of governmental secrets and

---

[1742] Criminal Act (South Korea) art.98(1).

[1743] Ibid art.98(2).

[1744] Ibid art.113.

[1745] Official Secrets Act (Singapore) art.3(1)(a).

[1746] Ibid arts.3(1)(b)-(c).

[1747] PC (Philippines) art.117(1)

[1748] Ibid art.117(2).

[1749] Official Secrets Act 1923, s3(1)(a).

[1750] Ibid s3(1)(b)-(c).

[1751] CC (Turkey) art.324.

[1752] Ibid art.325.

[1753] Ibid art.326.

[1754] Ibid art.327.

[1755] ibid art.329.

disloyalty in Government services,[1756] access to restricted information,[1757] disclosure of restricted information,[1758] including for political or military spying purposes,[1759] and holding documents relating to public security.[1760] International spying–i.e., 'to serve the interests of another foreign country with the intention of spying on political and military affairs'[1761]–and access to restricted information for spying purposes are also prohibited.[1762]

As to older practice, espionage was still prohibited by Israel in 1977,[1763] Thailand in 2003,[1764] and Malaysia in 2015.[1765] Espionage and treason were still prohibited by Azerbaijan[1766] and Tajikistan in 2000,[1767] as well as Kazakhstan in 2014.[1768]

As in Europe, some states prevent the acquisition of trade secrets by external elements to the firm, such as South Korea,[1769] and Thailand.[1770] Specific provisions regarding intrusions in computer-systems also exist in China,[1771]

[1756] Ibid art.330.

[1757] Ibid art.331.

[1758] Ibid art.333.

[1759] Ibid art.334.

[1760] Ibid art.336.

[1761] Ibid art.328.

[1762] Ibid art.332.

[1763] Israel Penal Law 5937/1977, arts.111-114.

[1764] PC (Thailand) art.122(3).

[1765] PC (Malaysia) arts.124M-N.

[1766] CC (Azerbaijan) arts.274, 276.

[1767] CC (Tajikistan) arts 305, 308.

[1768] PC (Kazakhstan) arts 175-176.

[1769] Unfair Competition Prevention and Trade Secret Protection Act 1961, art.10-14.

[1770] Trade Secrets Act (No.2) BE 2558 (2015).

[1771] Criminal Law of the PRC, art.285.

Malaysia,[1772] the Philippines,[1773] Singapore,[1774] South Korea,[1775] Thailand,[1776] and Turkey.[1777] They also used to be prohibited in Kazakhstan[1778] and Tajikistan.[1779]

iii. Africa

The acquisition [1780] and transmission [1781] of official information, as well as trespassing on restricted areas are prohibited in Nigeria.[1782]

Wartime espionage is prohibited in Kenya.[1783]

Anyone who delivers intelligence to foreign states or organizations hostile to Eritrea is a spy, if he/she knows that these elements should be kept secret and may be used to the prejudice of the country's interests.[1784] Participating and assisting a political, diplomatic, military or economic foreign intelligence service or an organization hostile to Eritrea is a similar offence,[1785] as well as being formally recruited by them.[1786] The offence is aggravated espionage if committed in wartime.[1787]

[1772] Computer Crimes Act 1997.

[1773] Cybercrime Prevention Act of 2012, ss4(a)(1)-(2).

[1774] Computer Misuse and Cybersecurity Act (1993) ss3-6.

[1775] The Act on Promotion of Information and Communications Network Utilization and Data Protection, Etc (16.01.2001) No.6330, s49.

[1776] Computer Crime Act 2017 (No.2) BE 2560.

[1777] CC (Turkey) art.243.

[1778] PC (Kazakhstan) art.205.

[1779] CC (Tajikistan) arts.298, 301.

[1780] Official Secrets Act (Nigeria) s1(1)(b).

[1781] Ibid s1(1)(a).

[1782] Ibid s2.

[1783] Kenya Defence Forces Act 2012, s60.

[1784] CC (Eritrea) art.114(1)(a).

[1785] Ibid art.114(1)(b).

[1786] Ibid art.114(2).

[1787] Ibid art.115.

The acquisition[1788] and transmission[1789] of intelligence kept secret in the interest of national defence or economy is an offence in Algeria. It is called treason when committed by an Algerian citizen, and espionage when committed by a foreigner.[1790]
The acquisition[1791] and transmission[1792] of intelligence kept secret in the interest of national defence is also prohibited in Chad. The distinction between treason and espionage, depending on the citizenship of the offender, is maintained.[1793]
Treason and espionage are also prohibited in Cameroon.[1794]

As to older practice, espionage and treason were prohibited by Comoros in 1995,[1795] Burkina Faso in 1996,[1796] Ethiopia,[1797] and the DRC in 2004,[1798] Tunisia in 2005,[1799] Burundi in 2009,[1800] the Central African Republic in 2010,[1801] Morocco in 2011.[1802] At the same time, intrusions in computer-systems were

---

[1788] CP (Algeria) art.63(2).

[1789] Ibid art.63(1).

[1790] Ibid art.64.

[1791] CP (Chad) art.87(b).

[1792] Ibid art.87(a).

[1793] Ibid art.88.

[1794] CP (Cameroon) art.103.

[1795] CP (Comoros) arts.57-58.

[1796] CP (Burkina Faso) arts.90-91.

[1797] CC (Ethiopia) art.252.

[1798] CP (DRC) arts.184-185.

[1799] CP (Tunisia) arts.60bis-ter.

[1800] CP (Burundi) arts.571-572.

[1801] CP (Central African Republic) arts 267(1), 270-271.

[1802] CP (Morocco) art.181(4), 185.

forbidden by Tunisia,[1803] and Morocco.[1804] Such provisions now exist in Chad,[1805] and Nigeria,[1806] while 'computer related espionage and unlawful access to restricted data' are now prohibited in South Africa.[1807] Following the ECOWAS directive on Fighting Cyber Crime and its reference to 'fraudulent access to computer systems',[1808] it is likely that many African states will prohibit this activity in their criminal legislation.

iv. America

The Argentinean *Código Penal* (CP) prohibits the disclosure of secrets obtained at work,[1809] the violation of confidential systems and data banks.[1810] It is also prohibited for a civil servant to reveal secret facts, conducts, documents or data.[1811] The revelation of political, industrial, technological and military secrets, regarding the security, defence capacity or external relations of Argentina is similarly prohibited.[1812]

The Chilean CP punishes the disclosure of military secrets,[1813] while cyber-attacks and cyber-spying are offences under ley 19.223.[1814]

Military and political espionage are forbidden in Bolivia.[1815]

[1803] CP (Tunisia) art.199.

[1804] CP (Morocco) arts.607(3)-(4).

[1805] CP (Chad) arts.429-430.

[1806] Computer Security and Critical Information Infrastructure Protection Bill 2005, s3.

[1807] Cybercrimes and Cybersecurity Bill (2015) s16.

[1808] Directive C/DIR. 1/08/11 On Fighting Cyber Crime Within ECOWAS (19.08.2011), art.5.

[1809] CP (Argentina) art.156.

[1810] Ibid art.157bis.

[1811] Ibid art.157.

[1812] Ibid art.222.

[1813] CP (Chile) art.109.

[1814] Ley 19.223, arts.1-4.

[1815] CP (Bolivia) art.111.

Ecuador describes as espionage numerous actions of civil servants, soldiers and agents of intelligence services. Some of them deal with information whose use could prejudice the security or sovereignty of the state: seeking to obtain them, when classified,[1816] sending,[1817] or altering them are forbidden.[1818] Obtaining[1819] or hiding[1820] military and political information is also prohibited.

Spying[1821] or disclosing[1822] information linked to national defence is forbidden in Peru.

Obtaining or disclosing political, economic or military secrets, related to the security of the state, are offences in Colombia.[1823]

Various forms of spying are included in Mexican legislation: when a foreigner supplies documents or data about military activities (the sentence is harsher in wartime),[1824] and when a Mexican citizen reveals confidential information to another country, if detrimental to Mexico.[1825]

Treason is sanctioned in Paraguay[1826] and Uruguay.[1827]

[1816] CP (Ecuador) art.354(1).

[1817] Ibid art.354(3).

[1818] Ibid art.354(5).

[1819] Ibid art.354(2).

[1820] Ibid art.354(4).

[1821] CP (Peru) art.331.

[1822] Ibid art.331(A).

[1823] CP (Colombia) art.463.

[1824] CP (Mexico) art.127.

[1825] Ibid art.128.

[1826] CP (Paraguay) art.282.

[1827] CP (Uruguay) art.132(3).

Specific provisions prohibiting intrusions in computer-systems exist in Argentina, [1828] Bolivia, [1829] Colombia, [1830] Ecuador, [1831] Mexico, [1832] and Venezuela.[1833]

Obtaining information 'respecting the national defense', and 'with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation' is forbidden.[1834] Trying to obtain such information 'from any person' is also an offence.[1835] Transmitting it is also prohibited, regardless of whether the person is in their 'lawful'[1836] or 'unauthorized' possession.[1837] Gathering and transmitting defence information, 'with intent or reason to believe that the information is to be used to the injury of the United States or to the advantage of any foreign nation, or to any faction or party or military or naval force within a foreign country', as well as to any individual, is prohibited.[1838] Sentences are harsher in wartime.[1839] Disclosure by negligence is also punished. [1840] Communicating other types of classified information 'to an unauthorized persons', or using them 'in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States' are offences.[1841] Committing economic espionage, when 'intending or knowing that the offense

---

[1828] CP (Argentina) art.153.

[1829] CP (Bolivia) art.363(ter).

[1830] CP (Colombia) arts.269A, 269C.

[1831] CP (Ecuador) art.190.

[1832] CP (Mexico) art.211bis (1).

[1833] Ley Especial contra los Delitos Informaticos (30.10.2001) GO 37.313, arts.6-12.

[1834] 18 USC §793(a).

[1835] Ibid §793(c).

[1836] Ibid §793(d).

[1837] Ibid §793(e).

[1838] Ibid §794(a).

[1839] Ibid §794(b).

[1840] Ibid §793(f).

[1841] Ibid §798.

will benefit any foreign government, foreign instrumentality, or foreign agent', infringes American law.[1842] Theft of trade secret is also prohibited.[1843]

v. Oceania

Four forms of spying are mentioned by the Australian Criminal Code Act. All of them concern 'information concerning the Commonwealth's security or defence', or 'information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth'. The first form is when a person communicates–or makes available–such information.[1844] Additional conditions are that 'the person does so intending to prejudice the Commonwealth's security or defence',[1845] and the act 'results in, or is likely to result in, the information being communicated or made available to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation'.[1846] A second form is when a person transmits the same information,[1847] with the same possible result,[1848] when done 'without lawful authority'[1849] and 'intending to give an advantage to another country's security or defence'.[1850] A third form is when a person 'makes, obtains or copies a record (in any form)' of such information,[1851] intending 'that the record will, or may, be delivered to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation'[1852] or to 'prejudice

---

[1842] Ibid §1831.

[1843] Ibid §1832.

[1844] Criminal Code Act 1995, s91.1(1)(a).

[1845] Ibid s91.1(1)(b).

[1846] Ibid s91.1(1)(c).

[1847] Ibid s91.1(2)(a).

[1848] Ibid s91.1(2)(c).

[1849] Ibid s91.1(2)(b)(i).

[1850] Ibid s91.1(2)(b)(ii).

[1851] Ibid s91.1(3)(a).

the Commonwealth's security or defence'.[1853] The fourth form is similar to the third one, but the person does so 'without lawful authority',[1854] 'intending that the record will, or may, be delivered to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation'[1855] and 'intending to give an advantage to another country's security or defence'.[1856]
Collecting[1857] and transmitting[1858] information 'to a country or organisation outside New Zealand or to a person acting on behalf of any such country or organisation' is an offence, when carried out by 'a person who owes allegiance to the Sovereign in right of New Zealand, within or outside New Zealand' and does so 'with intent to prejudice the security or defence of New Zealand'.
The disclosure of secrets related to defences by public officers,[1859] obtaining such disclosure,[1860] and the disclosure of other state secrets[1861] are prohibited by the criminal code of Papua New Guinea.

It results from this analysis that a majority of states tend to prohibit acts of foreign espionage directed against them. However, they also arrogate the right to carry out 'intelligence activities' on their counterparts.

[1852] Ibid s91.1(3)(b)(i).

[1853] Ibid s91.1(3)(b)(ii).

[1854] Ibid s91.1(4)(b)(i).

[1855] Ibid s91.1(4)(b)(ii).

[1856] Ibid s91.1(4)(b)(iii).

[1857] Crimes Act 1961, s78(b).

[1858] Ibid s78(a).

[1859] CC (Papua New-Guinea) s84.

[1860] Ibid s85.

[1861] Ibid s86.

b. National security law authorizing intelligence activities

Many legislations authorize the state to conduct intelligence activities, more or less obviously. Direct reference (i), indirect reference (ii), as well as ambiguous and suspicious provisions (iii) may be found in domestic laws.

i. Direct reference

The Bosnian Intelligence-Security Agency (OSA-OBA) is 'responsible for gathering intelligence both within and outside Bosnia-and-Herzegovina regarding threats to the security'.[1862]

The CSIS may 'perform its duties and functions […] within or outside Canada'.[1863]

The French intelligence services' mission is 'in France and abroad, to search, collect, harness and provide the Government with intelligence related to geopolitical and strategic issues, as well as threats and risks that could affect nation's life. They help knowing and anticipate these issues, as well as prevent and impede these risks and threats'.[1864]

In Georgia, '[t]he Service shall exercise its authority abroad, as well as in the entire territory of Georgia […]'.[1865]

Greek 'Regional Units shall comprise services, bodies and liaisons established or placed in various areas of Greece or abroad and shall perform their duties within a determined region'.[1866]

The Italian External Intelligence and Security Agency (AISE) 'shall also be responsible for identifying and countering outside national territory those espionage activities that are directed against Italy and those activities that are

---

[1862] Law on the Intelligence and Security Agency (2004) art.5.

[1863] CSIS Act, s12(2).

[1864] Code de sécurité intérieure, art.L811-2.

[1865] Law of Georgia on the Georgian Intelligence Service (27.04.2010) No.2984-RS, art.6(4).

[1866] Law No.3649, art.3(3).

aimed at damaging national interests'.[1867] Another reference is made in the provisions about security classification, as it 'shall be applied […] by the authority who […] acquires documents, records, information or things from abroad'.[1868]

In Kazakhstan, the 'competence of subjects of foreign intelligence shall include […] carrying out of intelligence activity in the territory of the Republic of Kazakhstan and beyond its borders'.[1869]

Kenyan services may 'obtain […] intelligence about the activities of foreign interference and capabilities, intentions or activities of people or organizations outside Kenya'.[1870] They may also 'investigate, gather, collate, correlate, evaluate, interpret, disseminate and store information which is relevant in the performance of its functions, under this Act, whether within or outside Kenya'.[1871]

The Director-General of Papuan National Intelligence Organization (NIO) 'shall authorize the Organization to collect intelligence information outside the country by overt means only'.[1872] But if he receives written authority from the PM for a particular matter, 'he may authorize the Organization to collect intelligence information outside the country by other than overt means'.[1873]

The functions of the Spanish National Intelligence Centre (CNI) include obtaining, evaluating and interpreting information to protect Spanish political, economic, industrial, commercial and strategic interest of Spain, 'in and outside the national territory'.[1874]

[1867] Law 124/2007 s6(3).

[1868] Ibid s42(2).

[1869] The Law of the Republic of Kazakhstan On Foreign Intelligence ('Law 277-IV') (22.05.2010) No.277-IV, art.8(2).

[1870] National Intelligence Service Act 2012, s5(1)(n).

[1871] Ibid s6(2)(a).

[1872] NIO Act, s12(1).

[1873] Ibid s12(2).

[1874] Ley reguladora del Centro Nacional de Inteligencia ('Ley 11/2002') (06.05.2002) No.11/2002, BOE-A-2002-8628, art.4(a).

Some states have more precise provisions regarding cyber-espionage and interceptions of communication. The Belgian General Intelligence and Security Service (SGRS) is entitled to 'research, capture, listen to, take note and record any form of communication emitted from or received abroad'.[1875] This includes the possibility, for the SGRS, 'to intrude in a computer-system located abroad, to circumvent any protection, to set-up technical devices to decrypt, decipher and manipulate data stored, processed or transmitted by the system, and to neutralise it'.[1876] Filming and photographing abroad is similarly authorized.[1877] The decision is taken by the Ministry of Defence, upon a proposal of the SGRS.[1878]

The Canadian Excerpt from the National Defence Act establishes the mandate of the CSEC, which 'is to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence […]'.[1879] Moreover, the CSEC may be authorized by the Minister to 'intercept private communications',[1880] but only if 'the interception will be directed at foreign entities located outside Canada [...]'.[1881] As to the CSIS, 'the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing'.[1882] Under such warrant, 'a judge may […] authorize activities outside Canada to enable the Service to investigate a threat to the security of Canada'.[1883] An instance of Federal Court ruling was previously analysed.[1884]

[1875] L.R&S art.44.

[1876] Ibid art.44/1.

[1877] Ibid art.44/2.

[1878] Ibid art.44bis.

[1879] Excerpt from the National Defence Act, s273.64(1)(a).

[1880] Ibid s273.65(1).

[1881] Ibid s273.65(2)(a).

[1882] CSIS Act s21(3).

[1883] Ibid s21(3.1).

[1884] See Chapter I-II.

French intelligence services are authorized to carry out communication surveillance, when initiating from or received abroad, including correspondence and connection data.[1885] If someone has a link with the French territory–such as subscription numbers or technical identifiers–communications cannot be intercepted except if the interceptions had already been authorized when he/she quit the French territory or if he/she is a threat to the nation's fundamental interest.[1886]

Dutch services 'are authorised, with the aid of a technical device, to tap, receive, record and monitor in a directed way any form of conversation, telecommunication or data transfer by means of an automated work, irrespective of where this takes place'.[1887] They are also authorised, 'with the aid of a technical device, to receive and record non-cable-bound telecommunication originating from or intended for other countries, on the basis of a technical characteristic to monitor the communication'.[1888] It has the 'power to undo the encryption of the conversations, telecommunication or data transfer' for the first activity,[1889] and to decrypt telecommunications for the second one.[1890] The AIVD also mentions that it 'is responsible for national security by timely identifying threats and risks that are not immediately visible. For this purpose the AIVD conducts investigations both within and outside the Netherlands'.[1891]

'When computer networks and systems located abroad are used to attack critical infrastructures in Switzerland, the SRC [Federal Intelligence Service] can infiltrate them in order to hinder, prevent or slowdown the access to information'. [1892] Moreover, the 'SRC may infiltrate computer networks and systems to collect information that are contained or have been transmitted by

---

[1885] Code de Sécurité intérieure, article L854-1.

[1886] Ibid.

[1887] Intelligence and Security Services Act 2002, art.25(1).

[1888] Ibid art.26(1).

[1889] Ibid art.25(1).

[1890] Ibid art.26(1).

[1891] AIVD, 'Annual Report 2006' (2007) 1 <https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2007/06/20/annual-report-2006/20070872jv2006-en.pdf> accessed:13.02.2017.

[1892] LRens, art.37(1).

them'.[1893] Finally, 'Switzerland can have a recording service of electromagnetic waves transmitted by telecommunication systems located abroad'.[1894] The SRC may also plug into the cables that cross the border.[1895]

The German G10 mentions that the secret of international telecommunications may be limited, when a person located abroad could be injured or killed,[1896] in the event of a risk of attack against Germany or to fight organised crime.[1897]

In New Zealand, '[i]t is a function of an intelligence and security agency to [...] collect and analyse intelligence in accordance with the New Zealand Government's priorities'.[1898] Two types of intelligence warrant are defined.[1899] Type 1 authorizes the NZSIS and the Government Communications Security Bureau (GCSB) 'to carry out an otherwise unlawful activity for the purpose of collecting information about, or to do any other thing directly in relation to [...] any person who is' or 'a class of persons that includes a person who is' a 'New Zealand citizen' or 'a permanent resident of New Zealand'.[1900] Type 2 authorizes agencies 'to carry out an otherwise unlawful activity for the purpose of collecting information, or to do any other thing, in circumstances where a Type 1 warrant is not required'.[1901] '[T]o give effect to the intelligence warrant', the GCSB may be authorized to 'access an information infrastructure, or a class of information infrastructures'.[1902] This includes 'instructing, communicating with, storing data in, retrieving data from, or otherwise making use of the resources or features of the infrastructure',[1903] as well as 'making photographs, videos, and sound

---

[1893] Ibid art.37(2).

[1894] Ibid art.38(1)

[1895] Ibid art.39(1).

[1896] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ('Artikel 10-Gesetz–G 10') (26.06.2001) BGBl. I S. 1254, 229, §8(1).

[1897] Ibid §5.

[1898] Intelligence and Security Act 2017, s10(1)(a).

[1899] Ibid s52(a).

[1900] Ibid s53.

[1901] Ibid s54.

[1902] Ibid s69(1)(a).

recordings, or using the infrastructure or any part of it'.[1904] It may also be authorized to 'install, use, maintain, or remove' device for 'visual surveillance',[1905] 'interception',[1906] as well as 'extract and use, in the course of carrying out activities allowed by the warrant, any electricity from a place or thing'.[1907] It may also do reasonable acts to keep these activities covert.[1908] Some information of New Zealand citizens or permanent residents are called 'privileged communication' or 'privileged information' and may not be obtained. They are related to 'communications or information protected by legal professional privilege or privileged in proceedings [...]'.[1909]

In the UK, the RIPA gives some modalities about the 'interception of external communications'.[1910] The latter are defined as 'a communication sent or received outside the British Islands',[1911] and they 'include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in the course of their transmission', but they 'do not include communications both sent and received in the British Islands, even if they pass outside the British Islands *en route*'.[1912] Moreover, 'bulk interception warrants' aimed at 'the interception of overseas-related communications'[1913] or 'the obtaining of secondary data from such communications'[1914] may be delivered

---

[1903] Ibid s69(3)(a).

[1904] Ibid s69(3)(b).

[1905] Ibid s69(1)(b).

[1906] ISA Act, s69(1)(c).

[1907] Ibid, s69(1)(d).

[1908] Ibid s69(1)(f).

[1909] Ibid s70.

[1910] Regulation of Investigatory Powers Act 2000 ('RIPA') ss8(4)-(5).

[1911] Ibid s20.

[1912] UK Government, 'Interception of Communications Code of Practice' (2015) [6.5] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf> accessed:14.02.2016.

[1913] Investigatory Powers Act 2016 ('IPA') s136(2)(a).

[1914] Ibid s136(2)(b).

under the IPA. [1915] 'Overseas-related communications' are defined as 'communications sent by individuals who are outside the British Islands'[1916] or 'communications received by individuals who are outside the British Islands'.[1917] While Executive Order (EO) 12.333 is not a legislative act *per se*–but an executive conduct–it is worth mentioning it. The directors of the Central Intelligence Agency (CIA), Defence Intelligence Agency (DIA) and NSA are in charge of collecting 'foreign intelligence and counterintelligence', 'including through clandestine means'.[1918] More precisely, the director of the NSA shall '[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions'.[1919]

Some states are thus very explicit regarding their espionage activities. However, some others refer to them through indirect references.

ii. Indirect reference

Russia, Slovakia and Switzerland are entitled to protect the members of their intelligence services if they are caught while on duty abroad. Russia 'is bound to take all possible steps to assist in the unconditional release of any staffer on the staff of a Russian Federation foreign intelligence organ and members of his family detained, arrested, or sentenced outside Russian Federation territory in connection with the performance of intelligence gathering activity'.[1920] Similarly, the Slovak Intelligence Service 'shall be authorized to provide protection of Members who execute their rights and obligations in accordance with the Act

---

[1915] Ibid s136.

[1916] Ibid s136(3)(a).

[1917] Ibid s136(3)(b).

[1918] EO 12333, 'United States intelligence activities' ('EO 12333') (04.12.1981) 56 FR59941, ss1.7(a)-(c).

[1919] Ibid s1.7(c)(1). See also: 50 USC §1802.

[1920] Federal Law On Foreign Intelligence (08.12.1995) No.5, art.22.

by the fulfilment of the tasks of the Information Service on the territory of the Slovak Republic or abroad'.[1921] The Swiss SRC protects its collaborators on duty abroad.[1922]

In sum, these states leave little doubt regarding the fact they send spies abroad. At the opposite, others resort to ambiguous and suspicious provisions, thus leaving an aura of mystery.

iii. Ambiguous and suspicious provisions

A first manifestation of this ambiguity is when domestic legislations acknowledge that information is searched 'about abroad', 'outside' the country, 'in relation to foreign States', or 'on the internal and international level'.
The Croatian Security Intelligence Agency (SOA) 'collects, analyses, processes and assesses the political, economic, scientific/technological and security-related information concerning the foreign countries […]'.[1923]
In Australia, 'the functions of ASIS [Australian Secret Intelligence Service] are […] to obtain […] intelligence about the capabilities, intentions or activities of people or organisations outside Australia [...]'.[1924] Then, '[t]he functions of ASD [Australian Signals Directorate] are […] to obtain intelligence about the capabilities, intentions or activities of people or organisations outside Australia in the form of electromagnetic energy […].[1925]
Similarly, SIS' functions 'shall be […] to obtain and provide information relating to the actions or intentions of persons outside the British Islands'.[1926] Then, the Government Communications Headquarters (GCHQ) has 'to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment

---

[1921] The Act of the National Council of the Slovak Republic on the Slovak Information Service ('Act on the Slovak Information Service') (21.01.1993) No.46/1993, [13.a]

[1922] LRens, art.36(7).

[1923] Act on the Security Intelligence System of the Republic of Croatia (30.06.2006) art.23(2).

[1924] Intelligence Service Act (2001) s6(1)(a).

[1925] Ibid s7(a).

[1926] Intelligence Service Act, s1(1)(a).

producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material',[1927] and 'in the interests of national security',[1928] 'the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands',[1929] or 'in support of the prevention or detection of serious crime'.[1930]

The BND gathers information about foreign countries, which is of interest for its foreign and security policies.[1931]

Kenya relies on 'an external intelligence division which shall be responsible for gathering foreign intelligence'.[1932]

Slovakian 'Information Service shall collect, accumulate and analyse information on activities arising abroad which are directed against the constitutional establishment and security of the Slovak Republic and information necessary for the implementation of its interests concerning the foreign policy'.[1933]

'The duties of the Turkish National Intelligence Organization include […] to procure national security intelligence on immediate and potential activities carried out in or outside the country targeting the territorial and national integrity, existence, independence, security, Constitutional order and all elements that constitute the national strength of the Republic of Turkey […]'.[1934]

The Defence Intelligence Agency (DIA) is in charge of 'the prevention and detection of crime of a military nature against the security of Nigeria',[1935] 'the protection and preservation of all military classified matters concerning the

---

[1927] Ibid s3(1)(a).

[1928] Ibid s3(2)(a).

[1929] Ibid s3(2)(b).

[1930] Ibid s3(2)(c).

[1931] Gesetz über den Bundesnachrichtendienst ('BND-Gesetz BNDG') (20.12.1990) BGBl I S2954, 2979, §1(2).

[1932] National Intelligence Service Act 2012, s14(1)(b).

[1933] Act on the Slovak Information Service, §2(2).

[1934] The Law on the State Intelligence Services and the National Intelligence Organization ('Law 2937') (1.11.1983) No.2937, art.4(a).

[1935] National Security Agencies Act 1986, s2(1)(a).

security of Nigeria, both within and outside Nigeria',[1936] 'other responsibilities affecting defence intelligence of a military nature, both within and outside Nigeria'.[1937] The National Intelligence Agency (NIA) is in charge of 'the general maintenance of the security of Nigeria outside Nigeria, concerning matters that are not related to military issues',[1938] and 'such other responsibilities affecting national intelligence outside Nigeria'.[1939]

'The Norwegian Intelligence Service shall procure process and analyse information regarding Norwegian interests viewed in relation to foreign states, organizations or private individuals […]'.[1940] Its main task is 'to collect, assess and analyse information on foreign countries' political and social development, intentions and military forces, which may constitute a real or potential risk'.[1941] In peacetime, it has to 'produce intelligence that provides national authorities with a basis for making decisions on, and to prevent and handle, episodes, crises and war' and, in wartime, to 'produce intelligence which provide higher military and political authorities with a basis for handling an armed conflict in accordance with national objectives, support military intelligence requirements, and contribute to NATO's common defence'.[1942]

In Ghana, a co-ordinator is responsible for assisting 'the relevant Intelligence Agency to gather defence intelligence both internal and external and use the information to detect and prevent threats to the security of the State'.[1943]

The Chilean *Agencia Nacional de Inteligencia* (ANI)[1944] and the Paraguayan *Sistema Nacional de Inteligencia*[1945] are in charge of collecting and processing information

---

[1936] Ibid s2(1)(b).

[1937] Ibid s2(1)(c).

[1938] Ibid s2(2)(a).

[1939] Ibid s2(2)(b).

[1940] Act relating to the Norwegian Intelligence Service (20.03.1998) s3.

[1941] Instructions for the Intelligence Service (31.08.2001) §8.

[1942] Ibid.

[1943] Security and Intelligence Agencies Act, s19(d).

[1944] Ley Sobre el Sistema de Inteligencia del Estado y crea la Agencia Nacional de Inteligencia ('Ley 19974') (02.10.2004) No.19974, art.8(a).

on the national and international levels. The Peruvian *Dirección General de Asuntos de Seguridad y Defensa del Ministerio de Relaciones Exteriores* does so only on the international level.[1946]

A second manifestation of this ambiguity is when provisions prevent declassification of information if such revelation is to damage relationships with other countries. This is the case for Norway[1947] and the Netherlands.[1948]

By referring to the protection of secrets, citizens and operations outside the country, Russian legislation is even more suspicious. Firstly, '[i]n the process of intelligence gathering activity, the Russian Federation foreign intelligence organs can use overt and covert methods and means'.[1949] For such purpose, they 'are empowered to use information systems, video and audio recordings, moving and still photography, the downloading of information from technical communications channels [...]'.[1950] Further details are inaccessible, as '[t]he contents of normative legal acts on questions concerning the use of covert methods and means for intelligence gathering activity constitute a state secret'.[1951] Secondly, '[i]n order to attain the objectives of intelligence gathering activity', they 'are granted the following powers: [...] to organize and ensure within the limits of its powers the protection of state secrets in Russian Federation institutions located outside Russian Federation territory […] to ensure the security of Russian Federation citizens who are posted outside Russian Federation territory and, by virtue of the nature of their work, have

[1945] Ley Que crea el Sistema Nacional de Inteligencia (20.08.2014) No.5241, art.14(1).

[1946] Ley del Sistema de Inteligencia Nacional–SINA y de la Dirección Nacional de Inteligencia–DINI (14.12.2005) No.26664, NL 04.01.2006, 309260, art.11.

[1947] Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee), 'Annual Report 2015' (2015) 35.

[1948] Intelligence and Security Services Act 2002, art.34(7)(b).

[1949] Federal Law On Foreign Intelligence, art.13.

[1950] Ibid.

[1951] Ibid.

access to information constituting state secrets, as well as the security of members of their families who are accompanying them'.[1952]

Some of these states detail collection techniques, but without expressly mentioning that such instruments are to be used abroad.

The Chilean *Agencia Nacional de Inteligencia* (ANI) is part of the *Sistema de Inteligencia Nacional*.[1953] When open sources are insufficient to collect intelligence, the latter may resort to 'special processes'.[1954] They include the tapping of phone, computer and radio communications–as well as any form of correspondence[1955]– interfering with computer-systems and networks,[1956] electronic listening and recording,[1957] and bugging of any other technologic systems dedicated to the transmission, storage and processing of communication and information.[1958]

The Croatian law defines 'measures of secret information collection, which temporarily restrict certain constitutional human rights and basic freedoms',[1959] and may be used by the SOA. They 'may be applied if the information can not be obtained in any other way or the collection thereof is linked with disproportionate difficulties'.[1960] They include 'secret surveillance' of 'communication content', 'telecommunication traffic data (intercept related information)', 'the location of the user', and 'international telecommunications'.[1961] The law also mentions the possibility to carry out 'strategic electronic reconnaissance'.[1962]

[1952] Ibid art.6.

[1953] Ley 19974, art.5.

[1954] Ibid art.23.

[1955] Ibid art.24(a).

[1956] Ibid art.24(b).

[1957] Ibid art.24(c).

[1958] Ibid art.24(d).

[1959] Act on the Security Intelligence System of the Republic of Croatia, art.33(1).

[1960] Ibid art.33(2).

[1961] Ibid art.33(3).

[1962] Ibid art.57.

'In the fulfilment of its duties [...] the [Slovakian] Information Service shall be authorized to use special measures'.[1963] They include 'operational-intelligence'[1964] and 'technical-intelligence' measures.[1965]

This analysis reveals that states actually spy on each other, and are quite explicit about this. However, studying on what ground they feel entitled to spy is of equal interest, and could confirm or neutralize a dual regime distinguishing economic espionage or intelligence for security purposes.

c. Grounds allowing intelligence collection

Earlier in this thesis, it has been demonstrated that states perceive espionage as means to detect and counter threats.[1966] In many cases, intelligence collection is indeed connected to national security (i). However, it is not uncommon for intelligence services to be entitled to defend other types of interest, such as 'national' or 'economic' interests (ii).

i. National security

In Argentina, 'national intelligence' includes collecting information linked to events, threats, risks and conflicts that may affect the external and domestic security.[1967]
The OSA-OBA is responsible for 'gathering, analysing and disseminating intelligence in order to protect the security, including the sovereignty, territorial integrity and constitutional order'.[1968]

[1963] Act on the Slovak Information Service, §10(1).

[1964] Ibid §10(1)(a).

[1965] Ibid §10(1)(b).

[1966] See Chapter I-III.

[1967] Ley de Inteligencia Nacional, art.2(1)

[1968] Law on the Intelligence and Security Agency, art.1.

The CSIS shall 'collect', 'analyse' and 'retain information and intelligence respecting activities that may […] be suspected of constituting threats to the security of Canada'.[1969]

The Chilean ANI protects national sovereignty and constitutional order.[1970]

The BND shall collect information, which is of interest for German foreign and security policies.[1971]

The CISEN conducts intelligence operation that 'contribute to preserve the integrity, stability and permanence of Mexican state'.[1972] It helps reinforcing the 'governability' and 'the rule of law'.[1973]

The National Security Agency of Montenegro 'is responsible for the performance of national security activities aimed at the protection of the constitutional order, independence, sovereignty, territorial integrity and security of Montenegro, human rights and freedoms guaranteed by the Constitution, as well as other duties of interest for the national security of Montenegro'.[1974]

The Dutch AIVD conducts investigations on 'organizations' and 'persons' who–through their purpose or activities–'are a danger to the continued existence of the democratic legal system' or 'to the security or other vital interest of the state',[1975] and on 'other countries'.[1976] It also protects information relating to 'national security', 'public service', and 'business community' that 'are of vital importance for the existence of the social order'.[1977] The MIVD conducts investigation 'into the potential and the armed forces of other powers',[1978] and factors concerning the international legal system and involving armed forces.[1979]

[1969] CSIS Act, art.12(1).

[1970] Ley Num 19974, art.4.

[1971] BND-Gesetz, 1-2.

[1972] Ley de Seguridad Nacional, art.19.

[1973] Ibid.

[1974] Law on the National Security Agency, art.1.

[1975] Intelligence and Security Services Act 2002, art.6(2)(a).

[1976] Ibid art.6(2)(d).

[1977] Ibid art.6(2)(c).

[1978] Ibid art.7(2)(a)(1).

It prevents activities aimed at damaging the security and the readiness of the armed forces,[1980] and may investigate over foreign countries, for matters of military relevance.[1981]

The Intelligence Service Act establishes 'conditions so that the Norwegian Intelligence Service can contribute effectively to monitoring and counteracting external threats to the independence and security of the realm and other important national interests'.[1982]

'[T]o procure national security intelligence on immediate and potential activities carried out in or outside the country targeting the territorial and national integrity, existence, independence, security, Constitutional order and all elements that constitute the national strength […]' is among the duties of the Turkish National Intelligence Organisation.[1983]

In Nigeria, the DIA is in charge of preventing and detecting crime of a military nature against the security of Nigeria,[1984] and 'the protection and preservation of all military classified matters concerning the security of Nigeria, both within and outside Nigeria',[1985] while the NIA 'is in charge with the general maintenance of the security of Nigeria outside Nigeria, concerning matters that are not related to military issues'.[1986]

Eleven states thus exclusively resort to intelligence activities for the preservation of their national security. However, they form a minority.

1979 Ibid art.7(2)(a)(2).

1980 Ibid art.7(2)(c)(1).

1981 Ibid art.7(2)(e).

1982 Act relating to the Norwegian Intelligence Service, s1(a).

1983 Law 2937, art.4(a).

1984 National Security Agencies Act 1986, s2(1)(a).

1985 Ibid s2(1)(b).

1986 Ibid s2(2)(a).

.

ii. National or economic interest

ASIS' functions 'are to be performed only in the interests' of Australia's 'national security', 'foreign relations' or 'national economic well-being', and 'only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia'.[1987]

Belgian *Sûreté de l'Etat* shall collect, analyse and process intelligence related to any threat that could affect internal safety, democratic and constitutional order, external safety and international relations, scientific and economic potential or any other fundamental interest of Belgium.[1988] Its military counterpart–the SGRS–has to 'seek, analyse and process the intelligence linked to factors that could influence national and international security, to the extent that armed forces are or could be involved'.[1989] It is also responsible for intelligence activities related to any activity that could treat: 'the territorial integrity or population',[1990] the 'military defence plans',[1991] 'the economic and scientific potential',[1992] 'the fulfilment of armed forces' mission',[1993] 'the safety of Belgian citizens abroad',[1994] and 'any other interest defined by the King'.[1995]

French intelligence services gather information linked to the 'defence and promotion of the nation's basic interests'.[1996] The latter include France's 'national independence, territorial integrity and national defence',[1997] 'major interests in foreign affairs',[1998] 'compliance with European and International

---

[1987] Intelligence Services Act 2001, s11(1).

[1988] L.R&S, art.7(1).

[1989] Ibid art.11.

[1990] Ibid art.11(1)(a).

[1991] Ibid art.11(1)(b).

[1992] Ibid art.11(1)(c).

[1993] Ibid art.11(1)(d).

[1994] Ibid art.11(1)(e).

[1995] Ibid art.11(1)(f).

[1996] Code de la sécurité intérieure, art.L811-3.

[1997] Ibid art.L811-3(1).

obligations and the prevention of any foreign interference',[1999] its 'economic, industrial and scientific main interest',[2000] and the 'prevention of terrorism'.[2001] They also have to prevent 'threats to republican institutions',[2002] 'actions favouring the existence or reconstitution of disbanded groups',[2003] 'collective violence that could harm public peace',[2004] 'organized crime',[2005] and 'the proliferation of WMD'.[2006]

The functions of the Ghanaian Intelligence Agencies are to 'collect, analyses retain and disseminate […] information and intelligence respecting activities that may constitute threats to the security of the State and the government'.[2007] They should also 'safeguard the economic well-being of the State against threats posed by the acts or omissions of persons or organisations both inside and outside the country'.[2008] Then, they 'protect the State against threats of espionage, sabotage, terrorism, hijacking, piracy, drug trafficking and similar offences',[2009] as well as 'against the activities of persons, both nationals and non-nationals, intended to overthrow the government of Ghana or undermine the constitutional order through illegal political, military, industrial or other means or through any other unconstitutional method'.[2010]

The mission of the Greek EYP 'shall be to seek, collect, process and notify to competent authorities information' aiming at '[p]rotecting and promoting the

---

1998 Ibid art.L811-3(2).

1999 Ibid.

2000 Ibid art.L811-3(3).

2001 Ibid art.L811-3(4).

2002 Ibid art.L811-3(5)(a).

2003 Ibid art.L811-3(5)(b).

2004 Ibid art.L811-3(5)(c).

2005 Ibid art.L811-3(6).

2006 Ibid art.L811-3(7)

2007 The Security and Intelligence Agencies Act, s12(1)(a).

2008 Ibid s12(1)(b).

2009 Ibid s12(1)(c).

2010 Ibid s12(1)(d).

country's political, economic, military and overall national strategic interests',[2011] 'preventing and dealing with activities constituting threats against the democratic regime, the fundamental human rights, the territorial integrity and the national security', [2012] 'the country's national wealth', [2013] the 'activities of terrorist organizations and other organized crime groups'.[2014]

Italian AISE's functions 'shall be to gather and process all intelligence […] that serves to defend the independence, integrity and security of the Republic […] against threats originating abroad'. [2015] It is also responsible for counter-proliferation concerning strategic materials and security intelligence performed outside the national territory, to protect military, economic, scientific, industrial interests,[2016] as well as for 'identifying and countering outside national territory' espionage and other damaging activities directed against Italy.[2017]

The intelligence services of Kazakhstan should provide 'intelligence information and analytical assessments required for adoption of decisions in a policy, financial economic, military politic, scientific technical, humanitarian, environmental and other oblasts concerning the national interests'.[2018] Their tasks also include 'the acquisition of intelligence information and realization of measures oriented to inadmissibility of the real and potential harm to the national interests and security […] from the side of special services and organizations of the foreign states, terroristic and extremist organizations, criminal organizations, as well as separate persons'.[2019] Interestingly, they are also supposed to provide 'assistance to economic development and scientific technical progress of the country and military technical safety ensuring […]'.[2020]

[2011] Law No.3649, art.2(1)(a).

[2012] Ibid art.2(1)(b).

[2013] Ibid.

[2014] Ibid art.2(1)(c).

[2015] Law No.124/2007, s6(1).

[2016] Ibid art.6(2).

[2017] Ibid art.6(3).

[2018] Law 277-IV, art.4(1).

[2019] Ibid art.4(4).

To 'detect and identify threats or potential threats to national security',[2021] and to 'safeguard and promote national security and national interests within and outside Kenya' are among the purposes of Kenyan intelligence collection.[2022]

In Papua New Guinea, intelligence is collected to tackle 'matters affecting the maintenance of good order in the country',[2023] 'the combatting of seditious enterprises, espionage and sabotage and the provision of warning of potential military attack, armed incursions […] or the use of military pressures […]'.[2024] It should help 'the preservation of national sovereignty and the detection of any attempts by a foreign power or person to engage in political, military or economic activities contrary to Papua New Guinea's interests'.[2025] '[A]s these could have implications for, or could affect' the country, 'the prospects for world and regional, political, economic and social stability' should be supplied.[2026] It also goes this way for 'future trends of the availability of resources and of prices as these could have implications for Papua New Guinea'.[2027]

In Russia, the objectives of intelligence gathering activity are to provide the institutions 'with the intelligence information they need for decision-making in the political, economic, defence, scientific, technical, and ecological spheres',[2028] 'to ensure conditions promoting the successful implementation of Russian Federation policy in the security sphere',[2029] 'to assist the country's economic development and scientific and technical progress and the ensuring of the Russian Federation's military-technical security'.[2030]

[2020] Ibid art.4(3).

[2021] National Security Intelligence Service Act, s5(1)(b).

[2022] Ibid s5(1)(d).

[2023] NIO Act, s7(a).

[2024] Ibid s7(b).

[2025] Ibid s7(c).

[2026] Ibid s7(d).

[2027] Ibid s7(e).

[2028] Federal Law On Foreign Intelligence, art.5-1.

[2029] Ibid art.5-2.

[2030] Ibid art.5-3.

Slovakian Services shall collect, accumulate and analyse information on activities 'threatening the constitutional establishment, territorial integrity and sovereignty of the Slovak Republic',[2031] or directed against its 'security',[2032] the 'activities of foreign intelligence services', [2033] 'organized criminal activity', [2034] on 'terrorism',[2035] its 'funding' and supporting',[2036] 'political and religious extremism, violent extremism and harmful sectarian groups',[2037] 'activities and threats within the cyber space if they pose a threat to the national security', [2038] 'illegal international people smuggling and migration',[2039] 'matters potentially capable of seriously threatening and/or inflicting damage upon the economic interests,[2040] and the disclosure of protected information.[2041]

The Spanish CNI is in charge of providing the President of Government with information, analyses, and studies in order to prevent threats, risks and aggressions against the independence, the territorial integrity, the national interest, the stability of institutions, and the rule of law.[2042]

The Swiss intelligence law aims at safeguarding democracy and the rule of law, protecting population's individual freedom,[2043] increasing the security of Swiss citizens (including abroad),[2044] supporting its capacity of action,[2045] and securing

---

[2031] Act on the Slovak Information Service, §2(1)(a).

[2032] Ibid §2(1)(b).

[2033] Ibid §2(1)(c).

[2034] Ibid §2(1)(d).

[2035] Ibid §2(1)(e).

[2036] Ibid.

[2037] Ibid §2(1)(f).

[2038] Ibid §2(1)(g).

[2039] Ibid §2(1)(h).

[2040] Ibid §2(1)(i).

[2041] Ibid §2(1)(j).

[2042] Ley 11/2002, art.1.

[2043] LRens, art.2(a).

[2044] Ibid art.2(b).

[2045] Ibid art.2(c).

its security international interests.[2046] 'In the event of a serious and imminent threat', the SRC may have to act to 'protect the constitutional order',[2047] 'support the foreign policy',[2048] and 'to protect the industrial, economic and financial interest'.[2049] Then, the SRC seeks and analyses information to detect and prevent threats to internal and external security: terrorism, [2050] espionage, [2051] the dissemination of nuclear, biologic, and chemical weapon, as well as the resources necessary to make them,[2052] attacks against critical infrastructures[2053] and violent extremism.[2054] The SRC also detects important foreign events related to security policy,[2055] and safeguards Swiss action capacity.[2056]

The SIS has to ensure 'national security with particular reference to the defence and foreign policies', [2057] 'economic well-being', [2058] and the 'prevention or detection of serious crime'.[2059] The GCHQ has an identical mission.[2060]

'The Georgian Intelligence Service [...] carries out intelligence activities in order to protect the national interests of Georgia'.[2061]

[2046] Ibid art.2(d).

[2047] Ibid art.3(a).

[2048] Ibid art.3(b).

[2049] Ibid art.3(c).

[2050] Ibid art.6(1)(a)(1).

[2051] Ibid art.6(1)(a)(2).

[2052] Ibid art.6(1)(a)(3).

[2053] Ibid art.6(1)(a)(4).

[2054] Ibid art.6(1)(a)(5).

[2055] Ibid art.6(1)(b).

[2056] Ibid art.6(1)(c).

[2057] Intelligence Services Act 1994, s1(2)(a).

[2058] Ibid s1(2)(b).

[2059] Ibid s1(2)(c).

[2060] Ibid s3(2).

[2061] Law of Georgia on the Georgian Intelligence Service, art.2.

In New Zealand, the 'principal objectives of the intelligence and security agencies are to contribute to' the 'protection' of 'national security',[2062] 'the international relations and well-being',[2063] and the 'economic well-being'.[2064]

EO 12.333 is worth mentioning again. 'The United States intelligence effort shall provide […] the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats'.[2065] 'Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations', [2066] '[i]nformation needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure',[2067] and '[i]nformation necessary for administrative purposes' are researched, *inter alia*.[2068]

A speech by the former Australian MFA–Kevin Rudd–is quite representative of this phenomenon. 'When Australia contemplates its foreign policy missions, we conceptualise it in the following terms: like all countries our first and foremost foreign policy objective is the maintenance of our national security and the protection of our political sovereignty. The second is the advancement of our national economic interests. The third is advancing the cause of good international citizenship'.[2069] A government report also says that 'States have always used espionage as a tool to pursue national interests'.[2070]

[2062] Intelligence and Security Act 2017, s9(a).

[2063] Ibid s9(b).

[2064] Ibid s9(c).

[2065] EO 12.333, s1.1.

[2066] Ibid s2.3(b).

[2067] Ibid s2.3(e).

[2068] Ibid s2.3(j).

[2069] Alexander Chapman and Sam Kealey (eds), 'Australian Practice in International Law 2011' (2013) 31 Australian Y.B.I.L. 285, 315-16.

[2070] PM&C, 'Strong and Secure–A Strategy for Australia's National Security' (2013) 16

In sum, some states indeed limit their intelligence activity to national security purposes. However, they are overwhelmed by legislations extending espionage to the defence of their economic interests. Likewise, executive conducts support the practice of espionage.

B. Executive conducts

In the USA, the purpose of EO 12.333 is 'to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers'.[2071] As of 1952, '[t]he COMINT mission of the NSA' was already 'to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments'.[2072]

In parallel, courts do not revolutionize the debate.

C. Decisions of national courts

Courts sometimes refer to international law, usually when they have to determine whether someone benefits from immunity under the VCDR, or may be considered a spy under The Hague Conventions,[2073] as well as for extradition

<www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf> accessed:19.09.2016.

[2071] Executive Order 12.333, s2.2.

[2072] Office of the Historian, 'Directive No 9 Revised' (1952) 2-b <history.state.gov/historicaldocuments/frus1950-55Intel/d257> accessed:27.12.2017.

[2073] Cour de Cassation, *Von Berenberg-Gossler* (1969) 52 ILR 492 in Jean-Francois Lachaume, 'Jurisprudence française concernant le droit international public–année 1969' (1970) 16 A.F.D.I. 875, 937-8; US Supreme Court, *Johnson v Eisentrager* (1950) 339 US 763.

requests.[2074] Apart from those cases, it is genuinely in compliance with domestic criminal law that spies have been condemned in peacetime: in Australia,[2075] Estonia,[2076] France,[2077] Japan,[2078] the Netherlands,[2079] the UK,[2080] the USA.[2081] The foreign power involved may be explicitly quoted,[2082] or just implied.[2083]

The analysis of legislative acts, executive conducts and decisions of national courts thus reveals a paradoxical practice of states. Yet, ascertaining *opinio juris* is decisive: this process helps confirming that no customary rules exist when it comes to cyber-espionage.

[2074] CA Paris, *Hachent et Wagih Martini c Veuve Martini* (1972 in Jean-Francois Lachaume, 'Jurisprudence française concernant le droit international public–Année 1972' (1973) 19 A.F.D.I. 974, 1012; Supreme Court, *GWD v Public Prosecutor* (21.12.1982) in LANM Barnhoorn, 'Netherlands Judicial Decisions involving Questions of Public International Law 1982–1983' (1984) 15 Netherlands Y.B.I.L. 423, 447.

[2075] ACT Supreme Court, *R v Lappas* (2003) 139 A Crim R 77.

[2076] 'L'Estonie condamne trois espions russes', *Le Courrier de Russie* (23.02.2016) <www.lecourrierderussie.com/international/2016/02/estonie-trois-espions-russes/> accessed:11.10.2017.

[2077] Cour de Cassation (12.02.1985) in Jean-Francois Lachaume, 'Jurisprudence française concernant le droit international public (Année 1985)' (1986) 32 A.F.D.I. 923, 953; Cour de Cassation (1987) Bull crim 1987 No.78; Cour de Cassation, Klaus Tscheu (12.01.1988) in Jean-Francois Lachaume, 'Jurisprudence française relative au droit international' (1989) 35 A.F.D.I. 842, 878-9.

[2078] Shuichi Furuya and Satsuki Konaka, 'Chronology of Japanese Foreign Affairs in 2008' (n.1469) 707.

[2079] CA of Den Bosch, *Public Prosecutor v WL* (12.11.1975) in LANM Barnhoorn, 'Netherlands Judicial Decisions involving Questions of Public International Law 1974–1975', (1976) 7 Netherlands Y.B.I.L. 303, 351.

[2080] Court of Appeal, *R v Blake (George)* (1961) 45 Cr App R 292; Court of Appeal, *R v Bingham (Maureen Grace)* (1973) 57 Cr App R 439.

[2081] California Northern District Court, *United States v Liew et al* (2014) Case No.3:11-cr-00573; US Court of Appeals for the Second Circuit, *United States v Rosenberg et al* (1952) 195 F 2d 583; US District Court, Massachusetts, *United States v Zehe* (1985) 601 F Supp 196.

[2082] Cour de Cassation (1984) Bull crim 1984 No.310.

[2083] Cour de cassation (1988) No.87-84.360.

2.2. *Opinio juris*

According to the ILC, 'public statements made on behalf of States' (A), 'official publications' (B), 'government legal opinions' (C), and 'treaty provisions' (D) contribute to *opinio juris*. These elements, when related to espionage, are thus alternatively analysed.

A. Public statements made on behalf of states

They consist in both explicit (a), and implicit acknowledgement of intelligence-collection (b).

a. Explicit acknowledgment of intelligence-collection

On some occasions, states have acknowledged their intelligence-gathering activities.

As of 1998, Castro claimed 'the right' to send spies.[2084] In 2004, Australian MFA Downer said that they would continue their efforts 'to ensure the timely collection and dissemination of operational intelligence in support of PSI [Proliferation Security Initiative] actions and objectives'. [2085] Following parliamentary questions on the visits of British nuclear submarines in Gibraltar, the Spanish government answered that 'as provided in Act 11/2002 of 6 May', 'information and confidential data necessary to prevent and avoid any hazard, threat or aggression against national interests' were collected and reported.[2086]

Declarations by the USA have been far more common, particularly since 2001. Following the adoption of UNSC resolution 1373, the USA had the following position. Firstly, '[t]he U.S. uses a full range of counterterrorism and counterintelligence techniques in preventing terrorist acts, including the use of

[2084] 'In rare admission, Castro says Cuba has dispatched spies across U.S.' (n.632).

[2085] Jennifer Cavenagh, 'Australian Practice in International Law 2004' (2006) 25 Australian Y.B.I.L. 463, 671.

[2086] Jiménez Piernas and others (eds), 'Spanish Diplomatic and Parliamentary Practice in Public International Law, 2009' (2011) 15 Spanish Y.B.I.L. 73, 210.

human and technical sources; aggressive undercover operations; analysis of telephone and financial records; mail; and physical surveillance'.[2087] Secondly, 'U.S. law enforcement and intelligence agencies have many active and aggressive information sharing programs to prevent terrorist acts'.[2088] CIA director George Tenet expressly referred to '[o]ur spies' who penetrate the 'network through a series of daring operations over several years' in 2004.[2089] Following questions by the Human Rights Committee (HRC), the US administration answered that 'NSA surveillance activities are subject to extensive oversight by the Executive Branch, the Congress, and the Judiciary. The FISC [FISA Court] plays an important role in overseeing certain NSA collection activities conducted pursuant to the FISA. It not only authorizes these activities, but it also plays a continuing and active role in ensuring that they are carried out lawfully'.[2090] In 2014, Secretary Kerry defined four principles guiding the reforms of intelligence collection, believed as 'universally applicable', which 'should help in distinguishing countries that use surveillance to repress their people': rule of law, legitimate purpose (national security), oversight, transparency.[2091]

Another approach is underlining that 'everyone does it'. When Indonesian politicians learnt they had been spied on by Australia, PM Abbott simply said that 'all government collect information'.[2092] According to the former French MFA, Bernard Kouchner, the USA and the NSA 'were originally looking for

---

[2087] Sally Cummins and David Stewart, *Digest of United States Practice in International Law 2001* (ILI 2002) 901.

[2088] Ibid.

[2089] George Tenet, 'Remarks as prepared for delivery by Director of Central Intelligence George J. Tenet at Georgetown University' (05.02.2004) <http://nsarchive.gwu.edu/NSAEBB/NSAEBB80/Remarks%20as%20prepared%20for%20delivery%20by%20Director%20of%20Central%20Intelligence%20George%20J_%20Tenet%20at%20Georgetown%20University%20February%205,%202004.htm> accessed:20.11.2017.

[2090] CarrieLyn Guymon, 'Digest of United States Practice in International Law 2014' (2015) 177 <www.state.gov/documents/organization/244504.pdf> accessed:19.03.2018.

[2091] US Department of State, 'Remarks to the Freedom Online Coalition Conference' (28.04.2014) <www.state.gov/secretary/remarks/2014/04/225290.htm> accessed:14.05.2017.

[2092] (2013) 59(11) Keesings, 53009.

information about terrorists'.[2093] However, 'what is shocking, now, is that they do so with individuals. We were shocked by the scale of eavesdropping'.[2094] But, 'to be honest, we listen to them too. Everybody is listening to everybody'.[2095] In 2011, John Brennan insisted on the fact that 'intelligence saves lives', and added that all actions–including covert actions–are to be carried out in compliance with the rule of law.[2096] Other governments are allegedly more likely to share intelligence thanks to this respect of the rule of law.[2097] In 2012, Eric Holder declared: 'we must–and will continue to–use the intelligence-gathering capabilities that Congress has provided to collect information that can save and protect American lives'.[2098]

A corollary argument, which has long been supported to by the USA, is reciprocity. According to the DoD, '[t]he lack of strong international legal sanctions for peacetime espionage may also constitute an implicit application of the international law doctrine called "tu quoque" (roughly, a nation has no standing to complain about a practice in which it itself engages)'.[2099] During the U-2 crisis, President Eisenhower said that '[i]t is certainly no secret that, given the state of the world today, intelligence collection activities are practiced by all countries'.[2100] At the Security Council, Cabot Lodge referred to the Soviets' spy rings and threats to use nuclear weapons, concluding that '[t]his record makes it

---

[2093] Ivan Valerio, 'Bernard Kouchner: "Nous écoutons aussi, mais nous n'avons pas les moyens des Etats-Unis, ça rend jaloux"', *Europe1* (22.10.2013) <lelab.europe1.fr/bernard-kouchner-nous-ecoutons-aussi-mais-nous-n-avons-pas-les-moyens-des-etats-unis-ca-rend-jaloux-11328> accessed:29.09.2016.

[2094] Ibid.

[2095] Ibid.

[2096] John Brennan, 'Strengthening our Security by Adhering to our Values and Laws' (16.09.2011) <www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an> accessed:30.11.2015.

[2097] Ibid.

[2098] DoJ, 'Attorney General Eric Holder Speaks at Northwestern University School of Law' (05.03.2012) <www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-northwestern-university-school-law> accessed:29.11.2015.

[2099] DoD/OGC, 'An Assessment' (n.676) 46.

[2100] (1960) 42 Dep't St Bull 809, 818.

particularly unsuitable for the Soviet Union to adopt a holier than thou attitude and to criticize others. The truth is that the USSR does not come into court with clean hands'.[2101]

Affirming that espionage is necessary is also quite common. During the U-2 case, the necessity of espionage was underlined by both China and the USA. Following the revelations about the NSA, Australian Foreign Secretary Julie Bishop affirmed that the FiveEyes Agreement 'is about saving lives'.[2102]

A strange position was once adopted by the former deputy director of the CSIS, Ray Boisvert. Following allegations of espionage by Canada on Brazilian companies, he declared that Canada could have been using Brazil as part of a war game scenario and not for actual espionage. He explained: 'it's a hypothetical thing, like "could we do something?" Quite often it's an exercise and they'll use any country just to test the theories'.[2103]

The acknowledgement of intelligence-collection may also happen in a subtler way, through an implicit confirmation.

b. Implicit acknowledgment of intelligence-collection

In some situations, states acknowledged that intelligence activities were carried out, but refused to disclose details, for reasons of national security. Such was the case in 2002, when some NATO states were requested by the International Criminal Tribunal for the former Yugoslavia (ICTY) to deliver intelligence linked to General Odjanic. Were concerned '[a]ll recordings, summaries, notes

[2101] UNSC 860th Meeting (26.05.1960) [72]-[73].

[2102] Katharine Murphy, 'Edward Snowden a traitor but US spy review is welcome, says Julie Bishop', *Guardian* (23.01.2014) <www.theguardian.com/world/2014/jan/23/edward-snowden-a-traitor-but-us-spy-review-is-welcome-says-julie-bishop> accessed:21.11.2015.

[2103] 'Brazil accuses Canada of spying after NSA leaks', *Guardian* (08.10.2013) <www.theguardian.com/world/2013/oct/08/brazil-accuses-canada-spying-nsa-leaks> accessed:08.11.2015.

or text of any intercepted communications (electronic, oral or written)', and '[a]ll correspondence, memoranda, reports, recordings or summaries of any statements […] including sources of information working on your behalf'.[2104]

Canada answered that some of these documents were 'of particular sensitivity' and their 'disclosure could prejudice national security interests'.[2105] Then, it made the following statement: 'Canada emphasizes the extreme sensitivity of information relating to the existence or non-existence of intercepted communications. To disclose whether such information does or does not exist would cause serious prejudice to national security interests by potentially revealing the existence and capabilities of any intelligence programs, by jeopardizing methods and sources, or by potentially revealing which areas and subjects are or are not of surveillance interest'.[2106] Canada also affirmed that 'discussion of such matters could put lives at risk and jeopardize a State's future capacity to collect information'.[2107] As a conclusion, Canada said that it 'would explore means to share the necessary information and prevent a miscarriage of justice, without prejudicing its national security interests'.[2108]

The USA reacted similarly to this order. 'The United States has a compelling national security interest in protecting information about intercepted communications, including whether or not it possesses them. Disclosure of such information may reveal not only the content of particular information, but the extent and nature of United States capabilities, and where and how they might be directed. Such information is among the most highly protected national security assets of the United States, and its compromise would cause grave damage to United States national security. It is for this reason that the United States refuses to confirm or deny the existence of intercepts [...] This approach

---

[2104] Colleen Swords, 'Canadian Practice in International Law–At the Department of Foreign Affairs and International Trade in 2002-3' (2003) 41 Canadian Y.B.I.L. 443, 450-1.

[2105] Ibid 456.

[2106] Ibid.

[2107] Ibid.

[2108] Ibid 457.

enables the United States to search in all sources, and to disclose relevant information in a manner that does not compromise any intelligence sources and methods [...]'.[2109]

Evidence of espionage acknowledgement is not only available in public statements, but also in official publications.

B. *Official publications*

The intelligence services' official reports and websites are sometimes more explicit about their field of action than law itself. Such is the case for Croatia, Norway and South Korea. A public report of 2014 assessed that SOA's mission consists of '[c]ollecting information in Croatia and abroad by using a wide range of measures, including human and open sources and technical devices'.[2110] The NIS's website affirms that it 'is Norway's only foreign intelligence service. NIS collects information about situations and conditions outside the nation's borders'.[2111] According to the Norwegian Parliament, '[t]here are fundamental differences between the regulatory framework and tasks of PST [Norwegian Police Security Service], which is primarily to operate in Norway, and NIS, which can only carry out surveillance abroad'.[2112] 'In the global era, intelligence activities must necessarily transcend borders. To protect the country's security and interests', the South Korean National Intelligence Service 'ceaselessly engages in intelligence affairs in every corner of the world all the year round'.[2113]

[2109] Sally Cummins and David Stewart, *Digest of United States Practice in International Law 2003* (ILI 2004) 217.

[2110] Security and Intelligence Agency, 'Public Report 2014' (2014), 7 <www.soa.hr/files/file/Public-Report-2014.pdf> accessed:13.12.2016.

[2111] EOS Committee, 'The Norwegian Intelligence Service' <https://eos-utvalget.no/english_1/services/the_eos_services/the_norwegian_intelligence_service/> accessed:17.05.2017.

[2112] EOS Committee, 'Abbreviated annual report for 2013' (2014) [2.4] <https://eos-utvalget.no/english_1/annual_reports/content_3/text_1401199189882/1403522809228/forkortet_rsmelding_engelsk_versjon.pdf> accessed:21.05.2017.

Evidence of *opinio juris* may also be found in government legal opinions and treaty provisions.

C. Government legal opinions

Switzerland expressly affirms that 'customary international law tolerates international espionage to some extent'.[2114]

D. Treaty provisions

Proposals to limit spying have been made at least three times, without any success. Vietnam asked China to sign an agreement to refrain from espionage and reconnaissance activities on their respective territory as well as 'other offensive activities'. [2115] Indonesia proposed Australia to sign a 'Code of Ethics'.[2116] Germany demanded the USA a 'no-spy agreement'.[2117] They were all rejected. In a testimony about the UNCLOS before the Senate Committee on Armed Services, Admiral Clark said: 'I just want to be on record in saying that we would never recommend a treaty that would require us to get a permission slip from anyone to conduct operations or restrict our intelligence activities around the world, because we know that those kind of freedoms are essential to what we have to do to be successful in our mission'.[2118] At the opposite, the Luxembourgian 'Government will support initiatives within the EU to

---

[2113] National Intelligence Service Korea <http://eng.nis.go.kr/EAF/1_3.do> accessed:03.02.2016.

[2114] Caflisch, Pratique Suisse 2013 (n.690) 106.

[2115] (1979) 25(10) Keesings, 29874.

[2116] (2013) 59(11) Keesings, 53009.

[2117] (2014) 60(5) Keesings, 53371.

[2118] S Hrg Doc 108–796. See Sally Cummins, *Digest of United States Practice in International Law 2004* (ILI 2006) 689.

implement a convention against espionage with its political and economic partners'.[2119]

Intelligence-sharing has actually promoted cooperation between states. Australia, Canada, New Zealand, the UK and the USA are part of the UKUSA agreement.[2120] The USA, South Korea and Japan have agreed on a Pact to share intelligence about North Korea.[2121] Russia, Iran, Iraq and Syria share intelligence on the Islamic State.[2122] Israel, Egypt and Jordan have 'put aside past animosities' to reach 'unprecedented' intelligence cooperation.[2123] Bilateral intelligence-sharing agreements exist between Israel and the USA.[2124] In Europe, 'terrorist threat has helped creating three clubs, in 1971, 1976 and 1979': Bern (terrorism and drug-trafficking), Trevi (terrorism, drug-trafficking and organized crime) and Vienna (terrorism and migratory movements).[2125]

The new conventional trend is actually combating cybercrime, with states agreeing to punish it in their domestic law. This is how member states are required by the Convention of Budapest to criminalize '[o]ffences against the

---

[2119] Gouvernement du Luxembourg, 'Programme gouvernemental 2013' (2013), 10 <www.sante.public.lu/fr/publications/p/programme-gouvernemental-2013/programme-gouvernemental-2013.pdf> accessed:27.04.2016.

[2120] UK–USA Agreement ('UKUSA'/Five Eyes/FVEY') (signed on 05.03.1946).

[2121] Ankit Panda, 'US, South Korea, Japan Start Sharing Intelligence on North Korea', *The Diplomat* (30.12.2014) <thediplomat.com/2014/12/us-south-korea-japan-start-sharing-intelligence-on-north-korea/> accessed:01.11.2016.

[2122] Dana Stuster, 'Russia, Iran, Iraq, and Syria to Share Intelligence on Islamic State', *Foreign Policy* (28.09.2015) <foreignpolicy.com/2015/09/28/russia-iran-iraq-and-syria-to-share-intelligence-on-islamic-state/> accessed:01.11.2016.

[2123] AFP and TOI Staff, 'Top IDF general: Israel, Egypt have "unprecedented" intel cooperation', *Times of Israel* (20.04.2016) <www.timesofisrael.com/top-idf-general-israel-egypt-have-unprecedented-intel-cooperation/> accessed:01.11.2016.

[2124] Amir Oren, 'Leaked Classified Memo Reveals U.S.-Israeli Intel Cooperation on Egypt, Iran', *Haaretz* (5.08.2014) <www.haaretz.com/israel-news/.premium-1.608802> accessed:01.11.2016.

[2125] Sébastien-Yves Laurent, *Atlas du Renseignement–Géopolitique du Pouvoir* (Les Presses de Sciences Po 2014) 174-8.

confidentiality, integrity':[2126] 'illegal access',[2127] 'illegal interception',[2128] 'data interference',[2129] 'system interference',[2130] 'misuse of devices' etc.[2131] This is also how the ECOWAS directive on Fighting Cyber Crime tackles the 'fraudulent access to computer systems',[2132] 'fraudulently remaining in a computer system',[2133] 'interfering with the operation of a computer system',[2134] 'fraudulent input of data in a computer system',[2135] 'fraudulent interception of computer data',[2136] 'fraudulent modification of computer data'.[2137] An EU directive similarly confronts 'illegal access to information systems',[2138] 'illegal system interference',[2139] 'illegal data interference',[2140] 'illegal interception'.[2141]

[2126] Convention on Cybercrime (Adopted:23.11.2001–EIF:01.07.2004) ETS 185, ch.2, s.2, t.1.

[2127] Ibid art.2.

[2128] Ibid art.3.

[2129] Ibid art.4.

[2130] Ibid art.5.

[2131] Ibid art.6.

[2132] Directive On Fighting Cyber Crime Within ECOWAS (n.1808) art.4.

[2133] Ibid art.5.

[2134] Ibid art.6.

[2135] Ibid art.7.

[2136] Ibid art.8.

[2137] Ibid art.9.

[2138] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, art.3.

[2139] Ibid art.4.

[2140] Ibid art.5.

[2141] Ibid art.6.

3. Conclusion

As required by the ILC, '[e]ach element' has been 'separately ascertained' with respect to cyber-espionage, and data, collected. It is now time for an inductive assessment.

'The relevant practice must be general, meaning that it must be sufficiently widespread and representative, as well as consistent'. It is obvious that the universal prohibition of espionage by domestic laws fulfils these conditions. The legislations available in French, English, German and Spanish reveal a clear prohibition on all five continents: in Europe (10-18 states), Asia (6-12), Africa (6-14), America (10), and Oceania (3). There is moreover a trend in explicitly tackling cyber-intrusions. In parallel, the self-authorization to carry out intelligence activities is also widespread and representative. Seventeen States authorize intelligence collection abroad: in Europe (11), Asia (1), America (2), Africa (1) and Oceania (2). Nine of them expressly refer to cyber-intelligence. Two other European states refer exclusively to the assistance due to national agents operating overseas, but this obviously amounts to a confession that espionage is carried out. Nine other states have adopted provisions that may be interpreted as a basis to commit espionage: in Europe (3), Africa (2), America (3), and Asia (1). As to a potential distinction between political-military and economic espionage, it is excluded: eleven States exclusively authorize espionage for the first purposes (including 5 in Europe, 4 in America, 1 in Africa and 1 in Asia), while seventeen extend their legislation for the second one (including 10 in Europe, 1 in America, 1 in Asia, 2 in Africa, 3 in Oceania). The number of states carrying out cyber-espionage activities is probably higher, as regularly

revealed by media, and includes Israel,[2142] Iran,[2143] and North Korea.[2144] Cuba also used to send or recruit agents abroad.[2145]

As to *opinio juris*, '[t]he requirement, as a constituent element of customary international law, that the general practice be accepted as law […] means that the practice in question must be undertaken with a sense of legal right or obligation'. The sense of right accompanying the prohibition of espionage on a state's own soil can hardly be denied, as it amounts to a sovereign prerogative. As to foreign intelligence gathering, nine states have acknowledged such activities or claimed their right do so, in Europe (4), America (3), Asia (1), and Oceania (1). However, instances of protest or denunciations–sometimes by the very same states–are as numerous, and have been regularly quoted along this essay.

The proverb '[d]o unto others as you would have them do unto you' is far from topical with respects to cyber-espionage. States prohibit activities of foreign intelligence services on their own soil, while allowing themselves to spy on their counterparts. Practice is both in favour and against espionage; *opinio juris* is often in favour, sometimes against espionage. In similar situations, the ICJ found 'the members of the international community profoundly divided',[2146] or affirmed

---

[2142] Jeff Stein, 'Israel won't stop spying on the U.S.', *Newsweek* (06.05.2014) <www.newsweek.com/2014/05/16/israel-wont-stop-spying-us-249757.html> accessed:06.09.2015.

[2143] Sami Kronenfeld and Gabi Siboni, 'Iranian Cyber Espionage: A Troubling New Escalation', *INSS Insight* (16.06.2014) <www.inss.org.il/publication/iranian-cyber-espionage-a-troubling-new-escalation/> accessed:06.09.2015.

[2144] Christine Kim, 'North Korea hacking increasingly focused on making money more than espionage: South Korea study', *Reuters* (28.07.2017) <www.reuters.com/article/us-northkorea-cybercrime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO> accessed:04.03.2018;

[2145] Terrence McCoy, 'Cuba deal reveals new clues in case of Ana Montes, "the most important spy you've never heard of"', *WP* (18.12.2014) <www.washingtonpost.com/news/morning-mix/wp/2014/12/18/cuba-deal-reveals-new-clues-in-case-of-ana-montes-the-most-important-spy-youve-never-heard-of/?utm_term=.adda1bff4747> accessed:17.01.2017;

[2146] *Nuclear Weapons* (n.477) [67].

that '[t]he facts brought to' its 'knowledge […] disclose so much uncertainty and contradiction, so much fluctuation and discrepancy […] and the practice has been so much influenced by considerations of political expediency in the various cases, that it is not possible to discern in all this any constant and uniform usage, accepted as law […]'.[2147] Espionage *per se* is in the same situation, and the existence of any customary rules–whether in favour or against–is thus excluded.

[2147] *Asylum case* (n.428), 277.

GENERAL CONCLUSION

In this general conclusion, a synthesis–or 'overview'–of the legal framework of cyber-espionage is developed (1). Then, a discussion about the topic's perspectives (2) conclude this thesis.

1. Overview

During decades, states were satisfied with the indirect–and ambiguous–control of espionage offered by the physical presence of the spy on their territories. Should he be a diplomat, the spy could be declared PNG and expelled. Should the spy's state of allegiance acknowledge his sending, the capturing state could openly blame it for a violation of sovereignty, and decides to exchange the spy. Failing this recognition–or should it be in wartime–the spy could be judged, according to the domestic legislation. This balance is affected by the dematerialization and the de-territorialisation of espionage, and the inapplicability of some rules is directly explained by this phenomenon.

Such is the case for the breach of sovereignty. The illegality of traditional spying only resides in its non-consensual territorial intrusion, and espionage *per se* is not regulated by sovereignty. What is more, state practice confirms this. Such is also the case for article 22(1) VCDR; while breaking into an embassy to install listening devices is an obvious breach of this article, it does not go this way for cyber-espionage–or even eavesdropping. The sole physical trespass into diplomatic premises is indeed targeted by article 22(1). Article 22(3) does not apply to cyber-espionage or eavesdropping for the same reasons: 'premises', 'furnishing', 'property' only refer to physical concepts. Similarly, the notion of 'intrusion' mentioned in article 22(2) tackles a physical intrusion. While Hague II (1899), Hague IV (1907), and Additional Protocol I authorize espionage between belligerents, they cannot be transposed to cyber-espionage. These rules have indeed been created in relation to specific fields: land, sea or airspace. To the extent that cyberspace is a different field–an element which is confirmed by states–these rules cannot be integrally transposed.

In contrast, the passage of espionage on the Internet has changed nothing with respect to some rules. JAB was silent regarding espionage, and remains mute regarding cyber-espionage. Indeed, none of them involves the resort to a weapon, and states are willing to exploit this silence to collect intelligence and reduce uncertainty. Then, the validity of meta-principles is disputed. This transition also remains without effect on non-intervention, as espionage *per se* is not coercive. Besides, both espionage and cyber-espionage are actually directed towards the political, economic, social and cultural systems of the state, but few spheres remain under its exclusive domestic jurisdiction. Neither traditional espionage nor cyber-espionage are apprehended by TRIPS, as article 3 has no extraterritorial vocation, while states are not prevented from spying on companies abroad under article 39. Under article 3, the State Party merely has to ensure national treatment on its own territory, while article 39 only aims to protect companies against the activities of other non-state actors (or 'third parties'), and obliges states ('Members') to effectively ensure the protection of undisclosed information. Security exceptions do not discourage cyber-espionage either. In the field of diplomatic espionage, the notions of 'damage', 'disturbance of the peace of the mission', 'impairment of the dignity' defined by article 22(2) VCDR are probably toothless for both espionage and cyber-espionage. They indeed aim at restraining any excess during protests. In terms of espionage by embassies, the VCDR delegates to State Parties the power to regulate and take measures against spies, without prohibiting espionage by itself. The hosting states can thus require the names and approve the nomination of military, naval or air attachés, limit the size of the mission and refuse to accept officials of a particular category. It is under the prism of the hosting state's domestic law that the 'lawful means'–those that the diplomats have to respect during intelligence-collection–have to be interpreted. Surprisingly, some of these rules are still of help regarding cyber-espionage. Following the hacking of the DNC, thirty-five Russian diplomats based in Washington and described as 'intelligence operatives' were declared PNG.[2148]

[2148] Laura Gambino, Sabrina Siddiqui and Shaun Walker, 'Obama expels 35 Russian diplomats in retaliation for US election hacking', *Guardian* (30.12.2016) <www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack> accessed:19.01.2017.

In the end, two bodies of rules are both applicable in cyberspace and relevant for cyber-espionage. First, article 8 of Hague V empowers a neutral state to tolerate cyber-espionage activities going through its infrastructure. However, this Convention only applies in wartime. Then, a textual interpretation reveals the applicability of article 3 of Hague V, but it only indirectly affects cyber-espionage by preventing the erection of internet infrastructures on the territory of a neutral state to communicate with belligerents, as well as the use of such structures–when not 'opened for the service of public message'.
Second, a textual and evolutionary interpretation of articles 24 and 27(2) reveals that the VCDR is the sole instrument to prohibit cyber-espionage, when directed towards digital and vocal forms of official correspondence, as well as electronic archives and documents of the diplomatic mission. In any case, cyber-espionage activities on embassies are prohibited.

Cyber-espionage is also defined by the absence of customary international rules, whether prohibitive or permissive. State practice is indeed contradictory, being both in favour of cyber-espionage–national agencies are authorized to collect intelligence abroad–and against–domestic criminal laws prevent other states from spying. *Opinio juris* is similarly contradictory, as other states often defend their own right to spy on the others, but denounce espionage, when carried out against their own interest.

The legal regime of cyber-espionage in international law is not uniform, rather fragmented: there is indeed no general prohibition or authorization of this activity. The only restriction of this activity concerns a specific form–spying on embassies–and comes under a specific instrument–the VCDR. Cyber-espionage is, outside this scope, characterised by an absence of law. It merely constitutes an unfriendly act, i.e. 'a conduct (act or omission) of a subject of international law which inflicts a disadvantage, disregard or discourtesy on another subject of international law without violating any legal norm'. [2149] Authors such as

[2149] Dagmar Richter, 'Unfriendly Act' (2013) M.P.E.P.I.L., [1].

Edmondson,[2150] Lotrionte,[2151] Lafouasse,[2152] Navarette,[2153] Cohen-Jonathan and Kovar[2154] had previously supported this theory regarding espionage *per se*, as well as Beard,[2155] and Talmon,[2156] regarding electronic and cyber-espionage. States all spy on each other, and they are eager to take advantage of this absence of rules.

2. Perspectives

Regarding the status of doctrine, this conclusion explains how authors have developed a managerialist approach to cyber-espionage (2.1). As to the legal framework, it predicts a triumph of domestic law (2.2).

2.1. Status of doctrine: A managerialist approach to cyber-espionage

Nature and international legal doctrine have something in common: they abhor a vacuum. Thus, 'international lawyers, notwithstanding other possible forms of (self-) regulation, have considered that cyber operations have been left dangerously unregulated–which, in their view, means unregulated by international law', and 'have come to feel a deontological duty to address such a legal vacuum with their own tools and ensure that cyber-operations are subjected to international legal rules […]'.[2157] In spite of a several-decades-old disinterest of states for regulating espionage through international rules, doctrine has tried to stretch the existing legal frameworks to cyber-espionage. This could actually reflect the fact that '[t]he role imagined for international law and international

[2150] Edmondson (n.1672) 444-5.

[2151] Lotrionte (n.797) 502.

[2152] Lafouasse, *L'Espionnage* (n.66) 236.

[2153] Navarette (n.708) 47.

[2154] Cohen-Jonathan and Kovar (n.567) 252.

[2155] Beard (n.594) 139.

[2156] Talmon, 'Tapping' (n.793).

[2157] Jean d'Aspremont, 'Cyber Operations and International Law: An Interventionist Legal Thought' (2016) 21 Journal of Conflict & Security Law 575, 577.

lawyers is premised upon an idealism about the capacity to do good through international law'.[2158] But in doing so, they have circumvented formality in both the 'evidence of law' (CIL) and the 'formal determination of the content of rules' (treaty interpretation),[2159] and rules have become a mean to achieve a pre-determined goal. As Koskenniemi describes it, 'we are left with managerialism in the precise sense that law turns onto rules of thumb or soft standards that refer to the best judgement of the experts in the box–substance, thoroughly committed to advance the purposes of the appropriate box'.[2160] Moreover, '[e]veryone participates in such efforts with two concerns in mind: to agree on nothing that might prejudice the future interests of my country, but to try as hard as possible to attain a definition that will strike at every conceivable future adversary'.[2161] This phenomenon is also denounced by d'Aspremont, as 'the doctrinal-formalist' succumbed, 'not only to his own weight and self-confidence, but also to the blows of the next hegemon, i.e. the managerialist international lawyer who thinks that international lawyers managing the world can no longer afford overly formal and sophisticated structures of argumentation'.[2162] He thus distinguishes 'legalism'–'the exercise of authority through rules'–and 'managerialism'–'the exercise of authority through groups of experts'.[2163] Kennedy similarly acknowledges that 'to say the world is covered in law is also to say we are increasingly governed by experts'.[2164] In such process, doctrine

---

[2158] Anne Orford, 'Embodying Internationalism: The Making of International Lawyers' (1988) 19 Australian Y.B.I.L. 1, 16.

[2159] The terms are those used in: d'Aspremont, *Formalism and the Sources of International* (n.522) 151, 157.

[2160] Martti Koskenniemi, 'International Law: Constitutionalism, Managerialism and the Ethos of Legal Education' (2007) 1(1) Eur.J.Legal.Stud. 8, 14.

[2161] Martti Koskenniemi, 'The Fate of Public International Law: Between Technique and Politics' (2007) 70(1) M.L.R. 1, 10.

[2162] Jean d'Aspremont, 'Managing Change in International Law and the Dream of the Managerialist International Lawyer', (*EJIL:Talk!*, 25.09.2015) <www.ejiltalk.org/managing-change-in-international-law-and-the-dream-of-the-managerialist-international-lawyer/> accessed:01.02.2018.

[2163] Jean d'Aspremont, 'The Law of International Organizations and the Art of Reconciliation' (2014) 11 I.O.L.R. 428, 443.

[2164] David Kennedy, 'Challenging Expert Rule: The Politics of Global Governance' (2005) 27 Syd.L.R. 5, 6.

echoes Jenks' recommendations: '[t]here are circumstances in which, while the law remains unsettled, it is the duty of international lawyers to put such weight as they may have behind the law which is struggling to be born, rather than to apply methods of meticulous logical analysis of the extent to which a firm international obligation can be said to have already arisen in a manner which makes it virtually impossible to develop the law to meet new needs, even when this can be done by recognised methods of legal reasoning by subsuming new facts under old principles'.[2165] Unfortunately, this effort proves to be counter-productive, as '[a]ll told, states are left without any real sense of what they can and cannot do in their IO'.[2166]

Hollis once mentioned: '[o]f course, lawyers can assess new technology and find it analogous to prior cases [...] But the more novel the technology–the more it can function in non-analogous ways, or with effects previously unimagined–the more lawyers may (or at least should) struggle with interpreting and applying the law to it'.[2167] 'New technologies [...] may require more than analogies to existing law; they may require entirely new frameworks'.[2168] This is precisely where the expertise of international lawyers is vital. Sometimes, existing international law may satisfactorily regulate new technologies. Otherwise, international lawyers should not stretch it by any means–and, in doing so–circumvent formality. In contrast, the existing framework's gaps should be highlighted. Then, if an activity is perceived as problematical, lawyers should resort to a legislative approach or make recommendations, taking into account the specificities of the technology and the different 'cultural' conceptions. Decision makers would thus benefit from a pool of legal expertise, suggestions, a better understanding of technical aspects and what positions should be expected from foreign negotiators.

[2165] Wilfred Jenks, *The Common Law of Mankind* (Stevens&Sons 1963) 48.

[2166] Duncan Hollis, 'Why States Need an International Law for Information' (2007) 11(4) Lewis&Clark L.R. 1023, 1045. Hollis also recommends the adoption of an 'international law for information operations' ('ILIO'), whose point 'is to afford a considered process in which states devise new rules in ways that afford more certainty to the use of IO than the current framework and facilitate its usage in appropriate situations' (1053-7).

[2167] Duncan Hollis, 'The fog of technology and international law' (SIDI, 14.05.2015) <www.sidiblog.org/2015/05/14/the-fog-of-technology-and-international-law/> accessed:16.11.2018.

[2168] Ibid.

Writing, rewriting, or reinterpreting law would be made easier for states, and could replace the successive declarations of intent and unsubstantial denunciations which characterize the area, and blur what is legal or not. Many tensions indeed stem from the ambiguity of the law, which states are eager to take advantage of. Adopting rules adapted to a given environment would make law more effective, breaching it would become more risky, while 'victim' states would be empowered with protecting themselves and demanding reparations.

2.2. Status of law: towards the triumph of domestic law?

In light of the previous development, three trends could materialise in practice.

First, it is highly unlikely that an international treaty prohibiting cyber-espionage will emerge soon. States have indeed spied on each other for centuries, and have not expressed any desire to create new rules. In the case of economic cyber-espionage, further declarations and codes of conduct will probably appear on the bilateral and regional levels. In the light of many States' double-dealing, binding rules remain improbable. Even the USA–that has vigorously denounced industrial spying–carries out economic cyber-espionage. To the extent that political and military cyber-espionage actually decrease risks of conflicts–allowing states to make sure that they are not on the verge of being attacked–their regulation is not desirable. Economic cyber-espionage, however, might be considered under a different perspective, and calls for some regulations. This wish has besides been recently reiterated in Paris Call.[2169] Yet, this is an arduous task. Distinguishing between state companies and private companies is not relevant: some state companies might have no link with the defence sector (public transports etc.), whereas private companies might actually be involved in the production of weapons. One could think of a gradation, and distinguish between industrial secrets, lacking any link with the defence sector; industrial secrets, linked to the defence sector; political and military secrets. However, this model is not sustainable, as only an access to the secret could reveal its actual nature. Another model could be the distinction between companies specialized

[2169] Paris Call (n.1621).

in the defence sector; companies having ties with the defence sectors; and other companies. However, the appearance of joint-ventures and industrial conglomerates could complicate it. Meanwhile, companies should adopt a good cyber-hygiene and rethink some aspects of their functioning: abandoning the storage of data overseas, developing their own software and operating systems to avoid backdoors and vulnerabilities, encrypt emails. With respect to the overlap between *attacks* and *espionage,* states could also agree on a lowest common denominator: not to carry any operation, regardless of its objective, which could cause human casualties–and, perhaps, the collapse of the whole economy. Paris Call seems to go in the first direction, underlining the need to '[p]revent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure'.[2170]

However–and second–international treaties on cybercrime will develop further. Paradoxically, thus, international law will promote the adoption of municipal legislations prohibiting illegal 'access', 'interception', 'intrusion' or offences against the 'confidentiality' of data–incriminations tackling cyber-espionage, focusing on the individual rather than his possible state of allegiance. As happened with traditional espionage, one will attend a triumph of domestic law. Yet, this corpus is probably less deterrent and efficient with cyber-espionage than it is with traditional spying. States put the life of their agents at risk by sending them on a foreign soil; in addition, their capture constitute a potential discredit and may give the other state considerable bargaining power. Training an agent, giving him a cover, setting up a network of informers is a costly and long process. A balance between risks and advantages is thus vital. With the migration of espionage on the Internet, this balance is upset. Cyber-espionage is cheaper, allows spies to operate in the comfort of their home countries, gives them a potential access to an enormous quantity of information,[2171] and provides states with the priviledge of denying their own spying activites. While states have indicted a growing number of state-sponsored hackers with cyber-espionage,

[2170] Ibid.

[2171] Pun (n.320) 378.

few of them have actually been arrested.[2172] Cybercrime treaties indeed rely on mechanisms of international co-operation (extradition,[2173] mutual assistance),[2174] and it is doubtful whether states will accept to extradite their own agents. For instance, China vigorously reacted after the indictement–by a Court in Pennslvania–of five military hackers, pointing at 'fabricated facts' and a violation of the 'basic norms governing international relations'. [2175] Domestic law nevertheless retains some value. As underlined by a DOJ official: 'imagine a world in which there are no criminal charges, no detailed, formal allegation of wrongdoing [...] The private sector would be left alone to accuse the guilty, without recourse. What message does that send to a foreign hacker? [...] And even in the cases [...] where we have yet to apprehend a defendant, the charges were never the end of the story: whether it is trade remedies, sanctions, contributions to network defense, or diplomatic efforts to rally likeminded nations to confront an adversary together, all of those charges served a greater purpose'.[2176] These measures may also discourage espionage through a 'name and shame' process,[2177] by highlighting the limits of anonymity in cyberspace and the attribution capacities of a state.

[2172] Michael Birnbaum, William Booth and Ellen Nakashima, 'U.S. and its allies target Russian cyber spies with indictments, public shaming', *WP* (04.10.2018) <www.washingtonpost.com/world/europe/britain-directly-blames-russian-military-intelligence-for-broad-range-of-cyberattacks/2018/10/04/13a3a1f8-c7b6-11e8-9158-09630a6d8725_story.html?utm_term=.5d52406ad31f> accessed:06.11.2018.

[2173] Convention on Cybercrime, arts.22(3), 24.

[2174] Directive On Fighting Cyber Crime Within ECOWAS, art.33.

[2175] Michael Schmidt and David Sanger, '5 in China Army Face U.S. Charges of Cyberattacks', *NYT* (19.05.2014) <www.nytimes.com/2014/05/20/us/us-treads-fine-line-in-fighting-chinese-espionage.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer> accessed:17.11.2018.

[2176] DOJ, 'Deputy Assistant Attorney General Adam Hickey of the National Security Division Delivers Remarks at CyberNextDC' (04.10.2018) <www.justice.gov/opa/pr/deputy-assistant-attorney-general-adam-hickey-national-security-division-delivers-remarks> accessed:06.11.2018.

[2177] Steve Ranger, 'The new weapon against Russian cyber-attacks: Naming and shaming', *ZDNet* (04.10.2018) <www.zdnet.com/article/the-new-weapon-against-russian-cyber-attacks-naming-and-shaming/> accessed:06.11.2018.

Last but not least, some words should be said about the international law of HR. To the extent that it involves a data breach, the right to privacy could indeed be relevant in some instances of cyber-espionage. Yet, some uncertainties remain as to the extraterritorial application and degree of control required in such a case, and will need to be answered in the future. The HRC has for instance started to affirm that 'a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking "at home"' while routing 'data collection and analytical tasks through jurisdictions with weaker safeguards for privacy [...] fails the test of lawfulness'.[2178] Then, 'digital surveillance […] may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure'.[2179] In addition, more and more states affirm that HR should be protected equally in and off cyberspace.[2180] How the right to privacy may benefit legal entities also remains obscure, and states probably oppose this idea. For instance, President Obama offered guarantees to aliens regarding their right to privacy, before highlighting that '[o]ur intelligence agencies will continue to gather information about the intentions of governments–as opposed to ordinary citizens–around the world, in the same way that the intelligence services of every other nation does. We will not apologize simply because our services may be more effective'.[2181]

[2178] HRC, 'The right to privacy in the digital age' (30.06.2014) UN-Doc A/HRC/27/37, [30].

[2179] Ibid [33]-[34].

[2180] See UNGA, 'Developments' (30.06.2014) (n.95) 2 (Australia), 3 (Austria), 17 (Switzerland); UNGA, 'Developments' (19.07.2016) (n.93) 16 (Poland); Croatia (n.933) 22.

[2181] 'Obama's Speech on N.S.A. Phone Surveillance' (n.712).

TABLE OF OFFICIAL DOCUMENTS

I. DOCUMENTS OF STATES

Afghanistan

Afghan Ministry of Communications and Information Technology, 'National Cyber Security of Afghanistan' (2014)
<http://mcit.gov.af/Content/files/National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf>

Australia

Australian Defence Forces, 'Operation Series - Information Activities' (2013) 3.13
<www.defence.gov.au/FOI/Docs/Disclosures/330_1314_Document.pdf>

Australian Department of Defence, *Defence White Paper 2013* (Commonwealth of Australia 2013)

Australian Government/Australian Security Intelligence Organisation, 'ASIO Annual Report 2015-16' (2016)
<www.asio.gov.au/sites/default/files/2016%20ASIO%20Annual%20Report%20UNCLASSIFIED.pdf>

Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy* (Commonwealth of Australia 2016)

Department of the Prime Minister and Cabinet, 'Strong and Secure–A Strategy for Australia's National Security' (2013)
<www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf>

Austria

Bundeskanzleramt, 'Austrian Cyber Security Strategy' (2013)
<www.digitales.oesterreich.gv.at/documents/22124/30428/AustrianCyberSecurityStrategy.pdf/35f1c891-ca99-4185-9c8b-422cae8c8f21>

Bundeskanzleramt**,** 'National ICT Security Strategy Austria' (2012)

<www.digitales.oesterreich.gv.at/documents/22124/30428/National_ICT_Security_Strategy_Austria_2012_print.pdf>

Bangladesh

Ministry of Public Administration, 'National Cybersecurity Strategy' (2014) <www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf>

Belgium

Belgian Ministry of Defence, 'Cyber Security Strategy for Defence' (2014) <www.ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf>

Comité permanent de contrôle des services de renseignement et de sécurité, 'Rapport d'Activités 2000' (2000) <www.comiteri.be/images/pdf/Jaarverslagen/2000%20fr.pdf?phpMyAdmin=97d9ae9d92818b6f252c014a4a05bdfb>

Comité permanent de contrôle des services de renseignement et de sécurité, *Rapport d'Activités 2013* (Intersentia 2014)

Comité permanent de contrôle des services de renseignement et de sécurité, *Rapport d'Activités 2014* (Intersentia 2015)

Brazil

Brazil, 'Statement by H. E. Dilma Rousseff, President of the Federative Republic of Brazil, at the Opening of the General Debate of the 68th Session of the United Nations General Assembly' (24.09.2013), 1-3.

Senado Federal, 'Brazil intends to discuss breach of sovereignty in international bodies' (22.12.2016) <www12.senado.leg.br/internacional/en/2013/brazil-intends-to-discuss-breach-of-sovereignty-in-international-bodies>

Bulgaria

Bulgarian Government, 'White Paper on Defence and the Armed Forces of the Republic of Bulgaria' (2010) <www.mod.bg/en/doc/misc/20101130_WP_EN.pdf>

Canada

Bernier M and Treurniet J, 'CF Cyber Operations in the Future Cyber Environment Concept' (2009)
<http://cradpdf.drdc-rddc.gc.ca/PDFS/unc92/p532776.pdf>

Canada, 'Developments in the Field of Information and Telecommunications in the Context of International Security' (2015)
<https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/08/CanadaISinfull.pdf>

Canadian Army Land Warfare Centre, *No man's land: tech considerations for Canada's future army* (National Defence 2014)

Chief of Defence Staff, 'Law of Armed Conflict at the Operational and Tactical Levels' (2001) B-GJ-005-104/FP-021
<www.fichl.org/fileadmin/_migrated/content_uploads/Canadian_LOAC_Manual_2001_English.pdf>

Department of National Defence, *The Future Security Environment 2013-2040* (National Defence 2014)

House of Commons, Hansard-41 (02.04.2014) 2536

House of Commons, Hansard-41 (02.04.2014) 2538

Public Safety Canada, 'National Cyber Security Strategy' (2018)
<www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>

Public Safety Canada, 'Security and Prosperity in the Digital Age' (2016)
<www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/2016-scrty-prsprty-en.pdf>

Royal Canadian Air Force Commander, *Canadian Forces Aerospace Shape Doctrine 2* (National Defence 2014)

Royal Canadian Air Force Commander, *Doctrine Aérospatiale des Forces Canadiennes-Acquisition de l'Avantage* (Défense Nationale 2014)

Chile

Chilean Government, 'National Cybersecurity Policy' (2017)
<http://ciberseguridad.interior.gob.cl/media/2017/04/NCSP-ENG.pdf>

Chilean Ministry of National Defence, 'Aprueba Política de Ciberdefensa' (2018) DO 42.003
<www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf>

Chilean Ministry of National Defence, 'Ciberdefensa'
<www.defensa.cl/temas-de-contenido/ciberdefensa/>

Chilean Ministry of National Defence, 'Libro de la Defensa Nacional de Chile' (2010)
<www.defensa.cl/libro-de-la-defensa-nacional-de-chile/libro-de-la-defensa-2010/>

China (Popular Republic of)

Ministry of Foreign Affairs of the People's Republic of China, 'Ambassador Liu Xiaoming Gives Interview to BBC Newsnight' (2015)
<www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbd_665378/t1308244.shtml>

Ministry of Foreign Affairs of the People's Republic of China, 'Consultation Between Director-Generals of the Departments of Treaty and Law of Ministries of Foreign Affairs of China and Russia Held in Moscow' (2016)
<www.fmprc.gov.cn/mfa_eng/wjbxw/t1337836.shtml>

Ministry of Foreign Affairs of the People's Republic of China, 'Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on October 13, 2015' (2015)
<www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1305571.shtml>

Ministry of Foreign Affairs of the People's Republic of China, 'International Strategy of Cooperation on Cyberspace' (2017)
<http://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml>

Ministry of National Defence of the People's Republic of China, 'China's National Defense in 2010' (2011)
<http://eng.mod.gov.cn/Database/WhitePapers/2010.htm>

Permanent Mission of the People's Republic of China to the United Nations, 'Statement by Ms. Liu Ying of the Chinese Delegation at the Thematic Debate

on Information and Cyber Security at the First Committee of the 68th Session of the UNGA' (30.10.2013)
<www.china-un.org/eng/hyyfy/t1094491.htm>

Colombia

National Council on Economic and Social Policy, 'Policy Guidelines on Cybersecurity and Cyberdefense' (2011)
<www.sites.oas.org/cyber/Documents/Colombia%20-%20National%20Cybersecurity%20and%20Cyberdefense%20Policy.pdf>

National Council on Economic and Social Policy, 'Política Nacional de Seguridad Digital' (2016)
<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Croatia

Croatia, 'Croatian National Cyber Security Strategy' (2015) OG 108/2015
<www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf>

Security and Intelligence Agency, 'Public Report 2014' (2014)
<www.soa.hr/files/file/Public-Report-2014.pdf>

Cyprus

Office of the Commissioner of Electronic Communications and Postal Regulation, 'Cybersecurity Strategy of the Republic of Cyprus' (2012)
<www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf>

Czech Republic

Czech Ministry of Defence, 'White Paper on Defence' (2011)
<www.army.cz/assets/en/ministry-of-defence/whitepaperondefence2011_1.pdf>

Czech Ministry of Foreign Affairs, 'Security Strategy of the Czech Republic 2015' (2015)
<www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf>

Czech Security Information Service, 'Annual Report of the Security Information Service for 2015' (2016)
<www.bis.cz/vyrocni-zpravaEN890a.html?ArticleID=1104>

National Security Authority, 'National Cyber Security Strategy for the period from 2015 to 2020' (2015)
<www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf>

Denmark

Center for Cybersecurity, 'The Cyber threat against Denmark' (2016)
<https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20-%20The%20cyber%20threat%20against%20Denmark.pdf>

Center for Cybersecurity, 'The Cyber threat against Denmark' (2017)
<https://fe-ddis.dk/cfcs/CFCSDocuments/The%20cyber%20threat%20against%20Denmark%202017.pdf>

Egypt

Egyptian Ministry of Communications and Information Technology, 'National ICT Strategy 2012-2017' (2012)
<http://mcit.gov.eg/Upcont/Documents/ICT%20Strategy%202012-2017.pdf>

Estonia

Estonian Information Board, 'International Security and Estonia' (2016) <www.valisluureamet.ee/pdf/2016-en.pdf>

Ministry of Economic Affairs and Communication**,** 'National Strategy for Cyber and Information Security' (2014)
<www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf>

Finland

Ministry of Defence of Finland, 'Finland's Cyber Security Strategy' (2013)
<www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf>

Ministry of Defence of Finland, 'Guidelines for Developing Finnish Intelligence Legislation' (2015)
<www.defmin.fi/files/3144/GUIDELINES_FOR_DEVELOPING_FINNISH_INTELLIGENCE_LEGISLATION.pdf>

Ministry of Defence of Finland, 'Security Strategy for Society' (2010)
<www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf>

Prime Minister's Office, 'Finnish Security and Defence Policy 2012' (2013)
<http://vnk.fi/documents/10616/1093242/J0113_FinnishSecurity_net.pdf/f7d0b3db-f566-4d32-af19-68a7064e24ee?version=1.0>

SUPO, 'Finnish Security Intelligence Service' (2011)
<www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/26154_2011_Supo-English.pdf?156efc9e4d2ad288>

France

Assemblée Nationale, '1ere séance du 23 février 2000' (2000)
<www.assemblee-nationale.fr/11/cra/1999-2000/2000022315.asp#TopOfPage>

Assemblée Nationale, 'Audition de M. Gérard Araud, représentant permanent de la France auprès des Nations Unies' (12.06.2013) CR No 71
<www.assemblee-nationale.fr/14/pdf/cr-cafe/12-13/c1213071.pdf>

Assemblée Nationale, 'Audition de M. Patrick Calvar' (26.02.2013) CR No 59
<www.assemblee-nationale.fr/14/pdf/cr-cdef/12-13/c1213059.pdf>

AN, 'Audition de M. Pierre Cochard' (1.07.2015) CR No 93
<www.assemblee-nationale.fr/14/pdf/cr-cafe/14-15/c1415093.pdf>

Assemblée Nationale, 'Audition, ouverte à la presse, de M. Louis Schweitzer, commissaire général à l'investissement et Mme Claude Revel, déléguée interministérielle à l'intelligence économique' (16.12.2014) CR No 20
<www.assemblee-nationale.fr/14/pdf/cr-eco/14-15/c1415020.pdf>

Assemblée Nationale, 'Audition du contre-amiral Arnaud Coustillière' (12.06.2013) CR No 79
<www.assemblee-nationale.fr/14/pdf/cr-cdef/12-13/c1213079.pdf>

Assemblée Nationale, 'Avis fait au nom de la Commission de la défense nationale et des forces armées sur le projet de loi (no 2669) relatif au renseignement', No 2691 (31.03.2015)

<www.assemblee-nationale.fr/14/rapports/r2691.asp>

Assemblée Nationale, 'Rapport d'information' (07.10.2014) No 2249
<www.assemblee-nationale.fr/14/rap-info/i2249.asp>

Assemblée Nationale, 'Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016' (02.03.2017)
<www2.assemblee-nationale.fr/static/14/DPR/i4573.pdf>

Assemblée Nationale, 'Surveillance des communications électroniques internationales' (01.10.2015)
<www.assemblee-nationale.fr/14/cri/2015-2016/20160002.asp>

Bockel J, 'Rapport d'Information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense' (18.07.2012) No 681
<www.senat.fr/rap/r11-681/r11-6811.pdf>

'Cyberdéfense - Discours de Jean-Yves Le Drian' (*Ministère de la Défense*, 12.12.2016)
<www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/cyberdefense-discours-de-jean-yves-le-drian-lundi-12-decembre-2016>

Commission du livre blanc, *Défense et Sécurité nationale : le Livre blanc* (Odile Jacob, 2008)

Commission du livre blanc, *French White Paper on Defence and National Security 2013* (Ministère de la Défense/SGA/SPAC 2013)

Gouvernement, 'List of Supporters of the Paris Call for Trust and Security in Cyberspace' (*France Diplomatie*, 2018)
<www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in#sommaire_4>

Gouvernement, 'Paris Call for Trust and Security in Cyberspace (*France Diplomatie*, 12.11.2018)
<www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf>

Gouvernement, 'Sabotage'
<www.gouvernement.fr/risques/sabotage>

Ministère de la Défense, 'Manuel du Droit des Conflits Armés' (2012)

<www.cicde.defense.gouv.fr/IMG/pdf/20130226_np_cicde_manuel-dca.pdf>

Premier Ministre, 'French National Digital Security Strategy' (2015) <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/information-systems-defence-and-security-frances-strategy/view/++widget++form.widgets.file/@@download/NCSS_FR2.pdf >

Sénat, 'Séance du 23 février 2017' (2017) CR No 20S. <www.senat.fr/seances/s201702/s20170223/s20170223.pdf>

Sénat, 'Cyberinterférences dans les processus électoraux - Audition de M. Guillaume Poupard' (01.02.2017) <www.senat.fr/compte-rendu-commissions/20170130/etr.html#toc2>

Secrétariat Général de la Défense et de la Sécurité Nationale, 'Revue stratégique de cyberdéfense' (2018) <www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf>

Germany (Federal Republic of)

Bundeskanzleramt, 'White Paper on German Security Policy and the Future of the Bundeswehr' (2016) <www.bundeswehr.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NzE3MzM1Njc2NDYyMzMyMDIwMjAyMDIw/2016%20White%20Paper.pdf>

Federal Ministry of Defence, 'Law of Armed Conflict Manual' (2013) ZDv 15/2 <www.bmvg.de/resource/blob/16630/ae27428ce99dfa6bbd8897c269e7d214/b-02-02-10-download-manual--law-of-armed-conflict-data.pdf>

Federal Ministry of the Interior, 'Cyber Security Strategy for Germany' (2011) <www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile>

Germany, 'Report on Developments in the Field of Information and Telecommunications in the Context of International Security (RES 69/28)' (2015) <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/08/GermanyISinfull.pdf>

Georgia

Georgia, 'UN General Assembly Resolution 68/243' (2014) <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/07/Georgia.pdf>

Guatemala

Guatemala Ministry of Defence, 'Libro de la Defensa Nacional de la República de Guatemala, Evolución 2015' (2015) <www.mindef.mil.gt/pdf/Libro%20de%20la%20Defensa%20Nacional%20de%20la%20Rep%C3%BAblica%20de%20Guatemala,%20Evolucion%20%202015.pdf>

Hungary

Hungarian Government, 'Government Decision No 1139/2013 on the National Cyber Security Strategy of Hungary' (2013) <www.unodc.org/res/cld/lessons-learned/national_cyber_security_strategy_of_hungary_html/National_Cyber_Security_Strategy_of_Hungary.pdf>

Hungarian Ministry of Defence, 'Hungary's National Military Strategy' (2012) <www.files.ethz.ch/isn/167317/Hungary%202012%20national_military_strategy.pdf>

Hungarian Ministry of Foreign Affairs, 'Hungary's National Security Strategy' (2012) <http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf>

India

India, 'Subject: UNGA Resolution 70-237 entitled–Developments in the field of Information and telecommunications in the context of international security' <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/10/India.pdf>

Indian Ministry of Defence, 'Joint Doctrine Indian Armed Forces' (2017) <http://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf>

Ministry of Electronics and Information Technology, 'National Cyber Security Policy' (2013)
<http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf>

Ireland

Department of Communications, Climate Action and Environment, 'National Cyber Security Strategy 2015-2017' (2015)
<www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf>

Department of Defence, 'White Paper on Defence' (2015) <www.defence.ie/WebSite.nsf/WP2015E>

Israel

Israeli Government, 'Advancing National Cyberspace Capabilities' (07.08.2011) Resolution 3611
<www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf>

Italy

Presidency of the Council of Ministers, 'Italian National Strategic Framework for Cyberspace Security' (2013)
<www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf>

Jamaica

Jamaican Government, 'National Cyber Security Strategy' (2015)
<http://mset.gov.jm/sites/default/files/pdf/Jamaica%20National%20Cyber%20Security%20Strategy.pdf>

Japan

Information Security Policy Council, 'Cybersecurity Strategy' (2013)

<www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf>

Information Security Policy Council, 'International Strategy on Cybersecurity Cooperation' (2013)
<www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf>

Japanese Government, 'Cybersecurity Strategy' (2015)
<www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf>

Japanese Ministry of Defence, 'Defence of Japan 2012' (2012)
<www.mod.go.jp/e/publ/w_paper/pdf/2012/14_Part1_Chapter2_Sec2.pdf>

Japanese Ministry of Defence, 'Defence of Japan 2013' (2013)
<www.mod.go.jp/e/publ/w_paper/pdf/2013/17_Part1_Chapter2_Sec1.pdf>

Japanese Ministry of Defence, 'Defence of Japan 2014' (2014)
<www.mod.go.jp/e/publ/w_paper/pdf/2014/DOJ2014_1-2-5_web_1031.pdf>

Japanese Ministry of Defence, 'Defence of Japan 2015' (2015)
<www.mod.go.jp/e/publ/w_paper/pdf/2015/DOJ2015_2-2-1_web.pdf>

Japanese Ministry of Defence, 'Defence of Japan 2016' (2016)
<www.mod.go.jp/e/publ/w_paper/e-book/2016/defense_of_japan_2016.epub>

Jordan

Ministry of Information and Communications Technology, 'National Information Assurance and Cyber Security Strategy (NIACSS)' (2012)
<http://nitc.gov.jo/PDF/NIACSS.pdf>

Kenya

Kenyan Ministry of ICT, 'National Cybersecurity Strategy' (2014)
<http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf>

Korea (Republic of)

'Report by the Republic of Korea' (2016)

<https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/08/ROKISinfull.pdf>

Latvia

Latvian Government, 'Cyber Security Strategy of Latvia 2014-2018' (2014) <www.unodc.org/res/cld/lessons-learned/lva/cyber_security_strategy_of_latvia_2014-2018_html/Cyber_Security_Strategy_of_Latvia.pdf>

Security Police, 'Annual report about the activities of the Security Police in 2015' (2016) <http://dp.gov.lv/en/?rt=documents&ac=download&id=15>

Security Police, 'Annual report about the activities of the Security Police in 2016' (2017) <www.dp.gov.lv/en/?rt=documents&ac=download&id=20.>

Lithuania

Lithuanian Government, 'Resolution no 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011-2019' (2011) <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf>

Lithuanian Ministry of National Defence, 'National Security Strategy' (2016) <https://kam.lt/download/57457/2017-nacsaugstrategijaen.pdf>

Lithuanian Ministry of National Defence, 'The World 2030' (2013) <https://kam.lt/download/35262/gl-111_world%202030_elektroninis.pdf>

State Security Department, 'Lithuanian Threat Assessment 2014' (2015) <www.vsd.lt/senoji/Files/Documents/635664369272603750.pdf>

Luxemburg

Gouvernment du Luxembourg, 'Programme gouvernemental 2013' (2013) <www.sante.public.lu/fr/publications/p/programme-gouvernemental-2013/programme-gouvernemental-2013.pdf>

Gouvernement du Luxembourg, 'Stratégie nationale en matière de cyber sécurité' (2011)
<www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Luxembourg_2011_Orig_Fr_CSB_Strat__gie_final_20111122_.pdf>

Gouvernement du Luxembourg, 'Stratégie nationale en matière de cyber sécurité II' (2015)
<https://cybersecurite.public.lu/content/dam/cybersecurite/fr/lu-ncss-2-fr-booklet.pdf>

Gouvernement du Luxembourg, 'Stratégie nationale en matière de cyber sécurité III' (2018)
<https://cybersecurite.public.lu/content/dam/cybersecurite/fr/cyber3-bro-2018-def-fr.pdf>

Malta

Ministry for Competitiveness and Digital Maritime and Services Economy, 'Malta Cyber Security Strategy' (2016)
<https://mita.gov.mt/en/maltacybersecuritystrategy/Documents/Mita%20_Malta%20Cyber%20Security%20Strategy%20-%20Book.pdf>

Mauritius

Republic of Mauritius, 'National Cyber Security Strategy 2014-2019' (2014)
<http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf>

Mexico

Mexican Government, 'Estrategia Nacional de Ciberseguridad' (2017)
<www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf>

Presidencia, 'Programa Sectorial de Defensa Nacional 2013-2018' (2013)
<www.sedena.gob.mx/archivos/psdn_2013_2018.pdf>

Presidencia, 'CLAN 2016 Seguridad y Defensa' (2016)
<www.gob.mx/presidencia/documentos/clan2016-seguridad-y-defensa>

Montenegro

Montenegrin Government, 'National Cyber Security Strategy for Montenegro 2013-2017' (2013)
<www.unodc.org/res/cld/lessons-learned/national-cyber-security-strategy-for-montenegro-2013-2017_html/National_Cyber_Security_Strategy_for_Montenegro_2013-2017.pdf>

Morocco

Administration de la Défense Nationale, 'Stratégie Nationale en matière de Cybersécurité' (2012)
<www.dgssi.gov.ma/dgssi_assets/user_upload/STRATEGIE_NATIONALE.pdf>

New Zealand

Department of the Prime Minister and Cabinet, 'New Zealand's Cyber Security Strategy' (2015)
<www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-action-plan-december-2015.pdf>

Cullen M and Reddy P, 'Intelligence and Security in a Free Society' (2016) G.24a
<www.parliament.nz/resource/en-nz/51dbhoh_pap68536_1/64eeb7436d6fd817fb382a2005988c74dabd21fe>

New Zealand Government, 'New Zealand's Cyber Security Strategy' (2011)
<www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/nzcybersecuritystrategyjune2011_0.pdf>

New Zealand Security Intelligence Service, 'Annual Report for the year ended 30 June 2013' (2013) G.35
<www.nzsis.govt.nz/assets/media/annual-reports/nzsis-ar13.pdf>

New Zealand Security Intelligence Service, 'Annual Report for the year ended 30 June 2014' (2014) G.35
<www.nzsis.govt.nz/assets/media/annual-reports/nzsis-ar14.pdf>

New Zealand Security Intelligence Service, '2016 Annual Report' (2016) G.35
<www.nzsis.govt.nz/assets/media/annual-reports/nzsis-ar16.pdf>

The Netherlands

Advisory Council of International Affairs, 'Cyber Warfare - Conclusions and recommendations' (21.03.2012)
<https://aiv-advies.nl/6ct/publications/advisory-reports/cyber-warfare>

Advisory Council of International Affairs/Advisory Committee on Issues of Public International Law, 'Cyber Warfare' (2011) 22/77
<https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf>

Dutch Government, 'Building Digital Bridges' (2017) AVT17/BZ122203
<www.government.nl/binaries/government/documents/parliamentary-documents/2017/02/12/international-cyber-strategy/International+Cyber+Strategy.pdf>

Dutch Government, 'Government response to the AIV/CAVV report on cyber warfare' (2012)
<www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf>

Dutch Government, 'International Security Strategy' (2013)
<www.government.nl/binaries/government/documents/policy-notes/2013/06/21/international-security-strategy/ivs-engels.pdf>

Dutch Ministry of Defence, '2013 Annual Report, Netherlands Defence Intelligence and Security Service' (2014)
<www.government.nl/documents/annual-reports/2014/06/30/annual-report-2013-netherlands-defence-intelligence-and-security-service>

Dutch Ministry of Defence, 'The Defence Cyber Strategy' (2012)
<www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf>

General Intelligence and Security Services, 'Analysis of vulnerability to espionage' (2011)
<https://english.aivd.nl/binaries/aivd-en/documents/publications/2011/01/13/aivd-analysis-of-vulnerability-to-espionage/aivd-analysis-of-vulnerability-to-espionage.pdf>

General Intelligence and Security Services, 'Annual Report 2006' (2007)
<https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2007/06/20/annual-report-2006/20070872jv2006-en.pdf>

General Intelligence and Security Services, 'Annual Report 2015' (2016) <https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2016/05/26/annual-report-2015-aivd/annual-report-2015-aivd.pdf>

General Intelligence and Security Services, 'Annual Report 2016' (2017) <https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2017/04/04/annual-report-2016/AIVD+Annual+Report+2016.pdf>

General Intelligence and Security Services, 'Annual Report 2017' (2018) <https://english.aivd.nl/publications/annual-report/2018/03/09/annual-report-2017-aivd>

Kingdom of the Netherlands, 'Developments in the field of information and telecommunications in the context of international security' (2015) <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/08/NetherlandsISinfull.pdf>

Koenders B, 'Speech Tallinn Manual 2.0' (2017) <www.rijksoverheid.nl/binaries/rijksoverheid/documenten/toespraken/2017/02/13/toespraak-minister-koenders-bij-presentatie-tallinn-manual-2.0/Speech+TALLINN+MANUAL+2.0.pdf>

Military Intelligence and Security Service, '2013 Annual Report' (2014) <www.government.nl/binaries/government/documents/annual-reports/2014/06/30/annual-report-2013-netherlands-defence-intelligence-and-security-service/web-jaarverslag-2013-mivd-eng.pdf>

Military Intelligence and Security Service, '2014 Annual Report' (2015) <www.government.nl/binaries/government/documents/annual-reports/2015/07/21/2014-annual-report-netherlands-defence-intelligence-and-security-service/mivd-openbaar-jaarverslag-2014-engels.pdf>

Ministry of Security and Justice/National Cyber Security Centrum, 'Cyber Security Assessment Netherlands 2014' (2014) <www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2014/1/Cyber%2BSecurity%2BAssessment%2BNetherlands%2B2014.pdf>

Ministry of Security and Justice/National Cyber Security Centrum, 'Cyber Security Assessment Netherlands 2016' (2016) <www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2016/1/CSAN2016.pdf>

Ministry of Security and Justice/National Cyber Security Centrum, 'Cyber Security Assessment Netherlands 2017' (2017) <www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2017/1/CSAN2017.pdf>

Nigeria

Office of the National Security Adviser, 'National Cybersecurity Strategy' (2017) <https://tekedia.com/wp-content/uploads/2017/04/ncss-STRATEGY.pdf>

Norway

Norway Ministries, 'Cyber Security Strategy for Norway' (2012) <www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf>

Norwegian Defence Command and Staff College, *Norwegian Armed Forces Joint Operational Doctrine* (The Defence Staff 2007)

Norwegian Parliamentary Intelligence Oversight Committee, 'Abbreviated annual report for 2013' (2014) <https://eos-utvalget.no/english_1/annual_reports/content_3/text_1401199189882/1403522809228/forkortet_rsmelding_engelsk_versjon.pdf>

Norwegian Parliamentary Intelligence Oversight Committee, 'The Norwegian Intelligence Service' <https://eos-utvalget.no/english_1/services/the_eos_services/the_norwegian_intelligence_service/>

Paraguay

Gobierno Nacional, 'Plan Nacional de Ciberseguridad' (2016) <http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg>

Philippines

Department of Information and Communications Technology, 'National Cybersecurity Plan 2022' (2017)

<www.dict.gov.ph/wp-content/uploads/2017/04/FINAL_NationalCyberSecurityPlan2022.pdf>

Office of the President, 'National Cyber Security Plan' (2004) <www.dict.gov.ph/wp-content/uploads/2014/07/Cyber-Plan-Pre-Final-Copy_.pdf>

Poland

Ministry of Administration and Digitisation, 'Cyberspace Protection Policy of the Republic of Poland' (2013) <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf>

National Security Bureau, 'National Security Strategy of the Republic of Poland' (National Security Bureau 2014) <www.bbn.gov.pl/ftp/dok/NSS_RP.pdf>

Qatar

Ministry of Transport and Communications, 'Qatar National Cyber Security Strategy' (2014) <www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf>

Russian Federation

Ministry of Foreign Affairs of the Russian Federation, 'Foreign Minister Sergey Lavrov's address and answers to questions at the 53rd Munich Security Conference, Munich, February 18, 2017' (2017) <www.mid.ru/en/web/guest/meropriyatiya_s_uchastiem_ministra/-/asset_publisher/xK1BhB2bUjd3/content/id/2648249>

Ministry of Foreign Affairs of the Russian Federation, 'Foreign Minister Sergey Lavrov's interview with Kurdish television channel Rudaw' (2017) <www.mid.ru/en/press_service/minister_speeches/-/asset_publisher/7OvQR5KJWVmR/content/id/2822361>

Ministry of Foreign Affairs of the Russian Federation, 'Foreign Minister Sergey Lavrov's remarks and answers to media questions at the Primakov Readings International Forum' (2017) <www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3239504>

Russian Government, Order 'On signing the Agreement between the Government of the Russian Federation and the Government of the people's Republic of China on cooperation in ensuring international information security' (30.04.2015) No 788-p

Russian Ministry of Defence, 'Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space' (2011) <www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf>

Russian Ministry of Defence, 'Russian Federation Armed Forces' Information Space Activities Concept' (2000) <http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle>

Security Council of the Russian Federation, 'Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020' (2013) <www.ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf>

Rwanda

Ministry of Information Technology and Communications, 'National Cyber Security Policy' (2015) <www.mitec.gov.rw/fileadmin/Documents/Policies/Rwanda_Cyber_Security_Policy.pdf>

Saudi Arabia

Ministry of Communications and Information Technology of Saudi Arabia, 'Developing National Information Security Strategy for the Kingdom of Saudi Arabia' (2013) <hwww.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-of-saudi-arabia/view/++widget++form.widgets.file/@@download/NCSS_Saudi+Arabia_draft_EN.pdf>

Senegal

Ministry of Post and Telecommunications, 'Stratégie Sénégal Numérique 2016-2025' (2016)

<www.sec.gouv.sn/sites/default/files/Strat%C3%A9gie%20S%C3%A9n%C3%A9gal%20Num%C3%A9rique%202016-2025.pdf>

Singapore

Cyber Security Agency, 'Singapore's Cybersecurity Strategy' (2016) <www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf>

Slovakia

Slovakian Ministry of Defence, 'The White Paper on Defence of the Slovak Republic' (2013) <www.mosr.sk/data/WP2013.pdf>

Slovakian Ministry of Defence, 'White Paper on Defence of the Slovak Republic' (2016) <www.mosr.sk/data/WPDSR2016_LQ.pdf>

Slovak Republic, 'National Strategy for Information Security in the Slovak Republic' (2008) <www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Slovakia_National_Strategy_for_ISEC.pdf>

Slovenia

Republic of Slovenia, 'Cyber Security Strategy' (2016) <www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf>

Slovenian National Assembly, *Resolution on the National Security Strategy of the Republic of Slovenia* (Ministry of Defence 2010)

South Africa

South African Defence, 'Defence Review 2015' (2014) <www.dod.mil.za/documents/defencereview/defence%20review%202015.pdf>

State Security Agency, 'National Cybersecurity Policy Framework for South Africa' (2015) <www.gov.za/sites/www.gov.za/files/39475_gon609.pdf>

Spain

Spanish Government, 'Estrategia de Seguridad Nacional' (2013) <www.dsn.gob.es/sites/dsn/files/Estrategia_Seguriad_Nacional_2017.pdf>

Spanish Government, 'Estrategia de Seguridad Nacional' (2017) <www.dsn.gob.es/sites/dsn/files/2017_Spanish_National_Security_Strategy_0.pdf>

Spanish Government, 'Informe Anual de Seguridad Nacional' (2013) <www.dsn.gob.es/sites/dsn/files/Informe_Seguridad_Nacional%202013.pdf>

Sweden

Prime Minister's Office, 'Finnish Security and Defence Policy 2012' (2013) <www.bbn.gov.pl/ftp/dok/07/FIN_Finnish_Security_Defence_Policy_2012_Government_Report.pdf>

Prime Minister's Office, 'National Security Strategy' (2017) <www.government.se/4aa5de/contentassets/0e04164d7eed462aa511ab03c890372e/national-security-strategy.pdf>

SAPO, *Swedish Security Service 2010* (Davidsons 2011)

SAPO, *Swedish Security Service 2013* (Edita 2014)

Sweden, 'Submission by Sweden to UNGA resolution 68/243 entitled "Developments in the field of information and telecommunications in the context of international security"' (12.09.2014) <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/10/Sweden.pdf>

Switzerland

Answer Guy Parmelin' to 'Question Glättli Balthasar. Surveillance d'autorités et d'agents publics suisses par le service de renseignement allemand' (07.03.2016) 16.5046 <www.parlament.ch/fr/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=36720>

'Avis du Conseil Fédéral' to 'Motion Evi Alleman. Affaire Snowden - Accord de non-espionnage avec les Etats-Unis' (19.02.2014) 13.4165 <www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20134165>

Delegation of Management Commissions, 'Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet «Onyx»)' (10.11.2003) 1404-5 <www.admin.ch/opc/fr/federal-gazette/2004/1377.pdf>

Federal Department of Defence, Civil Protection and Sport, 'National Strategy for Switzerland's Protection against Cyber Risks' (2012) <www.isb.admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/Strategie%20zum%20Schutz%20der%20Schweiz%20vor%20Cyber-Risiken.pdf.download.pdf/Strategie_zum_Schutz_der_Schweiz_vor_Cyber-Risiken_k-ENGL.pdf>

Federal Department of Justice and Police, 'Avis de droit sur les bases légales des opérations dans les réseaux informatiques par les services du DDPS' (2009) <www.parlament.ch/centers/documents/fr/gutachten-ejpd-computernetz-vbs-2009-03-10-f.pdf>

National Council, 'Moratoire sur le vote électronique' (21.09.2017) 17.471 <www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170471>

Trinidad and Tobago

Trinidadian Government, 'National Cyber Security Strategy' (2012) <www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf>

Turkey

Ministry of Transport, Maritime Affairs and Communication, 'National Cyber Security Strategy and 2013-2014 Action Plan' (2013) <www.unodc.org/res/cld/lessons-learned/national_cyber_security_strategy_and_2013-2014_action_plan_html/National_Cyber_Security_Strategy_and_2013-2014_Action_Plan.pdf>

Ministry of Transport, Maritime Affairs and Communication, '2016-2019 National Cyber Security Strategy' (2016)
<www.udhb.gov.tr/doc/siberg/UlusalSibereng.pdf>

United Kingdom

Cabinet Office, 'Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space' (June 2009)
<www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf>

Cabinet Office, 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world' (2011)
<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>

Foreign and Commonwealth Office, 'Response to General Assembly resolution 71/28 "Developments in the field of information and telecommunications in the context of international security"' (July 2017)
<https://s3.amazonaws.com/unoda-web/wp-content/uploads/2017/09/UK-ES-and-full.pdf>

Intelligence and Security Committee of Parliament, *Annual Report 2011-2012* (TSO 2012)

House of Lords Deb 14 October 2010, vol 721, col 688

Ministry of Defence, 'Cyber Primer' (2016)
<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf>

Ministry of Defence, 'Land Operations' (2017)
<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/605298/Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web.pdf>

Ministry of Defence, 'The Joint Service Manual of the Law of Armed Conflict (2004) JSP 383

National Cyber Security Centre, 'The principles of supply chain security' (28.01.2018)
<www.ncsc.gov.uk/guidance/principles-supply-chain-security>

UK, 'Response to General Assembly resolution 68/243 "Developments in the field of information and telecommunications in the context of international security"' (2014)
<https://ccdcoe.org/sites/default/files/documents/UN-14XXXX-ITISreplyUK.pdf>

UK Government, 'Interception of Communications Code of Practice' (2015)
<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf>

UK Government, 'National Cyber Security Strategy 2016-2021' (2016)
<www.ncsc.gov.uk/content/files/protected_files/document_files/National%20Cyber%20Security%20Strategy%20v20.pdf>

UK Government, 'New cyber reserve unit created' (29.09.2013)
<www.gov.uk/government/news/reserves-head-up-new-cyber-unit>

United States of America

Brennan J, 'Strengthening our Security by Adhering to our Values and Laws' (16.09.2011)
<www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an>

Carter A, 'Rewiring the Pentagon: Charting a New Path on Innovation and Cybersecurity' (2015)
<http://archive.defense.gov/speeches/speech.aspx?SpeechID=1935>

Central Intelligence Agency, 'Unclassified Version of March 6, 2015 Message to the Workforce from CIA Director John Brennan: Our Agency's Blueprint for the Future'
<https://www.cia.gov/news-information/press-releases-statements/2015-press-releases-statements/message-to-workforce-agencys-blueprint-for-the-future.html>

Committee on Foreign Relations of the Senate, 'Convention on the Law of the Sea' (2007) Exec Rept 110-9
<www.congress.gov/110/crpt/erpt9/CRPT-110erpt9.pdf>

Department of Defense, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012' (2012)
<www.defense.gov/Portals/1/Documents/pubs/2012_CMPR_Final.pdf>

Department of Defense, 'Joint Terminology for Cyberspace Operations' (2010-2011)
<www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf>

Department of Defense, 'Summary of the 2018 National Defense Strategy' (2018)
<www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>

Department of Defense Cyberspace Policy Report, 'A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934' (2011)
<https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf>

Department of Defense/Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations' (1999)
<www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf>

Department of Defense/Office of General Counsel, 'An Assessment of International Legal Issues in Information Operations' (2nd edn, 1999)
<https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-013.pdf>

Department of Defense /Office of General Counsel, 'Department of Defense Law of War Manual' (2015, updated 2016)
<www.defense.gov/Portals/1/Documents/law_war_manual15.pdf>

Department of Justice, 'Deputy Assistant Attorney General Adam Hickey of the National Security Division Delivers Remarks at CyberNextDC' (04.10.2018)
<www.justice.gov/opa/pr/deputy-assistant-attorney-general-adam-hickey-national-security-division-delivers-remarks>

Department of Justice, 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage' (19.05.2014)
<www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>

Department of the Navy, 'Implementing Instruction for Information Warfare Command and Control Warfare' (18.01.1995) 3420.260
<www.hsdl.org/?view&did=439853>

Egan B, 'Remarks on International Law and Stability in Cyberspace' (10.11.2016)

<https://2009-2017.state.gov/s/l/releases/remarks/264303.htm>

Government Accountability Office, 'Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates' (2011)
<www.gao.gov/assets/100/97674.pdf>

Government Publishing Office, 'Schumer calls on U.S. Trade Rep to file WTO Suit in Response to Chinese Cyber-Attacks' (22.05.2014).
Accessed via Factiva <https://global.factiva.com>

Hongju Koh H, 'International Law in Cyberspace', USCYBERCOM Inter-Agency Legal Conference in Fort Meade (18.09.2012)
<http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers>

House of Representatives, 'A bill to support US international cyber diplomacy' (introduced by Mr Royce) (2017) 115th Congress, 1st session

House of Representatives, Committee on Oversight and Government Reform, 'The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation' (07.09.2016)
<https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf>

Hsu K and Murray C, 'China International Law in Cyberspace' (2015)
<www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf>

Joint Chiefs of Staff, 'Cyberspace Operations' (2013) JP 3-12
<www.hsdl.org/?view&did=758858>

National Security Council Intelligence Committee, 'Directive No 9 Revised' (1952)
<https://history.state.gov/historicaldocuments/frus1950-55Intel/d257>

Office of the Historian, 'Directive No 9 Revised' (1952)
<history.state.gov/historicaldocuments/frus1950-55Intel/d257>

Tenet G, 'Remarks as prepared for delivery by Director of Central Intelligence George J. Tenet at Georgetown University' (05.02.2004)
<http://nsarchive.gwu.edu/NSAEBB/NSAEBB80/Remarks%20as%20prepared%20for%20delivery%20by%20Director%20of%20Central%20Intelligence

%20George%20J_%20Tenet%20at%20Georgetown%20University%20February%205,%202004.htm>

The White House, 'International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World' (2011)
<https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

The White House, 'National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23' (2008)
<https://fas.org/irp/offdocs/nspd/nspd-54.pdf>

The White House, 'President Xi Jinping's State Visit to the United States' (25.09.2015)
<https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>

The White House, 'Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment' (29.12.2016)
<https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity>

The Judge Advocate General's Legal Center and School, 'Information Operations and Cyberspace Operations' (2015)
<www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf>

The Judge Advocate General's Legal Center and School, 'Operational Law Handbook' (2015)
<www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdfpdf>

The Judge Advocate General's Legal Center and School, 'Operational Law Handbook' (17th edn, 2017)
<www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2017.pdf>

United States, *Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary House of Representatives, Ninety-Fourth Congress, Second Session 94 Congress on Foreign Intelligence Surveillance Act, April 12, May 5 and June 2, 1976, Serial No 65* (GPO 1977)
<https://babel.hathitrust.org/cgi/pt?id=mdp.39015005012367;view=1up;seq=3>

United States, *Hearings before the Subcommittee on Intelligence and the Rights of Americans of the Select Committee on Intelligence of the United States Senate, Ninety-Fifth Congress, Second session on S. 1566, Foreign Intelligence Surveillance Act of 1978, July 12, 21 and February 8, 24, 27, 1978* (GPO 1978)
<www.intelligence.senate.gov/sites/default/files/hearings/s1566.pdf>

United States, *Hearings before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary House of Representatives, Ninety-Fourth Congress, Second session on H.R. 7308 Foreign Intelligence Surveillance Act, June 22, 28 and 29, 1978, Serial No 48* (GPO 1978)
<https://babel.hathitrust.org/cgi/pt?id=mdp.39015005012292;view=1up;seq=3>

United States Computer Emergency Readiness Team, 'Alert (TA14-353A)-Targeted Destructive Malware' (30.09.2016)
<www.us-cert.gov/ncas/alerts/TA14-353A>

US House Committee on Ways and Means, 'Levin, Rangel to USTR: Consider Designating China "Priority Foreign Country" for Alleged Trade Secrets Theft' (28.03.2013)
<https://democrats-waysandmeans.house.gov/media-center/press-releases/levin-rangel-ustr-consider-designating-china-priority-foreign-country>

Bilateral/Multilateral

G7, 'G7 declaration on responsible states behavior in cyberspace' (2017)
<www.g7italy.it/sites/default/files/documents/Declaration_on_cyberspace_0.pdf>

'Joint statement by Prime Minister Stefan Löfven and Prime Minister Narendra Modi' (2016)
<www.government.se/statements/2016/02/joint-statement-by-prime-minister-stefan-lofven-and-prime-minister-narendra-modi/>

'New Zealand - United Kingdom Joint Statement on Cyber Security' (15.01.2013)
<www.gov.uk/government/news/new-zealand-united-kingdom-joint-statement-on-cyber-security--2>

Non-Aligned Movement, 'Final Document' (2016)
<http://cns.miis.edu/nam/documents/Official_Document/XVII-NAM-Summit-Final-Outcome-Document-ENG.pdf>

'Settlement of Claim between Canada and the USSR for Damage Caused by "Cosmos 954"' (02.04.1981)
<www.spacelaw.olemiss.edu/library/space/International_Agreements/Bilateral/1981%20Canada-%20USSR%20Cosmos%20954.pdf>

'US–Nordic Leaders' Summit, Joint Statement' (13.05.2016)
<https://obamawhitehouse.archives.gov/the-press-office/2016/05/13/us-nordic-leaders-summit-joint-statement>

II. DOCUMENTS OF INTERNATIONAL ORGANIZATIONS

Community of Latin American and Caribbean States (CELAC)

Statement by the Permanent Mission of Costa Rica to the UN on behalf of CELAC, 'Consideration of effective measures to enhance the protection, security and safety of diplomatic and consular missions and representatives' (2014)
<www.un.int/costarica/statements_speeches/consideration-effective-measures-enhance-protection-security-and-safety>

European Union (EU)

European Commission, 'Dual-use trade control'
<https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/>

European Commission, 'Joint Communication of the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity strategy of the European Union - An Open, Safe and Secure Cyberspace' (2013)
<https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf>

European Parliament, 'Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy' (2013) 2013/2682 RSP
<www.europarl.europa.eu/meetdocs/2009_2014/documents/ta/04/07/2013%20-%200322/p7_ta-prov(2013)0322_fr.pdf>

Mercado Común del Sur (MERCOSUR)

MERCOSUR, 'Decisión de Mercosur sobre el rechazo al espionaje por parte de los Estados Unidos' (2013) <www.mercosur.int/innovaportal/file/4506/1/decision_sobre_espionaje_es.pdf>

North Atlantic Treaty Organization (NATO)

NATO, *NATO Glossary of Terms and Definitions* (2013) AAP-06 <http://wcnjk.wp.mil.pl/plik/file/N_20160219_AAP6EN.pdf>

United Nations (UN)

Human Rights Committee (HRC)

Human Rights Committee, 'The right to privacy in the digital age' (30.06.2014) UN–Doc A/HRC/27/37

International Law Commission (ILC)

International Law Commission, 'Chapter V – Identification of customary international law' (2016) UN–Doc A/71/10

International Law Commission, 'Subsequent agreements and subsequent practice in relation to the interpretation of treaties' (2013) UN–Doc A/68/10

International Law Commission, 'Subsequent agreements and subsequent practice in relation to the interpretation of treaties' (2016) UN–Doc A/71/10

Humphrey Waldock, 'Third Report on the law of treaties' (1964) UN-Doc A/CN.4/167

Humphrey Waldock, 'Fifth Report on the Law of Treaties' (1965-6) UN–Doc A/CN.4/183

Michael Wood, 'First report on formation and evidence of customary international law' (2013) UN–Doc A/CN.4/663

Michael Wood, 'Second report on formation and evidence of customary international law' (2013) UN–Doc A/CN.4/672

Michael Wood, 'Third report on identification of customary international law' (2015) UN–Doc A/CN.4/682

Press releases and meeting coverages

International Trade Law Body Highlights Finalized Texts on Secured Transactions, Arbitration, Online Dispute Resolution, as Sixth Committee Takes Up Report', UN meeting coverage GA/L/3523 (10.10.2016) <www.un.org/press/en/2016/gal3523.doc.htm>

'Speakers Conclude Debates on Diplomatic Protection, Geneva Convention Additional Protocols, Protection of Missions', UN meeting coverage (10.10.2016) <www.un.org/press/en/2016/gal3523.doc.htm>

'Third Committee Approves Text Titled "Right to Privacy in the Digital Age", as It Takes Action on 18 Draft Resolutions' (2013) UN Press Release GA/SHC/4094 <www.un.org/press/en/2013/gashc4094.doc.htm>

Publications

(1996) 2 Y.B.I.L.C

UNCIO, Vol VI (1945), 558-9 <http://digitallibrary.un.org/record/1300969/files/UNIO-Volume-6-E-F.pdf>

United Nations General Assembly (UNGA)

United Nations General Assembly, 'Colombia, Cyprus, Ecuador, Ghana, Haiti, Iran, Madagascar, Uganda and Yugoslavia: proposal' (24.03.1969) UN Doc A/AC.134/L.16

United Nations General Assembly, 'Developments in the field of information and telecommunications in the context of international security' (20.07.2010) UN Doc A/65/154

United Nations General Assembly, 'Developments in the field of information and telecommunications in the context of international security' (15.07.2011) UN Doc A/66/152

United Nations General Assembly, 'Developments in the field of information and telecommunications in the context of international security' (16.07.2013) UN Doc A/68/156

United Nations General Assembly, 'Developments in the field of telecommunications in the context of international security' (30.06.2014) UN Doc A/69/112

United Nations General Assembly, 'Developments in the field of information and telecommunications in the context of international security' (08.09.2014) UN Doc A/69/112/Add.1

United Nations General Assembly, 'Developments in the field of information and telecommunications in the context of international security' (22.07.2015) UN Doc A/70/172

United Nations General Assembly, 'Developments in the field of information and telecommunications in the context of international security' (22.07.2015) UN Doc A/70/174

United Nations General Assembly, 'Developments in the field of information and telecommunications in the context of international security' (19.07.2016) UN Doc A/71/172

United Nations General Assembly, 'Developments in the field of information and telecommunications in the context of international security' (11.08.2017) UN Doc A/72/135

United Nations General Assembly, 'Follow-up to the outcome of the Millennium Summit' (02.12.2004) UN-Doc A/59/565

United Nations General Assembly, 'Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (14.09.2011) UN Doc A/66/359

United Nations General Assembly, 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (13.01.2015) UN Doc A/69/723

UNGA Res 2131 (XX) (21.12.1965) [Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty]

UNGA Res 2625 (XXV) (24.10.1970) [Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations]

UNGA Res 3314 (XXIX) (14.12.1974) [Definition of Aggression]

UNGA Res 34/101 (14.12.1979) [Non-interference in the internal affairs of States]

UNGA Res 41/65 (3.12.1986) [Principles relating to remote sensing of the Earth from space]

UNGA Res 69/121 (18.12.2014) [Consideration of effective measures to enhance the protection, security and safety of diplomatic and consular missions and representatives]

United Nations Security Council (UNSC)

UNSC, 858th Meeting (24.05.1960)

UNSC, 859th Meeting (25.05.1960)

UNSC 860th Meeting (26.05.1960)

UNSC Res 138 (23.06.1960) [Question relating to the case of Adolf Eichmann]

UNSC Resolution 487 (1981)

Unión de Naciones Suramericanas (UNASUR)

Unión de Naciones Suramericanas, 'Declaración de Paramaribo' (30.08.2013) <https://repo.unasursg.org/alfresco/service/unasursg/documents/content/SEPTIMA_REUNION_ORDINARIA_DEL_CONSEJO_DE_JEFAS_Y_JEFES_DE_ESTADO_Y_DE_GOBIERNO_DE_LA_UNION_DE_NACIONES_SURAMERICANAS__DECLARACION_DE_PARAMARIBO.pdf?noderef=36d7df26-5630-485a-8f1a-02a7341ecc8a>

Other Organizations

World Trade Organization, 'Interpretation and Application of Article 39'

<www.wto.org/english/res_e/booksp_e/analytic_index_e/trips_03_e.htm#article39>

International Organization for Standardization, 'Information Technology–Open Systems Interconnection–Basic Reference Model: The Basic Model' (1994) ISO/IEC7498-1
<https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip>

International Organization for Standardization, 'Information technology - Security techniques - Guidelines for cybersecurity' (2012) BS ISO/IEC 27032:2012
<www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en>

Wassenaar Arrangement Secretariat, 'List of Dual-Use Goods and Technologies and Munitions List' (2017) Public Doc Vol II, 4.D.4
<www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf>

BIBLIOGRAPHY

I. YEARBOOKS AND DIGESTS

Annuaire Français de Droit International (A.F.D.I.)

Charpentier J, 'Pratique Française du Droit International–1983' (1983) 29 A.F.D.I. 850

Lachaume J-F, 'Jurisprudence française concernant le droit international public - année 1969' (1970) 16 A.F.D.I. 875

Lachaume J-F, 'Jurisprudence française concernant le droit international public– Année 1972' (1973) 19 A.F.D.I. 974

Lachaume J-F, 'Jurisprudence française concernant le droit international public (Année 1985)' (1986) 32 A.F.D.I. 923

Lachaume J-F, 'Jurisprudence française relative au droit international' (1989) 35 A.F.D.I. 842

Australian Yearbook of International Law (Australian Y.B.I.L.)

Cavenagh J, 'Australian Practice in International Law 2004' (2006) 25 Australian Y.B.I.L. 463

Chapman A and Kealey S, 'Australian Practice in International Law 2011' (2013) 31 Australian Y.B.I.L. 285

Baltic Yearbook of International Law (B.Y.B.I.L.)

Vark R, 'Republic of Estonia Materials on International Law 2009' (2010) 10 B.Y.B.I.L. 203

Canadian Yearbook of International Law (Canadian Y.B.I.L.)

Legault L, 'Canadian Practice in International Law during 1979 as Reflected Mainly in Public Correspondence and Statements of the Department of External Affairs' (1980) 18 Canadian Y.B.I.L. 301

Swords C, 'Canadian Practice in International Law - At the Department of Foreign Affairs and International Trade in 2002-3' (2003) 41 Canadian Y.B.I.L. 443

Van Ert G, 'Canadian Cases in Public International Law in 2009-10' (2010) 48 Canadian Y.B.I.L. 493

Department of State Bulletin (Dep't St Bull)

(1960) 42 Dep't St Bull 809

(1960) 42 Dep't St Bull 849

(1960) 43 Dep't St Bull 157

(1960) 43 Dep't St Bull 233

Digest of United States Practice in International Law

Cummin S, *Digest of United States Practice in International Law 2004* (ILI 2006)

Cummins S and Stewart D, *Digest of United States Practice in International Law 2001* (ILI 2002)

Cummins S and Stewart D, *Digest of United States Practice in International Law 2003* (ILI 2004)

Guymon C, 'Digest of United States Practice in International Law 2014' <www.state.gov/documents/organization/244504.pdf>

Irish Yearbook of International Law (Irish Y.B.I.L.)

'Department of Foreign Affairs Statement of Strategy 2008-10' (2008) 3 Irish Y.B.I.L. 263

Foreign Relations of the United States (F.R.U.S.)

'Eastern Europe Region, Soviet Union, Cyprus' (1958-1960) X(1) F.R.U.S. <https://history.state.gov/historicaldocuments/frus1958-60v10p1/d147>

'Minutes of the Thirty-Eighth Meeting of the United States Delegation' (14.05.1945) 1 F.R.U.S.

<https://history.state.gov/historicaldocuments/frus1945v01/d226>

'Minutes of the Forty-Eighth Meeting (Executive Session) of the United States Delegation' (20.05.1945) 1 F.R.U.S.
<https://history.state.gov/historicaldocuments/frus1945v01/d243>

Japanese Annual of International Law (J.A.I.L.)/Japanese Yearbook of International Law (Japanese Y.B.I.L.)

Furuya S and Konaka S, 'Chronology of Japanese Foreign Affairs in 2008' (2009) 52 Japanese Y.B.I.L. 704

Oda S and Owada H, 'Annual Review of Japanese Practice in International Law XII (1973)' (1982) 25 J.A.I.L. 73

Keesing's Contemporary Archives/Keesing's Record of World Events (Keesings)

(1940) III-IV(10) Keesings, 4279

(1940) III-IV(12) Keesings, 4186

1941 IV(11) Keesings, 4887

(1942) IV(3) Keesings, 5079

(1942) IV(12) Keesings, 5335

(1943) IV-V(10) Keesings, 6057

(1944) V(10) Keesings, 6789

(1945) V(1) Keesings, 6970

(1945) V(3) Keesings, 7063

(1949) VII(4) Keesings, 9945

(1949) VII(12) Keesings, 10201

(1950) VII-VIII(1) Keesings, 10481

(1950) VII-VIII(3) Keesings, 10661

(1951) VIII(4) Keesings, 11401

(1951) VIII(12) Keesings, 11883

(1953) IX(1) Keesings, 12685

(1953) IX(1) Keesings, 12728

(1953) IX(3) Keesings, 12843

(1953) IX(10) Keesings, 13212

(1954) IX(12) Keesings, 13772

(1956) X(2) Keesings, 14700

(1960) 6(5) Keesings, 17437

(1960) 6(6) Keesings, 17498

(1960) 6(7) Keesings, 17551

(1960) 6(10) Keesings, 17724

(1961) 7(2) Keesings, 17910

(1961) 7(12) Keesings, 18279

(1962) 8(2) Keesings, 18584

(1962) 8(12) Keesings, 18951

(1963) 9(11) Keesings, 19744

(1968) 14(3) Keesings, 22585

(1969) 15(1) Keesings, 23120

(1973) 19(2) Keesings, 25711

(1974) 20(3) Keesings, 26389

(1974) 20(7) Keesings, 26595

(1979) 25(10) Keesings, 29874

(1982) 28(5) Keesings, 31512

(1982) 28(10) Keesings, 31784

(1984) 30(12) Keesings, 33086

(1985) 31(11) Keesings, 33991

(1986) 32(7) Keesings, 34505

(1987) 33(11) Keesings, 35543

(1988) 34(6) Keesings, 35991

(1989) 35(4) Keesings, 36601

(1996) 42(4) Keesings, 41071

(1998) 44(12) Keesings, 42445

(2001) 47(3) Keesings, 44072

(2002) 48(11) Keesings, 45086

(2004) 50(7) Keesings, 46124

(2005) 51(6) Keesings, 46692

(2007) 53(4) Keesings, 47881

(2007) 53(4) Keesings, 47896

(2010) 56(12) Keesings, 49994

(2013) 59(2) Keesings, 52489

(2013) 59(5) Keesings, 52668

(2013) 59(5) Keesings, 52676

(2013) 59(5) Keesings, 52686

(2013) 59(11) Keesings, 53009

(2014) 60(4) Keesings, 53287

(2014) 60(5) Keesings, 53371

Netherlands Yearbook of International Law (Netherlands Y.B.I.L.)

Barnhoorn LANM, 'Netherlands Judicial Decisions involving Questions of Public International Law 1974–1975' (1976) 7 Netherlands Y.B.I.L. 303

Barnhoorn LANM, 'Netherlands Judicial Decisions involving Questions of Public International Law 1982–1983' (1984) 15 Netherlands Y.B.I.L. 423

Swan Sik K, 'Netherlands State Practice for the Parliamentary Year 1969–1970' (1971) Netherlands Y.B.I.L. 136

Revue Suisse de Droit International et Européen/Swiss Review of International and European Law (R.S.D.I.E.)

Caflisch L, 'La Pratique Suisse en Matière de Droit International Public 1992' (1993) 3 R.S.D.I.E. 669

Caflisch L, 'Pratique Suisse en Matière de Droit International Public 1993' (1994) 4 R.S.D.I.E. 597

Caflisch L, 'La Pratique Suisse en Matière de Droit International Public 2004' (2005) 15 R.S.D.I.E. 713

Caflisch L, 'La Pratique Suisse en Matière de Droit International Public 2006' (2007) 17 R.S.D.I.E. 743

Caflisch L, 'La Pratique Suisse en Matière de Droit International Public 2009' (2010) 20 R.S.D.I.E. 511

Caflisch L, 'La Pratique Suisse en Matière de Droit International Public 2013' (2015) 25 R.S.D.I.E. 57

Spanish Yearbook of International Law (Spanish Y.B.I.L.)

Piernas J and others (eds), 'Spanish Diplomatic and Parliamentary Practice in Public International Law, 2009' (2011) 15 Spanish Y.B.I.L. 73

Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (Z.a.ö.R.V.)

Beyerlin U, 'Völkerrechtliche Praxis der Bundesrepublik Deutschland im Jahre 1974' (1976) 36 Z.a.ö.R.V. 760

II. DOCTRINAL SOURCES

Books

Bannelier K and Christakis T, *Cyber-Attacks, Prevention-Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale 2017)

Bederman D, *The Spirit of International Law* (U.G.A. Press 2002)

Belfer Center, *Deterring Terror - How Israel Confronts the Next Generation of Threats* (Belfer Center 2016)

Bell C and Fox M, *Learning Legal Skills* (3rd edn, Blackstone 1999)

Bento A, *Cloud Computing Service and Deployment Models: Layers and Management* (IGI Global 2012)

Betz D and Stevens T, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (Routledge 2012)

Beyerlin U and others (eds), *Recht zwischen Umbruch und Bewahrung* (Springer 1995)

Bianchi A, Peat D and Windsor M (eds), *Interpretation in International Law* (O.U.P. 2015)

Bilingsley A, Michalesen C, and Scott S, *International Law and the Use of Force: A Documentary and Reference Guide* (ABC-CLIO 2009)

Bosco D, *Five to Rule Them All: The UN Security Council and the Making of the Modern World* (O.U.P. 2009)

Brölmann C and Radi Y (eds), *Research Handbook on the Theory and Practice of International Lawmaking* (E.E. 2016)

Buchan R and Tsagourias N (eds), *Research Handbook on international law and cyberspace* (E.E. 2015)

Cane P and Conaghan J (eds), *The New Oxford Companion to Law* (O.U.P. 2008)

Cane P and Kritzer H (eds), *The Oxford Handbook of Empirical Legal Research* (O.U.P. 2010)

Cannizzaro E (ed), *The Law of Treaties Beyond the Vienna Convention* (O.U.P. 2011)

Collective publication, *Le droit international au service de la paix, de la justice et du développement : mélanges Michel Virally* (Pedone 1991)

Combacau J and Sur S, *Droit International Public* (11th edn, L.G.D.J. 2014)

Czosseck C, Ottis R, and Ziolkowski K (eds), *4th International Conference on Cyber Conflict. Proceedings 2012* (NATO CCD COE Publications 2012)

D'Amato A, *The Concept of Custom in International Law* (Cornell University Press 1971)

Dam K, Owens W and Lin H (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (N.A.P. 2009)

Danilenko G, *Law-Making in the International Community* (M.N.P. 1993)

D'Aspremont J, *Formalism and the Sources of International Law - A Theory of the Ascertainment of Legal Rules* (O.U.P. 2011)

D'Aspremont J (ed), *Participants in the International Legal System* (Routledge 2013)

D'Aspremont J, Besson S and Knuchel S (eds), *The Oxford Handbook of the Sources of International Law* (O.U.P. 2017)

D'Aspremont J and Kammerhofer J (eds), *International Legal Positivism in a Post-Modern World* (C.U.P. 2014)

Denza E (ed), *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations* (4th edn, O.U.P. 2016)

Dunoff J and Pollack M (eds), *Interdisciplinary Perspectives on International Law and International Relations: The State of the Art* (C.U.P. 2013)

Dupuy P-M and Kerbrat Y, *Droit international public* (Dalloz 2014)

Đuro Degan V, *Sources of International Law* (M.N.P. 1997)

Fastenrath U and others (eds), *From Bilateralism to Community Interest: Essays in Honour of Bruno Simma*, (O.U.P. 2011)

Gardiner J, *Treaty Interpretation* (2nd edn, O.U.P. 2008)

Golding M, *Legal Reasoning* (Broadview Press 2001)

Goldsmith J and Wu T, *Who Controls the Internet?* (O.U.P. 2006)

Gray C, *International Law and the Use of Force* (O.U.P. 2008)

Guisnel J, *Guerres dans le Cyberespace–Services Secrets et Internet* (La Découverte 2013)

Guzman A, *How International Law Works: A Rational Choice Theory* (O.U.P. 2008)

FireEye, *Redline drawn: China recalculates its Use of Cyber Espionage* (FireEye Incorporated 2016

Hart H, *The Concept of Law* (2nd edn, O.U.P. 1994)

Henderson C, *The Use of Force and International Law* (C.U.P. 2018)

Hernandez G, *The International Court of Justice and the Judicial Function* (O.U.P. 2014)

Hollis D (ed), *The Oxford Guide to Treaties* (O.U.P. 2012)

Institute of Electrical and Electronics Engineers, *2013 World Cyberspace Cooperation Summit IV* (Curran Associates 2009)

International Committee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Kluwer 1987)

International Institute of International Law, *Sanremo Handbook on Rules of Engagement* (IIHL 2009)

Jenks W, *The Common Law of Mankind* (Stevens&Sons 1963)

Jennings R and Watts A (eds), *Oppenheim's International Law* (9th edn, O.U.P. 2008)

Kahin B and Neeson C (eds), *Borders in Cyberspace* (MIT Press 1997)

Kelsen H, *General Theory of Law and State* (H.U.P. 1945)

Kish J and Turns D, *International Law and Espionage* (M.N.P. 1995)

Klabbers J*, An Introduction to International Institutional Law* (C.U.P. 2012)

Klaousen S and Pichevin T (eds), *Renseignement et Ethique, Le Moindre Mal Nécessaire* (Lavauzelle 2014)

Knight A and Ruddock L (eds), *Advanced Research Methods in the Built Environment* (Blackwell 2008)

Koskenniemi M, *From Apology to Utopia* (C.U.P. 2005)

Lafouasse F, *L'Espionnage dans le Droit International* (Nouveau Monde 2012)

Lathrop C, *The Literary Spy* (Y.U.P. 2004)

Laurent S-Y, *Atlas du Renseignement–Géopolitique du Pouvoir* (Les Presses de Sciences Po 2014)

Lewis J, *Conflicts and Negotiations in Cyberspace* (CSIS 2013)

MacCormick (K), *Legal Reasoning and Legal Theory* (Clarendon Press 1978)

Maykut P and Morehouse R, *Beginning Qualitative Research: A Philosophical and Practical Guide* (The Falmer Press 1994)

McConville M (ed), *Research Methods for Law* (E.U.P. 2007)

McElreath D and others, *Introduction to Homeland Security* (2nd edn, CRC Press 2013)

Murty BS, *The International Law of Diplomacy: The Diplomatic Instrument and World Public Order* (New Haven Press 1989)

Norton Moore J and Turner R (eds), *National Security Law* (C.A.P. 2005)

O'Leary Z, 'The Essential Guide to doing your Research Project' (2nd edn, Sage 2010)

Osula A-M and Röigas H (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016)

Pellet A and Daillier P, *Droit International Public* (7th edn, L.G.D.J. 2002)

Podins K, Stinissen J, and Maybaum M (eds), *5th International Conference in Cyber Conflict. Proceedings 2013* (NATO CCD COE Publications 2013)

Program on Humanitarian Policy and Conflict Research at Harvard University, *Manual on International Law Applicable to Air and Missile Warfare* ('HPCR Manual') (C.U.P. 2013)

Ragaini R (ed) *Aids And Infectious Diseases, Proceedings Of The International Seminar On Nuclear War And Planetary Emergencies - 26 Session* (World Scientific 2002)

Raz J, *The Morality of Freedom* (O.U.P. 1986)

Roberts I, *Satow's Diplomatic Practice* (O.U.P. 2009)

Ronzitti N and Venturini G (eds), *The Law of Air Warfare: Contemporary Issues* (Eleven International Publishing 2006)

Roscini M, *Cyber Operations and the Use of Force in International Law* (O.U.P. 2014)

Ruiz-Fabri H and others (eds), *Select Proceedings of the European Society of International Law* (Bloomsbury 2010)

Schmitt M (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* ('Tallinn Manual') (C.U.P. 2013)

Schmitt M (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* ('Tallinn Manual 2.0') (C.U.P. 2017)

Sharp WG, *CyberSpace and the Use of Force* (Aegis Research Corporation 1999)

Shingleton B and Stilz E (eds), *The Global Ethic and Law: Intersections and Interactions* (Bloomsbury 2016)

Simma B and others (eds), *The Charter of the United Nations: A Commentary* (3rd edn, O.U.P. 2012)

Stanger R (ed), *Essays on Espionage and International Law* (O.S.U. Press 1962)

Tams C and others (eds), *Research Handbook on the Law of Treaties* (E.E. 2014)

Thirlway H, *International Customary Law and Codification* (Springer 1972)

Thirlway H, *The Sources of International Law* (O.U.P. 2014)

Van Damme I, *Treaty Interpretation by the WTO Appellate Body* (O.U.P. 2009)

Weller M (ed), *The Oxford Handbook of the Use of Force in International Law* (O.U.P. 2015)

Wingfield T, *The Law of Information Conflict–National Security Law in Cyberspace*, (Aegis Research Corps 2000)

Wolfke K, *Custom in Present International Law* (Prace W.T.N. 1964)

Zimmermann A and others (eds), *The Statute of the International Court of Justice - A Commentary* (O.U.P. 2006)

Articles (journals)

Adams MJ, 'Jus Extra Bellum: Reconstructing the Ordinary, Realistic Conditions of Peace' (2014) 5 Harv.Nat'l.Sec.J. 377

Akehurst M, 'Custom as a Source of International Law' (1976) 47(1) British Y.B.I.L. 1

Aldrich R, 'How do you know you are at War in the Information Age' (2000) 22 Hous.J.Int'l.L. 223

Aloupi N, 'The Right to Non-Intervention and Non-Interference' (2015) 4(3) C.J.I.C.L. 566

Andres R and Shackelford S, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2011) 42 Geo.J.Int'l.L. 971.

Antolin-Jenkins V, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?' (2005) 51 Naval L.Rev. 132

Baker C, 'Tolerance of International Espionage: A Functional Approach' (2004) 19(5) Am.U.Int'l.L.Rev. 1091

Banks W, 'State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0' (2017) 95 Tex.L.Rev. 1487

Barkham J, 'Information Warfare and International Law on the Use of Force' (2001) 37 J.I.L.P. 57

Beard J, 'Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law' (2014) 47 Vanderbilt J.Transnatl.L. 67

Bederman D, 'Acquiescence, Objection and the Death of Customary International Law' (2010) 21 Duke J.Comp.&Int'l.L. 31

Benatar M, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 1 Go.J.I.L. 375

Beresford S, Surveillance Aircraft and Satellites: A Problem of International Law' (1960) 27(2) J. Air L. 107

Blake D and Imburgia J, '"Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of defining them as "Weapons"' (2010) 66 A.F.L.R. 157

Blank L, 'International Law and Cyber Threats from Non-State Actors' (2013) 89 I.L.S. 406

Blood C, 'Holding Foreign Nations Civilly Accountable for Their Economic Espionage Practices' (2002) 42(2) I.D.E.A. 227

Bos M, 'The Identification of Custom in International Law' (1982) 25 German Y.B.I.L. 9

Bowen G, 'Document analysis as a Qualitative Research Method' (2009) Q.R.J. 9(2) 27

Brenner S and Crescenzi A, 'State-Sponsored Crime: The Futility of the Economic Espionage Act' (2006) 28 Hous.J.Int'l.L. 389

Brewer S, 'Exemplary Reasoning: Semantics, Pragmatics, and the Rational Force of Legal Argument by Analogy' (1996) 109(5) Harv.L.Rev. 923

Brown G, 'Spying and Fighting in Cyberspace: What is Which' (2016) 8 J.Nat'l.Sec.L.&Pol'y 621

Brown G and Meltcaf A, 'Easier Said Than Done: Legal Reviews of Cyber Weapons' (2014) 7 J.Nat'l.Sec.L.&Pol'y 115

Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17(2) J.Conflict&Sec.L. 211

Caccamo J, 'A Comparison and Analysis of Immunities Defenses Raised by Soviet Nationals Indicted under United States Espionage Laws' (1980) 6 Brook.J.Int'l.L. 259

Chesterman S, 'The spy who came in from the cold war: intelligence and international law' (2006) 27 Mich.J.Intl.L. 1071

Cohen J, 'Cyberspace as/and Space' (2010) 107 Colum.L.Rev. 210

Cohen-Jonathan G and Kovar R, 'L'espionnage en temps de paix' (1960) 6 A.F.D.I. 239

Corn G and Taylor R, 'Sovereignty in the Age of Cyber' (2017-2018) 111 A.J.I.L. Unbound 207

Crane A, 'In the company of spies: when competitive intelligence gathering becomes industrial espionage' (2005) 48 Business Horizons 233

Danielson M, 'Economic espionage: a framework for a workable solution' (2008) 10(2) Minn.J.L.Sci.&Tech. 503

Danilenko G, 'The Theory of International Customary Law' (1988) 31 German Y.B.I.L. 9

D'Aspremont J, 'Cyber Operations and International Law: An Interventionist Legal Thought' (2016) 21 Journal of Conflict & Security Law 575

D'Aspremont J, 'The Decay of Modern Customary International Law in Spite of Scholarly Heroism' (2015) G.C.Y.I.L.J. 9

D'Aspremont J, 'The International Court of Justice, the Whales, and the Blurring of the Lines between Sources and Interpretation' (2016) 27(4) E.J.I.L. 1027

D'Aspremont J, 'The Law of International Organizations and the Art of Reconciliation' (2014) 11 I.O.L.R. 428

David E, 'Le Principe de Non-Intervention' (1990) 2 R.B.D.I. 351

Deeks A, 'An International Legal Framework for Surveillance' (2015) 55(2) Va.J.Int'l.L. 290

Delahunty R, 'Herbert Butterfield, Christianity, and International Law' (2009) 86 U.Det. Mercy L.Rev. 615

Dever J and Dever J, 'Cyberwarfare: Attribution, Preemption, and National Self Defense' (2013) 2 J.L.&Cyber Warfare 25

Dinstein Y, 'Computer Network Attacks and Self-Defense' (2002) 76 I.L.S. 99

Dinstein Y, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference' (2013) 89 I.L.S. 276

Dorondo P, 'The Military Attachés' (2008) 4(3) Studies Archive Indexes

Dworkin R, 'In Praise of Theory' (1997) 29 Ariz.St.L.J. 353

Edmondson L, 'Espionage in Transnational Law' (1971-2) 5 Vanderbilt J.Transnatl.L. 434

Efrony D and Shany Y, 'A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice' (2018) 112(4) A.J.I.L. 583

Epstein L and King G, 'The Rule of Inference' (2002) 69(1) U.Chi.L.Rev. 1

Everly M, 'Net Neutrality and the Department of the Internet: Creating Problems through Solutions' (2017) 42 U. Dayton L.Rev. 55

Farrar J, 'Reasoning by Analogy in the Law' (1997) 9(2) Bond L.R. 149

Fialka J, 'While America Sleeps' (1997) 21(1) The Wilson Quarterly 48

Fleck D, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 Mich.J.Int'l.L. 687

Forcese C, 'Spies without borders: international law and intelligence collection' (2011) 5 Nat'l. Security L.&Pol'y 179

Franzese P, 'Sovereignty in Cyberspace: Can it Exist?' (2009) 64 A.F.L.R. 1

Fray W, 'Network Communications Protocols: The OSI Model' (1993) 5 Trends L.Libr.Mgmt.&Tech. 4

Frieden L, 'Newsgathering by Satellites: A New Challenge to International and National Law at the Dawn of the Twenty-First Century' (1988-9) 25 Stan.J.Int'l.L. 103

Gaul A, 'Neutrality in the Digital Battle Space: Applications of the Principle of Neutrality in Information Warfare' (2013) 29 Syracuse J.O.S.T. 51

Georgieva I, 'The Right to Privacy under Fire - Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31 Utrecht J.Int'l.&Eur.L. 104

Gervais M, 'Cyber Attacks and the Laws of War' (2012) J.L.&Cyber Warfare 8

Giles C, 'Balancing the Breach: Data Privacy Laws in the Wake of the NSA Revelations' (2015) 37(2) Hous.J.Int'l.L. 543

Govier T, 'Analogies and Missing Premises' (1989) 11(3) Informal Logic 141

Grosswald L, 'Cyberattack Attribution Matters Under Article 51 of the U.N. Charter' (2011) 36 Brook.J.Int'l.L. 1151

Grzybowski K, 'The Regime of Diplomacy and the Tehran Hostages' (1981) 30 I.C.L.Q. 42

Haggenmacher P, 'La doctrine des deux éléments du droit coutumier international dans la pratique de la Cour internationale' (1986) 1 R.G.D.I.P. 6

Hanford E, 'The Cold War of Cyber Espionage' (2014) 20(1) P.I.L.R. 22

Heintschel Von Heinegg W, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 I.L.S. 123

Hollis D, 'Why States need an International Law for Importation Operations' (2007) 11 Lewis&Clark L.Rev. 1023

Jackamo T, 'From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary International Law of Non-Intervention' (1992) 32 Va.J.Int'l.L. 929

Jamnejad M and Wood M, 'The Principle of Non-Intervention' (2009) 22(2) L.J.I.L. 345

Jennings K, 'Espionage: Anything goes' (1987) 14 Pepp.L.Rev. 647

Johnson D and Post D, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48(5) Stan.L.Rev. 1367

Jolley J, 'Article 2(4) and Cyber Warfare: How do Old Rules Control the Brave New World?' (2013) 2(1) International Law Research 1

Jordan DA, 'Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice Over Protocol' (2005) 47(3) Bost CLR 505

Joyce D, 'Privacy in the Digital Era: Human Rights Online?' (2015) 16 Melb.J.Int'l.L. 270

Joyner C, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12(5) E.J.I.L. 825

Joyner C and Lotrionte C, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12(5) E.J.I.L. 825

Jupillat N, 'From the Cuckoo's Egg to Global Surveillance: Cyber Espionage That Becomes Prohibited Intervention' (2017) 42 N.C.J.Int'l.L.&Com.Reg. 933

Juthe A, 'Argument by Analogy' (2005) 19(1) Argumentation 1

Kamm F, 'Theory and Analogy in Law' (1997) Ariz.St.L.J. 405

Kennedy D, 'Challenging Expert Rule: The Politics of Global Governance' (2005) 27 Syd.L.R. 5

Khalil C, 'Thinking Intelligently about Intelligence: A Modal Global Framework protecting Privacy' (2015) 47 Geo.Wash.Int'l.L.Rev. 919

Kilovaty I, 'Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare' (2014) 5(1) N.S.L.B. 91

Kirchner S, 'Protection of Privacy Rights of Internet Users Against Cross-Border Government Interference' (2014) 42 I.J.L.I. 493

Kirsch C, 'Science Fiction No More: Cyber Warfare and the United States' (2012) 40 Denv.J.Int'l.L.&Pol'y 620

Kohen (M), 'The Principle of Non-Intervention 25 Years after the Nicaragua Judgment' (2012) 25 L.J.I.L. 157

Kolb R, 'Selected problems in the theory of customary international law' (2003) 50(2) N.I.L.R. 119

Koskenniemi M, 'International Law: Constitutionalism, Managerialism and the Ethos of Legal Education' (2007) 1(1) Eur.J.Legal.Stud. 8

Koskenniemi M, 'The Fate of Public International Law: Between Technique and Politics' (2007) 70(1) M.L.R. 1

Kraska J, 'Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters' (2015) 54 Col.J.T.L. 164

Kraska J and O'Donnell B, 'International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement' (2002) 76 I.L.S. 395

Kunz J, 'The Nature of Customary International Law' (1953) 47(4) A.J.I.L. 662

Kwiecien R, 'Armed Intervention and Violation of State Sovereignty in International Law' (2004) 13 Pol.Q.Int'l Affairs 73

Lafouasse F, 'L'Espionnage en Droit international' (2001) 47 A.F.D.I. 63

Lin H, 'Offensive Cyber Operations and the Use of Force' (2010) 4(1) J.Nat'l.Sec.L.&Pol'y 63

Lobel H, 'Cyber War Inc: The Law of War Implications of the Private Sector's Role in Cyber Conflict' (2012) 47 Tex.Int'l.L.J. 617

Lotrionte C, 'Countering State-Sponsored Cyber Economic Espionage Under International Law' (2014-2015) 40 N.C.J.Int'l.L.&Com.Reg. 443

Lubin A, 'Espionage as a Sovereign Right under International Law and its Limits' (2016) 24(3) I.L.S.A. Quarterly 22

Malawer S, 'Chinese Economic Cyber Espionage: U.S. Litigation in the WTO and Other Diplomatic Remedies' (2015) 16 Geo.J.Int'l.L. 158

McDougal M, Lasswell H, Reisman M, 'The Intelligence Function and World Public Order' (1973) 46(3) Temple L.Q. 365

McGavran W, 'Intended Consequences: Regulating Cyber Attacks' (2009) 12 Tul.J.Tech.&Intell.Prop. 259

Melnitzky A, 'Defending America against Chinese Cyber Espionage through the Use of Active Defences' (2012) 20 Cardozo J.Int'l.&Comp.L. 537

Menthe D, 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1998) 4 Mich.Telecomm.&Tech.L.Rev. 69

Mogalakwe M, 'The Use of Documentary Research Methods in Social Research' (2006) 10(1) African Sociological Review 221

Murphy J, 'Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?' (2013) 89 I.L.S. 309

Navarette I, 'L'Espionnage en Temps de Paix en Droit International Public' (2015) 53 Canadian Y.B.I.L. 1

O'Connell M-E, 'Cyber Security without Cyber War' (2012) 17(2) J.Conflict&Sec.L. 187

Ohlin J-D, 'Did Cyber Interference in the 2016 Election Violate International Law?' (2017) 95 Tex.L.Rev. 1579

Orford A, 'Embodying Internationalism: The Making of International Lawyers' (1988) 19 Australian Y.B.I.L. 1

Parajon-Skinner C, 'An International Law Response to Economic Cyber Espionage' (2014) 46(4) Conn.L.R. 1105

Pauwelyn J, 'The Role of Public International Law in the WTO: How far can we go?' (2001) 95 A.J.I.L. 535

Pelican L, 'Peacetime Cyber-Espionage: A Dangerous but Necessary Game' (2011-2012) 20 CommLaw Conspectus 363

Poché C, 'This means War! (Maybe?): Clarifying Casus Belli in Cyberspace' (2013) 15 Or.Rev.Int'l.L. 413

Polakiewicz J, 'Die völkerrechtliche Zulässigkeit der Überwachung des Telefonverkehrs von Konsulaten ausländischer Staaten' (1990) 50 Z.a.ö.R.V. 761

Pool P, 'War of the Cyber World: The Law of Cyber Warfare' (2013) 47 Int.Lawyer 299

Pun D, 'Rethinking Espionage in the Modern Era' (2017) 18(1) Chi.J.Int'l.L. 353

Radsan J, 'The Unresolved Equation of Espionage and International Law' (2007) 28 Mich.J.Int'l.L. 595

Roberts S, 'Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors' (2014) 41(3) N.Ky.L.Rev. 535

Savage D, 'Law of the LAN' (1993) 9 Santa Clara Computer&High Tech.L.J. 193

Schaap A, 'Cyber Warfare Operations: Developments and Use under International Law' (2009) 64 A.F.L.R. 121

Schmitt M, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Col.J.T.L. 885

Schmitt M, "Computer Network Attack: The Normative Software' (2001) 4 Y.B.I.H.L. 53

Schmitt M, 'Cyber Operations and the Jus Ad Bellum Revisited' (2011) 56 Vill.L.Rev. 569

Scott R, 'Territorially intrusive intelligence collection and international law' (1999) 46 A.F.L.R. 217

Shackelford S, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27 Berk.J.Int'l.L. 192

Scoville H, 'Is Espionage Necessary for Our Security' (1976) 54 Foreign Affairs 482

Smith J, 'State Intelligence Gathering and International Law - Keynote address' (2007) 28 Mich.J.Int'l.L. 543

Solis G, 'Cyber Warfare' (2014) Mil.L.Rev. 1

Soraghan J, 'Reconnaissance Satellites: Legal Characterization and Possible Utilizations for Peacekeeping' (1967) 13(3) McG.L.J. 458

Spector P, 'In Defense of Sovereignty, in the Wake of Tallinn 2.0' (2017-2018) 111 A.J.I.L. Unbound 219

Stanton Watson H, 'Armed Conflict and Humanitarian Intervention - International Standard Rules of Engagement' (2000) Austl.Int'l.L.J. 151

Strawbridge J, 'The Big Bluff - Obama, Cyber Economic Espionage, and the Threat of WTO Espionage' (2016) 47 Geo.J.Int'l.L. 833

Sulmasy G and Yoo J, 'Counterintuitive: Intelligence Operations and International Law' (2007) 28 Mich.J.Int'l.L. 625

Sunstein C, 'On Analogical Reasoning' (1992-3) 106 Harv.L.Rev. 741

Svantesson D, 'Lagom Jurisdiction–What Viking Drinking Etiquette Can Teach Us about Internet Jurisdiction and Google France' (2018) Masaryk U.J.L.&Tech. 29

Swaine M, 'Chinese Views on Cybersecurity in Foreign Relations' (2013) 42 China Leadership Monitor 1

Talmon S, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion' (2015) 26(2) E.J.I.L. 417

Tzanakopoulos A, 'The Right to be Free from Economic Coercion' (2014) 4(3) C.J.I.C.L. 616

Van Arnam R, 'Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection' (2001) 27 N.C.J.Int'l.L.&Com.Reg. 95

Walden R, 'The Subjective Element in the Formation of Customary International Law' (1977) 12 Is.L.R. 344

Wall A, 'Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action' (2011) 3 Harv.Nat'l.Sec.J. 85

Ward N, 'Espionage and the Forfeiture of Diplomatic Immunity' (1977) 11(4) The International Lawyer 657

Watts S, 'Combatant Status and Computer Network Attack' (2010) 50 Va.J.Int'l.L. 391

Watts S, 'Law-of-War Perfidy' (2014) Mil.L.Rev. 106

Waxman M, 'Cyber Attacks as "Force" under UN Charter Article 2(4)' (2011) 87 I.L.S. 43

Weissbrodt D, 'Cyber-Conflict, Cyber-Crime, and Cyber-Espionage' (2013) 22 Minn.J.Int'l.L. 347

Williams R, '(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action' (2011) 79(4) Geo.J.Int'l.L. 1162

Witiw E-P, 'Persona Non Grata: Expelling Diplomats who abuse their Privileges' (1988) 9 N.Y.L.Sch.J.Int'l.&Comp. 345

Wood M, 'The Interpretation of Security Council Resolutions' (1998) 2 M.P.Y.U.N.L. 73

Worster WT, 'The Inductive and Deductive Methods in Customary International Law Analysis: Traditional and Modern Approaches' (2014) 45(2) Geo.J.Int'l.L. 445

Wortham A, 'Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?' (2012) 64 Fed.Comm.L.J. 643

Wright Q, 'Legal Aspects of the U-2 Incident' (1960) 54 A.J.I.L. 836

Articles (unpublished)

AECT, 'The Handbook of Research for Educational Communications and Technology' (*aect,* 03.08.2001)
<www.aect.org/edtech/ed1/41/41-01.html>

Barela S, 'Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion' (*Just Security*, 12.01.2017)
<www.justsecurity.org/36212/cross-border-cyber-ops-erode-legitimacy-act-coercion/>

Barzon A, 'An Issue for all Seasons: Peacetime Espionage and International Law' (2018)
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3169247>

Cohen H, 'Methodology and Misdirection: Custom and the ICJ' (*EJIL:Talk!*, 01.12.2015)
<www.ejiltalk.org/methodology-and-misdirection-a-response-to-stefan-talmon-on-custom-and-the-icj/>

D'Aspremont J, 'Managing Change in International Law and the Dream of the Managerialist International Lawyer', (*EJIL:Talk!*, 25.09.2015)
<www.ejiltalk.org/managing-change-in-international-law-and-the-dream-of-the-managerialist-international-lawyer/>

D'Aspremont J, 'What Was Not Meant to Be: General Principles of Law As a Source of International Law' (2017) 11
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3053158>

DeFranzo S, 'What's the difference between qualitative and quantitative research?' (*snapsurveys*, 16.09.2011)
<www.snapsurveys.com/blog/qualitative-vs-quantitative-research/>

Duarte d'Almeida L and Michelon C, 'The Structure of Arguments by Analogy in Law' (2017) Edinburgh School of Law Research Paper No 06/2017
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2948558>

Duquet S and Wouters J, 'Diplomacy, Secrecy and the Law' (2015) Leuven Centre for Global Governance Studies, Working Paper No 151 <https://ghum.kuleuven.be/ggs/publications/working_papers/2015/151duquetwouters>

Fidler D, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies' (*ASIL*, 17.03.2013) <www.asil.org/sites/default/files/insight130320.pdf>

Fidler D, 'Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage' (*Arms Control Law,* 11.02.2013) <https://armscontrollaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/>

Forcese C, 'The "Hacked" US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards?' (*Just Security*, 16.12.2016) <www.justsecurity.org/35652/hacked-election-international-law-silent-faced-clatter-cyrillic-keyboards/>

Goldsmith J, 'The Internet and the Legitimacy of Remote Cross-Border Searches' (2011) 16 Chicago - Public Law and Legal Theory Working Paper <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://www.google.fr/&httpsredir=1&article=1316&context=public_law_and_legal_theory>

Goodman R, 'International Law and the US Response to Russian Election Interference', (*Just Security, 2017*) <www.justsecurity.org/35999/international-law-response-russian-election-interference/>

Hankinson O, 'Due Diligence and the Grey Zones of International Cyberspace Laws' (*MJIL* 2017) <www.mjilonline.org/due-diligence-and-the-gray-zones-of-international-cyberspace-laws/>

Hollis D, 'Russia and the DNC Hack: What Future for a Duty of Non-Intervention?' (*Opinio Juris,* 25.07.2016) <http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/>

Hollis D, 'The fog of technology and international law' (*SIDI*, 14.05.2015) <www.sidiblog.org/2015/05/14/the-fog-of-technology-and-international-law/>

Klabbers J, 'The Invisible College' (*Opinio Juris*, 03.03.2009) <opiniojuris.org/2009/03/03/the-invisible-college/>

Kostadinov D, 'Cyber Exploitation' (*Infosec Institute,* 25.02.2013) <http://resources.infosecinstitute.com/cyber-exploitation/>

Lewis J, 'The US Really Does Want to Constrain Commercial Espionage: Why Does Nobody Believe It?' (*Lawfare*, 1.07.2016) <www.lawfareblog.com/us-really-does-want-constrain-commercial-espionage-why-does-nobody-believe-it>

Lusa Bordin F, 'Induction, Assertion and the Limits of the Existing Methodologies to Identify Customary International Law' (*EJIL:Talk!,* 02.12.2015) <www.ejiltalk.org/induction-assertion-and-the-limits-of-the-existing-methodologies-to-identify-customary-international-law/>

Peters A, 'Surveillance Without Borders - The Unlawfulness of the NSA-Panopticon' (*EJIL:Talk!*, 04.11.2013) <www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/>

Schneier B, 'When Does Cyber Spying Become a Cyber Attack?' (*DefenseOne*, 10.03.2014) <www.defenseone.com/technology/2014/03/when-does-cyber-spying-become-cyber-attack/80206/>

Sender O and Wood M, 'The International Court of Justice and Customary International Law: A Reply to Stefan Talmon' (*EJIL:Talk!*, 30.11.2015) <www.ejiltalk.org/the-international-court-of-justice-and-customary-international-law-a-reply-to-stefan-talmon/>

Shull A, 'Cyber Espionage and International Law*'* (2013) <api.ning.com/files/Ug-Ogup9PZ*wyVLXDplSNaUjM*f0HUBBaN*HklqwwORwnR7xopUarjsRlt7Db4H6M7Fa271aTs6Abfp4uYRTjlaVVpQwHEAV/giganet2013_Shull.pdf>

Smirnova M, 'Is the Right to Education a New "Jus Cogens" of Our Times? Methodology of Research' (2013) <https://ssrn.com/abstract=3088502>

Talmon S, 'Tapping the German Chancellor's Cell Phone and Public International Law' (*C.I.L.J.*, 06.11.2013)

<http://C.I.L.J..co.uk/2013/11/06/tapping-german-chancellors-cell-phone-public-international-law/>

Traynor I, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guadian* (17.05.2007)
<www.theguardian.com/world/2007/may/17/topstories3.russia>

Tsagourias N, 'Economic cyber espionage and due diligence' (*Syracuse University,* 2015)
<insct.syr.edu/wp-content/uploads/2015/06/Tsagourias_Due_Diligence.pdf>

Van De Velde J, 'The Law of Cyber Interference in Elections' (2017)
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828>

Watts S, 'International Law and Proposed U.S. Responses to the D.N.C. Hack' (*justsecurity,* 14.10.2016)
<www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/>

Theses

Delerue F, 'State-sponsored Cyber Operations and International Law' (PhD Thesis, EUI, 2016)

Jolley J, 'Attribution, state responsibility, and the duty to prevent malicious cyber-attacks in international law' (PhD thesis, University of Glasgow, 2017)

Singh L, 'The United Nations Convention on Contracts for the International Sale of Goods 1980 (CISG): an examination of the buyer's remedy of avoidance under the CISG: how is the remedy interpreted, exercised and what are the consequences of avoidance?' (PhD thesis, University of the West of England, 2015)

Shoshan E, 'Applicability of International Law on Cyber Espionage Intrusions' (Master thesis, Stockholm University, 2014)

Collected Courses of The Hague Academy of International Law

Abi-Saab G, 'Cours général de droit international public' (1987) 207 Recueil de Cours de l'Académie de Droit International 9

Bernhardt R, 'Custom and Treaty in the Law of the Sea' (1987) 205 Recueil des Cours de l'Académie de Droit International 247

Mendelson M, 'The formation of customary international law' (1998) 272 Recueil des Cours de l'Académie de Droit International 197

Nahlik S, 'Developments of Diplomatic Law - Selected Problems' (1990) 222 Recueil des Cours de l'Académie de Droit International 187

Sorensen M, 'Principes de Droit International Public' (1960) 101 Recueil des Cours de l'Académie de Droit International 1

Zourek J, 'La définition de l'agression et le droit international : développements récents de la question', (1958) 92 Recueil des Cours de l'Académie de Droit International 755

III. DICTIONARIES AND ENCYCLOPEDIAES

Max Planck Encyclopedia of Public International Law

Benvenisti E, 'Occupation, Belligerent' (2009) M.P.E.P.I.L.

Besson S, 'Sovereignty' (2011) M.P.E.P.I.L.

Blay S, 'Territorial Integrity and Political Independence' (2010) M.P.E.P.I.L.

Blokker N, 'International Organizations or Institutions, Implied Powers' (2009) M.P.E.P.I.L.

Boothby W, 'Weapons, prohibited' (2015) M.P.E.P.I.L.

Bothe M, 'Neutrality, Concept and General Rules' (2015) M.P.E.P.I.L.

Danai O and Hostettler P, 'Neutrality in Land Warfare' (2015) M.P.E.P.I.L.

Dinstein Y, 'Aggression' (2015) M.P.E.P.I.L

Dörr O, 'Use of Force, Prohibition of' (2011) M.P.E.P.I.L.

Joyner C, 'Coercion' (2008) M.P.E.P.I.L.

Klabbers J, 'Treaties, Object and Purpose' (2006) M.P.E.P.I.L.

Klein E, 'Self-Contained Regime' (2006) M.P.E.P.I.L.

Kunig P, 'Intervention, Prohibition of' (2008) M.P.E.P.I.L.

Richter D, 'Unfriendly Act' (2013) M.P.E.P.I.L.

Vöneky S, 'Analogy in International Law' (2008) M.P.E.P.I.L.

Woltag J-C, 'Cyber Warfare' (2010) M.P.E.P.I.L.

Woltag J-C, 'Internet' (2010) M.P.E.P.I.L.

Ziegler K, 'Domaine Réservé' (2013) M.P.E.P.I.L.

Dictionaries of English and French languages

Black's Law Dictionary (10th edn, 2014)

Collins, 'English Dictionary'
<www.collinsdictionary.com>

Larousse, 'Dictionnaire de français'
<www.larousse.fr/dictionnaires/francais-monolingue>

Merriam-Webster, 'Dictionary'
<www.merriam-webster.com/>

Oxford English Dictionary (O.U.P. 2018)
<www.oed.com/>

Oxford Living Dictionary, 'English Dictionary'
<en.oxforddictionaries.com/english>

Other sources

Heslop A, 'Political System' (*Britannica*)
<www.britannica.com/topic/political-system>

Morrow R, 'Telecommunications network' (*Britannica*)
<www.britannica.com/technology/telecommunications-network>

Philpott D, 'Sovereignty' (2003, 2010) (*Stanford Encyclopedia of Philosophy*)
<http://plato.stanford.edu/entries/sovereignty/>

Wood M, 'Non-Intervention (Non-interference in domestic affairs)' (*Encyclopedia Princetoniensis*)
<https://pesd.princeton.edu/?q=node/258>

Zwass V, 'Information system' (*Britannica)*
<www.britannica.com/topic/information-system>

IV. MEDIA

Online press

AFP and TOI Staff, 'Top IDF general: Israel, Egypt have 'unprecedented' intel cooperation', *Times of Israel* (20.04.2016)
<www.timesofisrael.com/top-idf-general-israel-egypt-have-unprecedented-intel-cooperation/>

Associated Press, 'Brazil accuses Canada of spying after NSA leaks', *The Guardian* (08.01.2013)
<www.theguardian.com/world/2013/oct/08/brazil-accuses-canada-spying-nsa-leaks>

Axe D, 'The Navy's underwater eavesdropper', *Reuters* (19.06.2013)
<http://blogs.reuters.com/great-debate/2013/07/18/the-navys-underwater-eavesdropper/>

'Bahamas Foreign Affairs Minister addresses OAS Regular Session', *The Bahamas Weekly* (06.06.2014)
<www.thebahamasweekly.com/publish/oas-media-releases/Bahamas_Foreign_Affairs_Minister_addresses_OAS_Regular_Session35338.shtml>

Baumgärtner M, Knobbe M and Schindler J, 'German Intelligence Also Snooped on White House', *Spiegel* (22.06.2017)
<www.spiegel.de/international/germany/german-intelligence-also-snooped-on-white-house-a-1153592.html>

Beaumont P, Bright M and Vulliamy E, 'UN launches inquiry into American spying', *The Guardian* (09.03.2003)
<www.theguardian.com/world/2003/mar/09/iraq.unitednations1>

Birnbaum M, Booth M and Nakashima E, 'U.S. and its allies target Russian cyber spies with indictments, public shaming', *The Washington Post* (04.10.2018)
<www.washingtonpost.com/world/europe/britain-directly-blames-russian-military-intelligence-for-broad-range-of-cyberattacks/2018/10/04/13a3a1f8-c7b6-11e8-9158-09630a6d8725_story.html?utm_term=.5d52406ad31f>

Borger J, Oltermann P and Watt N, 'Germany calls in British ambassador over spy claims', *BBC* (05.11.2013)
<www.bbc.com/news/world-europe-24824633>

Brenner J, 'The New Industrial Espionage', *The American Interest* (10.12.2014)

<www.the-american-interest.com/2014/12/10/the-new-industrial-espionage/>

Chinea E and Gupta G, 'Venezuela president orders investigation after report on U.S. spying', *Reuters* (18.11.2015)
<www.reuters.com/article/us-venezuela-usa-idUSKCN0T80AB20151119>

Chouza P, 'México rechaza "categóricamente" cualquier labor de espionaje', *El Pais* (02.09.2013)
<https:/elpais.com/internacional/2013/09/02/actualidad/1378158712_855137.html>

Erdbrink T, 'Iran Confirms Attack by Virus That Collects Information', *New York Times* (29.05.2012)
<www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html?_r=1&hp>

Follorou J and Johannès F, 'Révélations sur le Big Brother français', *Le Monde* (07.07.2013)
<www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html>

Freedberg S, 'DNI, NSA Seek Offensive Cyber Clarity; OPM Not An "Attack"' *Breaking Defense* (10.09.2015)
<https://breakingdefense.com/2015/09/clapper-rogers-seek-cyber-clarity-opm-not-an-attack/>

'French president wants "all information" on reported German spying', *Deutsche Welle* (12.11.2015)
<www.dw.com/en/french-president-wants-all-information-on-reported-german-spying/a-18845907>

Gady F-Z, 'CIA to Expand Cyber Espionage Capabilities', *The Diplomat* (24.02.2015)
<http://thediplomat.com/2015/02/cia-to-expand-cyber-espionage-capabilities/>

Gambino L, Siddiqui S and Walker S, 'Obama expels 35 Russian diplomats in retaliation for US election hacking', *The Guardian* (30.12.2016)
<www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack>

Greenberg A, 'An Interview With WikiLeaks' Julian Assange', *Forbes* (29.11.2010)

<www.forbes.com/sites/andygreenberg/2010/11/29/an-interview-with-wikileaks-julian-assange/8/#1e3eb8747153>

Hager N, 'Au coeur du renseignement américain', *Le Monde Diplomatique* (Novembre 2001)
<www.monde-diplomatique.fr/2001/11/HAGER/8141>

'In rare admission, Castro says Cuba has dispatched spies across U.S.', *CNN* (20.10.1998)
<http://edition.cnn.com/US/9810/20/cuban.espionage/>

Jacobs J, 'After Reports on N.S.A., China Urges End to Spying', *The New York Times* (24.03.2014)
<www.nytimes.com/2014/03/25/world/asia/after-reports-on-nsa-china-urges-halt-to-cyberspying.html>

Kirkpatrick D, Pelroth N and Sanger D, 'The World Once Laughed at North Korean Cyberpower. No More.', *New York Times* (15.10.2017)
<www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html>

Khazan O, 'Gentlemen Reading Each Other's' Mail: A Brief History of Diplomatic Spying', *The Atlantic* (17.06.2013)
<www.theatlantic.com/international/archive/2013/06/gentlemen-reading-each-others-mail-a-brief-history-of-diplomatic-spying/276940/>

Kim C, 'North Korea hacking increasingly focused on making money more than espionage: South Korea study', *Reuters* (28.07.2017)
<www.reuters.com/article/us-northkorea-cybercrime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO>

Kronenfeld S and Siboni G, 'Iranian Cyber Espionage: A Troubling New Escalation', *INSS Insight*, (16.06.2014)
<www.inss.org.il/publication/iranian-cyber-espionage-a-troubling-new-escalation/>

Leloup D, 'Révélation après révélation, le silence de la France face à l'espionnage de la NSA', *Le Monde* (23.06.2015)
<www.lemonde.fr/pixels/article/2015/06/23/revelation-apres-revelation-le-silence-de-la-france-face-a-l-espionnage-de-la-nsa_4660310_4408996.html>

Lennon M, 'Hackers Used Sophisticated SMB Worm Tool to Attack Sony', *SecurityWeek* (19.12.2014)

<www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony>

'L'Estonie condamne trois espions russes', *Le Courrier de Russie* (23.02.2016) <www.lecourrierderussie.com/international/2016/02/estonie-trois-espions-russes/>

Lewis O, 'Israel warns against computer-hacker vigilantism', *Reuters* (12.01.2012) <www.reuters.com/article/us-israel-hackers/israel-warns-against-computer-hacker-vigilantism-idUSTRE80B23420120112>

Lischka K, 'BND leitet seit 2007 Daten an die NSA weiter', *Spiegel* (08.08.2013) <www.spiegel.de/netzwelt/netzpolitik/geheimdienste-bnd-leitet-seit-2007-daten-an-die-nsa-weiter-a-915589.html>

MacAskill E and others, 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian* (21.06.2013) <www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

McCoy T, 'Cuba deal reveals new clues in case of Ana Montes, "the most important spy you've never heard of"', *The Washington Post* (18.12.2014) <www.washingtonpost.com/news/morning-mix/wp/2014/12/18/cuba-deal-reveals-new-clues-in-case-of-ana-montes-the-most-important-spy-youve-never-heard-of/?utm_term=.adda1bff4747>

Mufson S and Nakashima E, 'The U.S. and China agree not to conduct economic espionage in cyberspace', *The Washington Post* (25.09.2015) <www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html?utm_term=.4a06681508e1>

Murphy K, 'Edward Snowden a traitor but US spy review is welcome, says Julie Bishop', *The Guardian* (23.01.2014) <www.theguardian.com/world/2014/jan/23/edward-snowden-a-traitor-but-us-spy-review-is-welcome-says-julie-bishop>

Oren A, 'Leaked Classified Memo Reveals U.S.-Israeli Intel Cooperation on Egypt, Iran', *Haaretz* (05.08.2014) <www.haaretz.com/israel-news/.premium-1.608802>

Panda A, 'US, South Korea, Japan Start Sharing Intelligence on North Korea', *The Diplomat* (30.12.2014)

<thediplomat.com/2014/12/us-south-korea-japan-start-sharing-intelligence-on-north-korea/>

'Putin: cyber espionage is direct violation of state's sovereignty', *Interfax* (11.07.2014)
<www.interfax.com/newsinf.asp?id=519963>

'Putin suggests to create int'l information security system against wiretapping', *Sputniknews* (11.07.2014)
<http://sputniknews.com/voiceofrussia/2014_07_11/Putin-suggests-to-create-intl-information-security-system-against-wiretapping-9052/>

Ranger S, 'The new weapon against Russian cyber-attacks: Naming and shaming', *ZDNet* (04.10.2018)
<www.zdnet.com/article/the-new-weapon-against-russian-cyber-attacks-naming-and-shaming/>

Reed J and Jee-Sheok Shin E, 'Statue wars reveal contested history of Japan's "comfort women"', *The Huffington Post* (02.07.2017)
<www.huffingtonpost.com/the-conversation-global/statue-wars-reveal-contes_b_14635786.html?guccounter=1>

Reuters and Pfeffer A, 'How Cyberwarfare Has Made MI a Combat Arm to the IDF', *Haaretz* (16.12.2009)
<www.haaretz.com/how-cyberwarfare-has-made-mi-a-combat-arm-of-the-idf-1.2051>

Reuters staff, 'German intelligence spied on Interpol: Spiegel', *Reuters* (22 April 2017)
<www.reuters.com/article/us-germany-spying-interpol/german-intelligence-spied-on-interpol-spiegel-idUSKBN17O08X>

Riley M and Robertson J, 'The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies', *Bloomberg* (04.10.2018)
<www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

Sanger D, 'Differences on Cybertheft complicate China Talks', *The New York Times* (10.07.2013)
<www.nytimes.com/2013/07/11/world/asia/differences-on-cybertheft-complicate-china-talks.html?ref=technology>

Schmidt M and Sanger D, '5 in China Army Face U.S. Charges of Cyberattacks', *The New York Times* (19.05.2014)

<www.nytimes.com/2014/05/20/us/us-treads-fine-line-in-fighting-chinese-espionage.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer>

Staff, 'Documents Reveal Top NSA Hacking Unit', *Spiegel* (29.12.2013) <www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html>

Stein J, 'Israel won't stop spying on the U.S.', *Newsweek* (06.05.2014) <www.newsweek.com/2014/05/16/israel-wont-stop-spying-us-249757.html>

Stuster D, 'Russia, Iran, Iraq, and Syria to Share Intelligence on Islamic State', *Foreign Policy* (28.09.2015) <foreignpolicy.com/2015/09/28/russia-iran-iraq-and-syria-to-share-intelligence-on-islamic-state/>

Sullivan S, 'Obama: North Korea hack "cyber-vandalism," not "act of war"', *The Washington Post* (21.12.2014) <www.washingtonpost.com/news/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/?utm_term=.fa09e66b5422>

Tabassum Z, 'U.S. blames China, Russia for cyber espionage', *Reuters* (03.11.2011) <www.reuters.com/article/us-usa-cyber-china-idUSTRE7A23FX20111103>

'Text: Bush Signs Anti-Terrorism Legislation', *The Washington Post* (25.10.2001) <www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushtext_102601.html>

Untersinger M, 'Cyberattaques : la France menace de « mesures de rétorsion » tout Etat qui interférerait dans l'élection', *Le Monde* (15.02.2017) <www.lemonde.fr/pixels/article/2017/02/15/cyberattaques-la-france-menace-de-mesures-de-retorsion-tout-etat-qui-interfererait-dans-l-election_5080323_4408996.html>

Untersinger M, 'Cybersécurité : pour Jean-Yves Le Drian, "la menace est à nos portes"', *Le Monde* (25.01.2017) <www.lemonde.fr/pixels/article/2017/01/25/cybersecurite-menaces-averees-ou-marketing-de-la-peur_5068669_4408996.html>

Valadés B, 'El ciberespionaje persigue información de altísimo valor y debe considerarse una amenaza crítica', *Red Seguridad* (15.06.2015)

<www.redseguridad.com/instituciones/administracion/el-ciberespionaje-persigue-informacion-de-altisimo-valor-y-debe-considerarse-una-amenaza-critica>

Valerio I, 'Bernard Kouchner : "Nous écoutons aussi, mais nous n'avons pas les moyens des Etats-Unis, ça rend jaloux"', *Europe1* (22.10.2013) <lelab.europe1.fr/bernard-kouchner-nous-ecoutons-aussi-mais-nous-n-avons-pas-les-moyens-des-etats-unis-ca-rend-jaloux-11328>

'WikiLeaks: US spied on Angela Merkel's minister too, says German newspaper', *The Guardian* (02.07.2015) <www.theguardian.com/media/2015/jul/02/wikileaks-us-spied-on-angela-merkels-ministers-too-says-german-newspaper>

Wilkinson T, 'Israel Refuses Apology to Swiss in Spy Scandal', *Los Angeles Times* (27.02.1998) <http://articles.latimes.com/1998/feb/27/news/mn-23642>

Williams C, 'Cyber espionage virus targets Lebanese banks', *Telegraph* (10.08.2012) <www.telegraph.co.uk/technology/internet-security/9466718/Cyber-espionage-virus-targets-Lebanese-banks.html>

Woolsey J, 'Why We Spy on Our Allies', *Wall Street Journal* (17.03.2000) <www.wsj.com/articles/SB95326824311657269>

Online articles

'How TCP/IP Works' (*Microsoft,* 29.10.2008) <https://technet.microsoft.com/pt-pt/library/cc786128(v=ws.10).aspx>

'IT Infrastructure' (*DELL-EMC Glossary*) <www.emc.com/corporate/glossary/it-infrastructure.htm>

MacMichael D, 'Windows Network Architecture and the OSI Model' (*Microsoft*, 20.04.2017) <https://docs.microsoft.com/fr-fr/windows-hardware/drivers/network/windows-network-architecture-and-the-osi-model>

'Paul Baran and the Origins of the Internet' (*RAND*) <www.rand.org/about/history/baran.html>

'Practice Relating to Rule 107. Spies' (*ICCR*)

<ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule107_sectionb>

'Route Control' (*Technopedia*)
<www.techopedia.com/definition/2532/route-control accessed>

'Tapping of fibre networks' (*Deloitte*, 2017)
<https://zybersafe.com/wordpress/wp-content/uploads/2018/01/Deloitte_Fiber_tapping_Q1_2017_English.pdf>

'TCP/IP Protocols' (*IBM*)
<www.ibm.com/support/knowledgecenter/en/ssw_aix_72/com.ibm.aix.networkcomm/tcpip_protocols.htm>

'The Geneva Conventions of 1949 and their Additional Protocols' (*ICRC*, 01.01.2014)
<www.icrc.org/en/document/geneva-conventions-1949-additional-protocols>

'What does ICANN Do?' (*ICANN*)
<www.icann.org/resources/pages/what-2012-02-25-en>

Videos

Corten O, 'La légitime défense préventive: un oxymore?' (*UN WebTV,* 24.03.2017)
<http://webtv.un.org/watch/olivier-corten-sur-la-l%C3%A9gitime-d%C3%A9fense-pr%C3%A9ventive-un-oxymore/5511732829001>

'Guillaume Poupard : "Il faut établir le droit international dans le cyberespace"' (*France24,* 03.04.2017)
<www.youtube.com/watch?v=4qEq0AR-GzI>

'Sixth Committee 15th meeting, 69th General Assembly' (*UN Web TV,* 14.10.2014)
<http://webtv.un.org/watch/sixth-committee-14th-meeting-69th-general-assembly/3849676513001>

RESUME SUBSTANTIEL DE LA THESE / EXTENDED SUMMARY

INTRODUCTION

1. Structure et Choix Méthodologiques

Les Etats s'espionnent depuis des siècles. Malgré les tensions provoquées par l'espionnage, on ne trouve de régulation expresse de ce comportement qu'en temps de guerre. Dans ce cadre, il est paradoxalement admis que l'Etat qui envoie des espions en territoire étranger ne viole pas le droit international. En revanche–et s'il est capturé–l'agent pourra être jugé. En temps de paix, les Etats se satisfont d'une appréhension indirecte de l'espionnage. En droit international, celle-ci est permise par l'application de la règle de souveraineté : l'envoi d'un agent en territoire étranger sans le consentement de celui-ci en est une violation. Ensuite, en vertu de sa législation pénale, l'Etat qui capture un espion peut tout à fait le juger. Toutefois, ces règles ont vocation à s'appliquer sur un territoire, une notion intrinsèquement physique. Or, le cyber-espionnage est une activité dématérialisée, et ne requiert plus l'envoi d'un agent sur un territoire étranger.
La thèse a donc pour objectif spécifique d'étudier les conséquences qu'ont la dématérialisation et la déterritorialisation de l'espionnage sur sa régulation par le droit international. La structure de la thèse met ce but en évidence, en organisant l'étude des instruments juridiques existants selon leur *connexion à l'intégrité territoriale* (partie I) ou leur *déconnexion de l'intégrité territoriale* (partie II). La première partie regroupe en son sein *le principe de souveraineté* (chapitre 1), *le principe de non-intervention* (chapitre 2), le *jus ad bellum* (chapitre 3) et le *jus in bello* (chapitre 4). La seconde partie inclut quant à elle *la Convention de Vienne sur les Relations diplomatiques* (chapitre 1), et l'*Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce* (chapitre 2). Enfin, la thèse s'interroge sur l'existence de nouvelles *règles coutumières spécifiques au cyber-espionnage* (partie III). Par ailleurs, elle propose d'établir et de comparer tant l'*état de la doctrine* que l'*état du droit*. Cette binarité se retrouve au cœur de chaque chapitre, et en forge les subdivisions.

L'introduction établit tout d'abord les objectifs de la recherche, ainsi que les méthodes utilisées pour les remplir.

a) Afin d'établir l'*état de la doctrine*, les arguments utilisés par les auteurs sont identifiés, et une classification de leurs modes de raisonnement est opérée.
b) Afin de contribuer à l'établissement de l'*état du droit*, les règles d'interprétation contenues dans la Convention de Vienne sur le Droit des Traités sont appliquées aux dispositions conventionnelles existantes en vue d'établir leur pertinence quant au cyber-espionnage.
c) Il est fait usage des conclusions de la Commission du Droit International (CDI) sur l'identification du droit international coutumier afin de

déterminer si des règles coutumières spécifiques au cyber-espionnage existent.

d) La potentielle contradiction entre le cyber-espionnage et les règles de souveraineté et de non-intervention est établie.
e) L'*état de la doctrine* et *l'état du droit* sont comparés, afin de révéler les failles du premier.

2. Applicabilité du droit international au cyberespace

Le cyberespace est souvent présenté comme un nouveau domaine, qui se distinguerait de la terre, de la mer, des espaces aériens et extra-atmosphériques. Par conséquent, la question d'une possible transposition du droit international existant se pose. Cette applicabilité est en fait reconnue par de nombreux Etats : Australie, Canada, Etats-Unis, Géorgie, Inde, Japon, Mexique, Nouvelle-Zélande, Pologne, Royaume-Uni, Russie, Suède. Toutefois, certains Etats soulignent encore les incertitudes affectant les modalités de transposition du droit international en pratique (Finlande, France, Italie, Pays-Bas), tandis qu'une minorité réclame de nouvelles règles (Autriche et Suisse).

3. Définition du cyberespace et du cyber-espionnage

3.1. Définition du Cyberespace

En ce qui concerne le cyberespace, la thèse souligne une différence de perception entre deux groupes d'Etats.

D'une part, la Russie, la Chine, le Kazakhstan, le Kirghizistan, le Tadjikistan et l'Ouzbékistan n'utilisent pas nécessairement la notion de 'cyberespace', mais font davantage référence à un 'espace d'information'. Celui-ci inclurait 'l'étendue des activités relatives à la création, la transformation, le transfert, l'utilisation et le stockage information qui influencent, en particulier, la pensée individuelle et collective, l'infrastructure informatique et l'information elle-même' (Ordre du gouvernement russe du 30 avril 2015, 'On signing the Agreement between the Government of the Russian Federation and the Government of the people's Republic of China on cooperation in ensuring international information security'). La thèse note, toutefois, que le terme 'cyberespace' n'est pas totalement absent des discours russes et chinois, et est notamment utilisés par leur Ministère des Affaires Etrangères respectifs.

D'autre part, une quarantaine d'Etats utilise le terme 'cyberespace', sans toutefois parvenir à une définition commune. Une dizaine d'Etats recourt au terme 'cyberespace' sans le définir (Chili, Egypte, Guatemala, Irlande, Jordanie, Paraguay, Rwanda, Sénégal, Singapour, Tanzanie, Ouganda, et Zimbabwe), mais l'étude des définitions de douze autres Etats (Afghanistan, Allemagne, Canada, Colombie, République tchèque, Israël, Lettonie, Mexique, Pologne, Qatar,

Royaume-Uni, Turquie, Nouvelle-Zélande) permet d'identifier des éléments de convergence. En effet, toutes ces définitions s'articulent autour de deux éléments : 1) la nature du cyberespace; et 2) les éléments constitutifs du cyberespace. D'autres configurations sont toutefois possibles : certains Etats ajoutent un troisième élément constitutif, basée sur interactions permises par le cyberespace (Colombie, Mexique), d'autres combinent éléments constitutifs du cyberespace et ces mêmes interactions (Philippines, Trinidad-et-Tobago), tandis que cinq autres adoptent une définition centrée sur les éléments constitutifs du cyberespace (Hongrie, Maroc, Slovénie et Pays-Bas). La thèse note alors que toutes ces éléments sont représentés dans la définition ISO du cyberespace, que la recherche fait alors sienne : 'un environnement complexe, résultant de l'interaction de personnes, de logiciels et de services sur Internet au moyen de dispositifs technologiques et de réseaux qui y sont connectés, et n'ayant pas d'existence physique' (ISO, 'Information technology–Security techniques–Guidelines for cybersecurity').

3.2. Définition du Cyber-espionnage

Vient ensuite la définition du cyber-espionnage. En dépit de la diversité des termes utilisés ('attaque de réseau informatique', 'cyber-attaque', 'sabotage', 'espionnage de réseau informatique', 'cyber-espionnage'), la thèse note que de nombreux Etats opèrent une distinction entre les opérations portant atteinte à l'*intégrité* ou la *disponibilité* d'un système informatique, et les simples *intrusions* dans le but de *collecter des informations* (Allemagne, Australie, Autriche, Belgique, Canada, Etats-Unis, Pays-Bas, Royaume-Uni). La thèse qualifie alors les premières de *cyber-attaques*, tandis que les secondes rentreront dans le champ du *cyber-espionnage.* Ces éléments restent valides pour les Etats qui se contentent de définir une seule des deux notions : 'cyber-attaque' (Colombie, Pologne, Turquie, Maroc) et 'cyber-espionnage' (Afrique du Sud, Monténégro, Nigeria, Philippines). Ces définitions s'articulent toujours autour des mêmes éléments.

La relation entre 'cybercriminalité', 'cyber-sécurité' et 'cyber-espionnage' est ensuite éclaircie. La thèse note qu'une vingtaine d'Etats s'accordent pour dire que le but de la 'cyber-sécurité' est de préserver la confidentialité, l'intégrité et la disponibilité des données. Dans la mesure où le cyber-espionnage porte atteinte à la confidentialité des données, il va à l'encontre de la cyber-sécurité. En ce qui concerne la cybercriminalité, la thèse note que de plus en plus d'Etats s'engagent à adopter des règles relatives aux cyber-intrusions dans leurs législations pénales, par exemple à travers la *Convention du Conseil de l'Europe contre la Cybercriminalité.* Des cyber-espions gouvernementaux pourraient donc tout à fait être poursuivis devant des juridictions étrangères.

Ce raisonnement permet à la thèse de donner la définition suivante du cyber-espionnage : 'une activité menée à distance par un Etat, cherchant un accès non autorisé à des données confidentielles basées sur un système informatique, au moyen de réseaux informatiques, afin de collecter des informations'.

4. Modes de raisonnement

Les modes de raisonnement mis en œuvre dans la thèse sont ensuite exposés : il s'agit de l'interprétation des traités, et la théorie des sources. La vision qu'a la thèse de la *pratique étatique* est également développée.

4.1. L'interprétation des traités

Les règles d'interprétation des traités ont été consacrées par la Convention de Vienne sur le Droit des Traités (1969). Celle-ci définit une règle générale d'interprétation (article 31) et des moyens complémentaires d'interprétation (article 32). L'article 31 mentionne que le 'traité doit être interprété de bonne foi suivant le sens ordinaire à attribuer aux termes du traité dans leur contexte et à la lumière de son objet et de son but'. Ce contexte inclue le texte, le préambule, les annexes, '[t]out accord ayant rapport au traité et qui est intervenu entre toutes les parties à l'occasion de la conclusion du traité', et '[t]out instrument établi par une ou plusieurs parties à l'occasion de la conclusion du traité et accepté par les autres parties en tant qu'instrument ayant rapport au traité'. Outre le contexte, il doit être tenu compte de 'tout accord ultérieur intervenu entre les parties au sujet de l'interprétation du traité ou de l'application de ses dispositions', de 'toute pratique ultérieurement suivie dans l'application du traité par laquelle est établi l'accord des parties à l'égard de l'interprétation du traité', et de 'toute règle pertinente de droit international applicable dans les relations entre les parties'. Lorsque le sens reste 'ambigu ou obscur', ou '[c]onduit à un résultat qui est manifestement absurde ou déraisonnable', l'article 32 permet un recours 'aux travaux préparatoires et aux circonstances dans lesquelles le traité a été conclu'. Il peut également y être fait recours afin de confirmer 'le sens résultant de l'application de l'article 31'.

Toutefois, la Convention de Vienne ne traite pas de certaines modalités d'interprétation.
Pour les traités 'ordinaires'–par opposition aux traités constitutifs des organisations internationales–il s'agit des interprétation *évolutives*, *strictes* et *extensives*. L'étude de la jurisprudence révèle que c'est toujours vis-à-vis de l'intention des parties, telle que reflétée dans le texte, que le traité doit être interprété. En ce qui concerne l'interprétation évolutive, la CIJ a déterminé que 'lorsque les parties ont employé dans un traité certains termes de nature générique, dont elles ne pouvaient pas ignorer que le sens était susceptible d'évoluer avec le temps, et que le traité en cause a été conclu pour une très longue période ou "sans limite de durée", les parties doivent être présumées, en règle générale avoir eu l'intention de conférer aux termes en cause un sens évolutif' (*Différend relatif à des droits de navigation et des droits connexes* (*Costa Rica c. Nicaragua)* (arrêt), [66]).

Certaines spécificités concernent les traités constitutifs des organisations internationales. En effet, '[l]es compétences conférées' à celles-ci 'font normalement l'objet d'une formulation expresse dans leur acte constitutif. Néanmoins, les exigences de la vie internationale peuvent mettre en lumière la nécessité pour les organisations de disposer, aux fins d'atteindre leurs buts, de compétences subsidiaires non expressément prévues dans les textes fondamentaux qui gouvernent leur activité. Il est généralement admis que les organisations internationales peuvent exercer de tels pouvoirs dits "implicites"' (CIJ, *Licéité de l'utilisation des armes nucléaires par un Etat dans un conflit armé*, avis consultatif, para 25). Par ailleurs, '[d]e tels traités peuvent poser des problèmes d'interprétation spécifiques en raison, notamment, de leur caractère à la fois conventionnel et institutionnel'. Certains éléments vont donc jouir d'une 'attention spéciale au moment d'interpréter ces traités constitutif' (*Licéité de l'utilisation des armes nucléaires dans un conflit armé* (avis consultatif) [19]). L'intention des parties, telle que reflétée dans le texte, guide donc toujours l'interprétation.

La thèse applique cette méthode tant dans la première partie (*Jus ad Bellum* et *Jus in Bello*) que dans la seconde (*Convention de Vienne sur les Relations Diplomatiques, l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce*).

4.2. La théorie des sources

La théorie des sources (droit international coutumier) est ensuite à l'étude. Selon la doctrine dominante de la CIJ et de la CDI, la coutume comprend deux éléments constitutifs : une pratique générale, qui doit être acceptée comme étant le droit (ou *opinio juris*). Comme le précise les conclusions de la CDI sur l'Identification du droit international coutumier, les actes législatifs, exécutifs et judiciaires permettent d'établir la première, tandis que les déclarations publiques des Etats, les publications officielles, les avis juridiques des gouvernements et des dispositions conventionnelles caractérisent le second. Ensuite, la 'présence' de 'règles coutumières' dans 'l'*opinio juris* des Etats' se 'prouve par voie d'induction en partant de l'analyse d'une pratique suffisamment étoffée et convaincante, et non pas par voie de déduction en partant d'idées préconstituées à priori' (CIJ, *Délimitation de la frontière maritime dans la région du golfe du Maine (Canada/Etats-Unis d'Amérique)* (arrêt) [111]).
La thèse décide donc d'appliquer cette méthode dans la partie III, en soulignant toutefois–et après une analyse rigoureuse de la jurisprudence de la CIJ– que la Cour elle-même ne respecte pas toujours cette méthode (recours à la déduction, analyse inégale des deux éléments constitutifs).

4.3. La pratique étatique

Après avoir expliqué que la thèse suivait adoptait une méthode basée sur les sources du droit international et centrée sur l'Etat, la vision qu'elle a de la

pratique étatique est développée ici. Les conclusions de la CDI concernant les « Accords et pratique ultérieurs dans le contexte de l'interprétation des traités » ainsi que sur l'identification du droit international coutumier sont rappelées ici. Il s'agit en l'occurrence de montrer que la vision de la pratique développée par les premières est plus large que celle des secondes, permet d'englober la grande diversité de documents utilisée dans la thèse. Faute de consignes concernant l'application des règles de souveraineté et de non-intervention, il est expliqué qu'une large vision de la pratique étatique prévaudra également dans leur analyse.

PREMIERE PARTIE – LES REGLES CONNECTEES A L'INTEGRITE TERRITORIALE

I – LA REGLE DE SOUVERAINETE

1. Etat de la doctrine

La doctrine relative à l'espionnage traditionnel s'accorde pour dire que cette activité constitue une violation de souveraineté [Chesterman, Williams, Cohen-Jonathan et Kovar]. Toutefois, cette illégalité réside-t-elle dans l'activité d'espionnage *per se* ou dans la pénétration non-consensuelle en territoire étranger, qui est son corollaire ? C'est le point soulevé par certains auteurs, qui distinguent les deux [Stone, Lafouasse, Kraska, McDougal, Lasswell, Reisman].
Ces deux courants de pensée se retrouvent dans la doctrine relative au cyber-espionnage. Les auteurs opèrent généralement une analogie entre le régime applicable au cyber-espionnage et celui de l'espionnage traditionnel, pour deux résultats différents. Certains considèrent que le cyber-espionnage constitue une violation de souveraineté [Antolin-Jenkins, Buchan, Parajon-Skinner, Schneier], à l'image de l'espionnage traditionnel [Delerue, Shoshan]; d'autres considèrent qu'en l'absence d'incursion physique, le cyber-espionnage est une activité légale [Beard, Goldsmith, Sharp].

2. Etat du droit

Cette nécessité de distinguer entre espionnage *per se* et incursion physique est validée par la thèse. De nombreuses affaires d'espionnage parsèment en effet les relations internationales. Leur étude révèle que, dans le discours des Etats victimes, c'est toujours l'intrusion physique–et jamais l'espionnage en lui-même– qui est dénoncée. A l'opposé, les Etats auteurs estiment que la collecte de 'renseignement' est essentielle à la protection de leur sécurité nationale, afin de se prémunir contre de potentielles attaques.
En ce qui concerne la relation entre cyber-espionnage et souveraineté, le discours des Etats est beaucoup plus hétérogène.

Suite aux révélations sur la NSA, seuls le Parlement européen, le MERCOSUR, l'UNASUR, la Bolivie, le Brésil et la Russie ont dénoncé une violation de souveraineté. La Belgique et l'Equateur ont quant à eux estimé que seul l'espionnage à grande échelle constituait une violation de souveraineté. Le département de la Défense des États-Unis, le gouvernement canadien, l'Australie et les Bahamas considèrent le cyber-espionnage comme une potentielle violation de souveraineté, sans toutefois adopter une position définitive. Le département d'Etat américain, le parlement canadien, la France, la Suisse, le Royaume-Uni estiment que le cyber-espionnage ne constitue pas une violation de souveraineté. En insistant sur la différence entre la collecte de renseignement et l'interruption/altération des systèmes–qualifiant seulement ces dernières de violation de souveraineté–la Finlande parvient à la même conclusion.

Ce qui n'est pas dit par les Etats lorsqu'ils sont victimes de cyber-espionnage est également d'importance. En l'occurrence, jamais la France ni l'Allemagne n'ont qualifié l'espionnage par la NSA de violation de souveraineté. François Hollande a considéré la pratique comme 'inacceptable' tandis qu'Angela Merkel estimait que 'l'espionnage entre amis, ça ne va pas du tout'. L'Indonésie a qualifié des activités d'espionnage menées par l'Australie comme 'inamicale' tandis que les Etats-Unis, l'Allemagne et l'Australie ont refusé de blâmer la Chine pour des actions similaires. Par ailleurs, la Suisse, le Royaume-Uni, le Danemark, la Finlande, l'Islande, la Norvège, la Suède et les Etats-Unis ont renoncé à l'adoption de règles contraignantes concernant le cyber-espionnage ou le cyberespace.

Au vue de cette extrême hétérogénéité, la thèse conclut que le cyber-espionnage ne constitue pas une violation de souveraineté. En effet, les Etats se contentent de réagir conformément à ce que leur dictent leurs intérêts : les Etats-Unis, puissance économique majeure engluée dans le scandale de la NSA, tentent d'instaurer un régime binaire, distinguant espionnage économique et politique; l'Allemagne, la France, et le Royaume-Uni–des espions notoires–nient la contradiction entre cyber-espionnage et souveraineté ; la Belgique, qui reconnait des activités d'espionnage 'modérées' et doit respecter la Convention Européenne des Droits de l'Homme, condamne le seul espionnage à grande échelle. Certains Etats font preuve d'une approche plus subtile, parvenant au même résultat, mais par des voies détournées : qualification de la seule cyber-attaque comme violation de souveraineté (Finlande), référence exclusive au droit interne (Estonie, services secrets finlandais et suédois), soutien de l'adoption de mesures non contraignantes (Danemark, Finlande, Islande, Norvège, Suède). La thèse estime en revanche que les positions australiennes, bahamiennes et néerlandaises sont délibérément vagues ou ambiguës, ces Etats n'ayant probablement pas de position définitive sur la question. Quant aux Etats sud-américains, leur qualification consensuelle du cyber-espionnage comme violation de souveraineté est sans doute liée à leur statut de perdant du 'grand jeu'.

II – LA REGLE DE NON-INTERVENTION

L'arrêt de la CIJ dans l'affaire opposant le Nicaragua et les Etats-Unis permet d'identifier les deux composantes du principe de non-intervention : 'l'intervention interdite' doit 'porter sur des matières à propos desquelles le principe de souveraineté des Etats permet à chacun d'entre eux de se décider librement'–notamment le 'choix du système politique, économique, social et culturel et de la formulation des relations extérieures'–et utiliser 'des moyens de contrainte' (Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique)(arrêt) [206]).

1. Etat de la doctrine

Les auteurs ne parviennent pas à un consensus quant à la qualification de l'espionnage comme une intervention prohibée. Certains considèrent que, dans la mesure où il viole la législation de l'Etat visée, il y a intervention subversive [Wright], d'autres font état d'une certaine ambiguïté [McDougal, Lasswell et Reisman]. En revanche, tous considèrent que l'élément de contrainte est manquant pour l'interception des télécommunications [Peters, Talmon]. Les avis au sujet du cyber-espionnage sont plus partagés. Certains considèrent que l'élément de contrainte est présent [Jupillat], absent [Banks, Kilovaty, Ohlin, Watts, Van de Velde], ou spécifique au cyber-espionnage économique [Lotrionte, Parajon-Skinner, Barkham]. D'autres estiment qu'il y a juridiction exclusive de l'Etat sur ses secrets [Buchan, Shull], ses secrets économiques [Parajon-Skinner, Lotrionte], ou nient une telle juridiction [Ohlin].

2. Etat du droit

L'influence de l'espionnage avec le 'choix du système politique, économique, social et culturel et de la formulation des relations extérieures' est ensuite démontrée. Pour ce faire, ces termes–mentionnés par la CIJ dans l'affaire du Nicaragua–sont définis dans un premier temps ('choix', 'système politique', 'système économique', 'système social', 'culture' et 'relations extérieures'). Dans un second temps, une analyse de la pratique étatique révèle que la plupart des Etats considèrent effectivement l'espionnage comme une interférence avec ces éléments.

Cependant–et après avoir défini la notion–la recherche estime que le recours à des 'moyens de contrainte' manquent dans le cas de l'espionnage. En effet, le cyber-espionnage ne force à aucun moment un Etat à adopter–ou à ne pas adopter–telle ou telle mesure. De plus, la plupart des Etats–notamment à l'occasion de la définition des activités de leurs services secrets–distinguent l'espionnage d'activités plus déstabilisantes, comme celles dirigées contre l'indépendance de l'Etat ou la pérennité des institutions.

La thèse conclut que le cyber-espionnage en soi ne constitue pas une intervention prohibée. La divulgation au grand public d'informations obtenues

à l'occasion d'un acte d'espionnage–comme ce fut le cas lors du piratage du Comité National Démocrate–doit alors être distinguée de l'espionnage *per se*. La première situation est en effet plus ambiguë.

III – LE JUS AD BELLUM

Selon l'article 2(4) de la Charte des Nations Unies, '[l]es Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies'. Selon l'article 51, '[a]ucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales […]'. La Charte des Nations Unies porte donc son attention sur un instrument précis : le recours à la force armée.
La plupart des Etats ont reconnu l'applicabilité de la Charte des Nations Unies dans le cyberespace (Australie, Chili, Etats-Unis, Géorgie, Allemagne, Qatar, Suède, Danemark, Islande, Norvège, Chine, Russie, Kazakhstan, Kirghizstan, Tadjikistan et Ouzbékistan, Royaume-Uni, Slovaquie, Croatie, Malte, Mexique). D'autres reconnaissent une telle applicabilité, mais soulignent des divergences de la communauté internationale ou font appel à davantage de travaux sur le sujet (Canada, Finlande, Japon).

1. Etat de la doctrine

Les auteurs s'accordent pour dire que l'espionnage traditionnel ne constitue pas un recours à la force ou une agression armée [Lubin, Weissbrodt, Blake and Imburgia]. La doctrine relative au cyber-espionnage est en revanche beaucoup plus hétérogène, mais l'on retrouve deux principaux types de raisonnement.

Le premier est le recours à des méta-principes d'interprétation, avec tout d'abord l'approche *conséquentialiste*. Celle-ci se concentre sur les effets d'une cyber-opération : s'ils causent une destruction dans le monde physique ou affectent l'intégrité de données dans le monde virtuel, alors on considère qu'il y a violation de la Charte des Nations Unies, car ses effets sont similaires à ceux qu'aurait une attaque armée. C'est généralement sous la qualification de 'cyber-attaque' que les auteurs réfèrent à des activités ayant cet effet, tandis que le cyber-espionnage n'est pas perçu comme une violation de la Charte. En effet, ils considèrent que les données sont simplement copiées [Hanford, Gervais, Watts, Schaap, Buchan, Weissbrodt, Solis, Shackelford, Andres, Blank, Wortham, Poché]. De rares auteurs, traitant du cyber-espionnage économique, estiment toutefois que cette

activité va à l'encontre de la Charte [Barkham, Brenner and Crescenzi, Melnitzky].
On retrouve ensuite le raisonnement *analogique*. Certains auteurs considèrent en effet que–l'espionnage traditionnel n'ayant jamais été perçu comme contraire à la Charte–il en va de même pour le cyber-espionnage [Gervais, Roscini, Kostadinov, Lotrionte, Lobel, Schmitt, Lin]. Les références à l'affaire du U-2 (durant laquelle un projet de résolution porté par l'URSS, et qualifiant le survol de son territoire par un avion espion américain de recours à la force fut rejeté par le Conseil de Sécurité) sont récurrentes. En effets, ces auteurs considèrent que, si une telle intrusion physique ne peut être considérée comme une violation de la Charte, alors il ne peut en aller autrement du cyber-espionnage [Antolin-Jenkins, Sharp, Wingfield, Pelican].
La troisième et dernière forme de méta-principe fait appel à la *cible* de la cyber-opération. A partir du moment où celle-ci est dirigée contre un système vital aux intérêts de l'Etat visé–et peu importe son objectif ou ses effets–alors l'Etat serait en droit d'invoquer la légitime défense [Sharp, Joyner and Lotrionte].

Un second type de raisonnement est plus classique, et fait appel à la volonté initiale des parties ou à leur pratique subséquente. Les auteurs font valoir que jamais les Etats n'ont souhaité prohiber la collecte d'information ou les intrusions virtuelles dans la Charte [Beard, O'Connell, Sulmasy and Yoo], ou ont continuellement eu recours à l'espionnage et n'ont jamais répliqué par la force lorsqu'ils étaient victimes de telles activités [Kirchner, Shackelford and Andres].

2. Etat du droit

2.1. Définition des notions centrales de la Charte des Nations Unies

Afin d'établir l'état du droit, la thèse propose de recourir à l'interprétation des articles 2(4) et 51 de la Charte des Nations Unies, et commence par définir les termes clés de ces deux articles.

Dans l'article 2(4), les termes méritant une telle attention sont 'menace ou emploi de la force', 'contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies' et 'relations internationales'.
La thèse soutient que la notion de 'force' se limite à la seule force *armée*. L'analyse du contexte, de la pratique subséquente et des travaux préparatoires permet de tirer cette conclusion. En effet, l'article 44 de la Charte connecte 'recours à la force' et 'force armée', tandis que la CIJ qualifie les seules interventions militaires d'une certaine ampleur et d'une certaine durée comme violation de l'article 2(4) (*Activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda)* (arrêt) [165]). Enfin, une proposition brésilienne visant à inclure certaines

mesures économiques dans la définition de menace ou de recours à la force fut rejetée.
Afin de définir 'intégrité territoriale', la thèse fait appel aux travaux de Blay, qui estime qu'elle fait référence au contrôle effectif et à la possession d'un territoire. En ce qui concerne l'atteinte à l'indépendance politique d'un Etat, Blay estime qu'elle est atteinte dès lors que des actes étrangers visent à prendre le contrôle d'organes étatiques ou à influencer leur capacité de décision par le biais de menace, recours à la force, ou autre moyens subversifs [Blay].
Enfin, 'toute autre manière incompatible avec les buts des Nations Unies' peut designer divers comportements, tels que l'appui à de mouvements séparatistes ou d'actes terroristes au détriment territoire d'un autre Etat.
Quant à 'relations internationales', le terme doit être compris comme 'relations interétatiques'.

En ce qui concerne l'article 51, la version française de la Charte permet d'affirmer que seule l'*agression armée* permet d'activer la légitime défense. Cette interprétation est consolidée par les exemples d'agression recensés dans la résolution 3314 de l'Assemblée Générale des Nations Unies (invasion, occupation, bombardement ou emploi d'armes à l'encontre d'un territoire étranger, blocus, attaques contre les forces armées d'un autre Etat, violation d'un accord de stationnement de troupes, mise à disposition de son territoire en vue de commettre une agression, envoi de forces armées irrégulières).

2.2. Définition de l'objet et du but de la Charte des Nations Unies

L'objet et le but de la Charte sont ensuite définis, grâce au préambule et à son article 1. Il s'agit du maintien de la paix, de réaffirmer la 'foi dans les droits fondamentaux de l'homme, dans la dignité et la valeur de la personne humaine, dans l'égalité de droits des hommes et des femmes, ainsi que des nations, grandes et petites', 'favoriser le progrès social et instaurer de meilleures conditions de vie dans une liberté plus grande', la 'justice' et le 'respect des traités'.

2.3. Evaluation du traité

La thèse montre que le recours aux méta-principes d'interprétation, si commun dans la doctrine, demeure en fait litigieux. L'approche conséquentialiste n'a en effet été reconnue que par 7 Etats (Belgique, Etats-Unis, France, Hongrie, Pays-Bas, Royaume-Uni, Suisse), tandis que seuls les Etats-Unis et la Suisse ont recours à un raisonnement analogique. Enfin, une trentaine d'Etats reconnaissent l'existence d'infrastructures vitales, mais aucun n'affirme que leur simple ciblage constitue un recours à la force (Afghanistan, Autriche, Bangladesh, Belgique, Colombie, Chypre, République Tchèque, Estonie, Ethiopie, Finlande, Allemagne, Ghana, Hongrie, Italie, Irlande, Côte d'ivoire, Jamaïque, Japon, Jordanie, Kenya, Lituanie, Luxembourg, Malaisie, Ile Maurice,

Monténégro, Norvège, Paraguay, Qatar, Rwanda, Arabie Saoudite, Slovaquie, Afrique du Sud, Trinidad-et-Tobago, Turquie, Ouganda). Bien ayant pris parti en faveur de l'approche conséquentialiste, les Pays-Bas reconnaissent que de plus amples travaux sont nécessaires pour éclairer le cadre juridique applicable. Ils sont accompagnés dans cette démarche par l'Australie, la Corée du Sud, l'Espagne, l'Inde, le Japon, le Qatar.

De plus, l'espionnage n'équivaut pas à un recours à la force. Il a été précédemment expliqué que la Charte visait à prévenir le recours à la force armée. Or, les définitions d'une 'arme' pointent toutes dans la même direction : il s'agit d'un objet conçu ou utilisé pour infliger des dommages corporels ou physiques. Un logiciel espion rentre difficilement dans cette définition. Par ailleurs, seuls les Etats-Unis, la Slovaquie et la Russie envisagent l'existence d'armes dans le cyber-espace. L'Arrangement de Wassenaar et le règlement européen 428/2009 font bien mention des 'logiciels d'intrusion', mais les classent dans la catégorie des biens à double-usage. Quant au Traité sur le Commerce des Armes des Nations Unies, il ne fait pas référence aux logiciels informatiques. Ensuite, le cyber-espionnage ne peut être rattaché à aucune des activités mentionnées dans la résolution 3314 qui, bien que n'étant pas exhaustive, implique systématiquement une intrusion physique. En ce qui concerne d'autres formes de pratique étatique, les Etats-Unis, la Finlande, et les Pays-Bas estiment qu'une simple intrusion n'équivaut pas à une attaque armée. *A contrario,* le Mexique et l'Indonésie ont qualifié la surveillance extraterritoriale de violation de la Charte des Nations Unies.

Ensuite, le cyber-espionnage ne viole pas l'intégrité territoriale et l'indépendance politique d'un Etat, comme cela a été démontré dans les précédents chapitres de la thèse. De plus, la pratique étatique montre que même les actes d'espionnage impliquant une intrusion territoriale n'ont jamais été considérés comme une violation de la Charte des Nations Unies. Comme expliqué précédemment, les débats tenus au Conseil de Sécurité suite à l'abattage d'un avion espion américain au-dessus du territoire soviétique en témoignent.

Enfin, l'espionnage n'est pas contraire à l'objet et au but de la Charte. Les Etats reconnaissent en effet ouvertement mener des activités de renseignement dans le cyberespace (Allemagne, Australie, Arabie Saoudite, Bulgarie, France, Etats-Unis, Mexique, République Tchèque, Royaume-Uni, Nouvelle Zélande, Pays-Bas, Pologne, Israël, Slovaquie). De leur doctrine, il ressort une justification essentielle : se prémunir contre d'éventuelles attaques extérieures.

La thèse conclue donc que le cyber-espionnage ne peut en aucun cas être considéré comme une violation de la Charte des Nations Unies.

IV – LE JUS IN BELLO

1. Etat de la doctrine

1.1. L'espionnage entre belligérants

L'espionnage entre belligérants est expressément autorisé par les Conventions de La Haye *concernant les lois et coutumes de la guerre sur terre* (1899, 1907) et le Protocole Additionnel I aux Conventions de Genève. Néanmoins, si l'espion est capturé, il pourra être jugé, voire exécuté.
Par conséquent, la quasi-totalité des auteurs a recours à l'analogie entre espionnage traditionnel et cyber-espionnage, et démontre la légalité de ce dernier [McGavran, Aldrich, Solis, Schaap, Kirchner, Joyner et Lotrionte].

1.2. L'espionnage impliquant un Etat neutre

Un corpus de règles différent s'applique dans les relations entre un belligérant et un Etat neutre. Sur terre, il s'agit de la *Convention (V) concernant les droits et les devoirs des Puissances et des personnes neutres en cas de guerre sur terre.* Sur mer, il s'agit de la *Convention (XIII) concernant les droits et les devoirs des Puissances neutres en cas de guerre maritime.* Des Règles de la guerre aérienne existent par ailleurs, mais ne sont jamais entrées en vigueur. Deux courants doctrinaux sont identifiables.

Le premier repose sur les articles 1, 2 et 3 de la Convention V, sur l'article 5 de la Convention XIII et les Règles de la guerre aérienne. Ces articles énoncent respectivement l'inviolabilité du territoire des puissances neutres (article 1, Convention V), l'interdiction pour les belligérants d'y faire passer des convois, munitions et approvisionnements (article 2, Convention V), et d'y installer 'une station radiotélégraphique ou tout appareil destiné à servir comme moyen de communication avec des forces belligérantes sur terre ou sur mer' ou même 'd'utiliser toute installation de ce genre établie par eux avant la guerre sur le territoire de la Puissance neutre dans un but exclusivement militaire et qui n'a pas été ouverte au service de la correspondance publique' (article 3, Convention V). L'installation ou l'utilisation de tels appareils–y compris les 'stations mobiles belligérantes de radiotélégraphie'– dans le port ou les eaux d'un Etat neutre est également interdite (article 5, Convention XIII). Selon les Règles de la guerre aérienne, l'Etat neutre doit prendre les mesures à sa disposition pour faire cesser l'observation aérienne dans sa juridiction (article 47).
Bien que le raisonnement analogique s'impose parmi les auteurs, les conclusions tirées sont très diverses. L'application de l'article 47 des Règles de la guerre aérienne permet de déduire que le cyber-espionnage est interdit [Gaul]. Les auteurs divergent quant à la qualification du cyber-espionnage, en vertu des conventions V et XIII, comme un acte hostile ou une violation de neutralité.

Certains répondent par la positive [Roscini], d'autres par la négative [Heintschel von Heinegg ; Woltag].

Le second courant doctrinal identifiable repose sur l'article 8 de la Convention V, les articles 7 et 10 de la Convention XIII. Selon ces dispositions, '[u]ne Puissance neutre n'est pas tenue' 'd'interdire ou de restreindre l'usage, pour les belligérants, des câbles télégraphiques ou téléphoniques, ainsi que des appareils de télégraphie sans fil, qui sont, soit sa propriété, soit celle de compagnies ou de particuliers' (article 8 Convention V), 'd'empêcher l'exportation ou le transit, pour le compte de l'un ou de l'autre des belligérants, d'armes, de munitions, et, en général, de tout ce qui peut être utile à une armée ou à une flotte' (article 7 Convention XIII), tandis que 'le simple passage dans ses eaux territoriales des navires de guerre et des prises des belligérants' ne compromet pas la neutralité (article 10 Convention XIII). Certains auteurs pensent donc que les cyber-opérations ne sont pas interdites [Bothe], alors que d'autres ne se prononcent pas définitivement sur ce point [Hostettler et Danai].

2. Etat du droit

2.1. L'espionnage entre belligérants

Tout d'abord, la thèse estime qu'une interprétation textuelle va à l'encontre d'une transposition de ce corps de règles au cyberespace

L'article 29 de la Convention II de La Haye (1899) et de la Convention IV de La Haye (1907) prévoient que '[n]e peut être considéré comme espion que l'individu qui, agissant clandestinement ou sous de faux prétextes, recueille ou cherche à recueillir des informations dans la zone d'opérations d'un belligérant, avec l'intention de les communiquer à la partie adverse. Ainsi les militaires non déguisés qui ont pénétré dans la zone d'opérations de l'armée ennemie, à l'effet de recueillir des informations, ne sont pas considérés comme espions […]'. Premièrement, les termes clés de ces articles–'faux prétextes', 'clandestinement', 'uniforme', 'information'–sont successivement définis. Deuxièmement, les autres dispositions de ces Conventions (le *contexte* mentionne par les règles d'interprétation de la Convention de Vienne) sont examinées, et cet exercice révèle des références récurrentes au territoire, et à des concepts n'ayant de sens que sur terre : 'chevaux' (article 4), 'ville, forteresse, camp' (article 5), 'villages', 'bâtiments' (article 25). Troisièmement–et si l'on revient au titre même des Conventions II de 1899 et IV de 1907–c'est bien les 'lois et coutumes de la guerre sur terre' qu'il s'agit de règlementer. Or, cette notion de 'terre' peut être définie comme un 'espace en trois dimension inamovible et indestructible, consistant d'une portion de la surface de la terre, l'espace au-dessus et en dessous de cette surface, et tout élément y poussant ou y étant apposé en permanence', 'matière solide de la terre, quel que soit les éléments qui la compose : terre, pierre, ou

autre substance' [Black's Law Dictionary]. Quatrièmement, il apparait qu'en 1899 et 1907, les Etats contractants ont souhaité faire des instruments différents et sur mesure pour la guerre sur terre (Convention II de 1899, Convention IV de 1907), sur mer (Convention III de 1899, Conventions VI, VII, VIII, IX, X, XI de 1907) et dans les airs (déclaration IV-I de 1899, Convention XIV de 1907). De cette analyse, il ressort que des conventions conçues pour s'appliquer sur terre ne peuvent en aucun cas s'étendre au cyberespace. De manière similaire, la notion d'espion de l'article 29 ne vise à s'appliquer qu'à l'espion opérant dans le cadre d'un conflit sur terre, et est intrinsèquement territoriale. Le comportement d'un cyber-espion ne saurait donc être régulé par ce biais.

L'article 26 du Protocole I aux Conventions de Genève définit trois catégories d'espions. L'alinéa 2 s'applique à '[un] membre des forces armées d'une Partie au conflit qui recueille ou cherche à recueillir, pour le compte de cette Partie, des renseignements dans un territoire contrôlé par une Partie adverse'. Celui-ci 'ne sera pas considéré comme se livrant à des activités d'espionnage si, ce faisant, il est revêtu de l'uniforme de ses forces armées'. L'alinéa 3 s'applique à '[u]n membre des forces armées d'une Partie au conflit qui est résident d'un territoire occupé par une Partie adverse, et qui recueille ou cherche à recueillir, pour le compte de la Partie dont il dépend, des renseignements d'intérêt militaire dans ce territoire'. Celui-ci 'ne sera pas considéré comme se livrant à des activités d'espionnage, à moins que, ce faisant, il n'agisse sous de fallacieux prétextes ou de façon délibérément clandestine'. De plus, 'ce résident ne perd son droit au statut de prisonnier de guerre et ne peut être traité en espion qu'au seul cas où il est capturé alors qu'il se livre à des activités d'espionnage'. L'alinéa 4 s'applique à '[u]n membre des forces armées d'une Partie au conflit qui n'est pas résident d'un territoire occupé par une Partie adverse et qui s'est livré à des activités d'espionnage dans ce territoire'. Celui-ci 'ne perd son droit au statut de prisonnier de guerre et ne peut être traité en espion qu'au seul cas où il est capturé avant d'avoir rejoint les forces armées auxquelles il appartient'. Une nouvelle fois, c'est le territoire qui est au centre de la définition ; et donc, un espace éminemment physique.

Par ailleurs, la pratique étatique subséquente confirme que le *jus in bello* ne saurait être intégralement transposé au cyberespace.
D'une part, l'applicabilité globale du droit des conflits armés dans le cyberespace n'est en effet reconnue que par certaines institutions européennes et quelques Etats (Australie, Belgique, Canada, Chili, Croatie, Etats-Unis, Japon, Royaume-Uni, Suisse). Toutefois, certains de ces Etats eux-mêmes atténuent leur position. Le Canada reconnaît que cette interprétation n'engage que lui (un avis partagé par la Finlande), tandis que l'Australie reconnait l'ambiguïté du cadre juridique (ce qui est également l'avis de l'Allemagne). Le Japon et la Suisse demandent de plus amples travaux sur le sujet (et sont rejoints sur ce point par l'Espagne). Par ailleurs, c'est l'adoption de règles d'engagement qui semble en fait être la priorité

pour certains Etats (Australie, Canada, Etats-Unis, France, Japon). *A contrario*, la Russie demande simplement le respect de normes minimales, tandis que la Chine ne reconnait pas l'application du DIH dans le cyberespace et demande l'adoption de nouvelles règles.
Un élément décisif est toutefois le fait que le cyberespace est considéré comme un « cinquième domaine » par un nombre croissant d'Etats. Cet espace, nouveau, vient s'ajouter à la terre, la mer, l'espace aérien et extra-atmosphérique (Allemagne, Australie, Canada, Chili, Guatemala, France, Inde, Israël, Lituanie, Mexique, Norvège, Royaume-Uni, République Tchèque, Slovaquie, Slovénie). Une transposition automatique d'un instrument conçu vis-à-vis d'un territoire ne peut s'appliquer.

Dans ces conditions, les activités du cyber-espion ne sauraient être automatiquement régulées par un *jus in bello* exclusivement relatif aux conflits sur terre, sur mer et sur terre.

2.2. L'espionnage impliquant un Etat neutre

Conformément à ce qui a été dit dans le premier chapitre, la thèse estime que le cyber-espionnage ne viole pas la souveraineté territoriale d'un Etat, même neutre. Ceci est confirmé par la pratique subséquente ; en effet, les Etats-Unis, les Pays Bas et la Suisse s'accordent pour dire que la neutralité d'un Etat n'est violée que quand ses réseaux subissent un dommage. Or, le cyber-espionnage ne cause aucun dommage, et ne va donc pas à l'encontre de l'article 1 de la Convention V.

L'article 2 semble s'appliquer à des éléments intrinsèquement physiques. 'Troupes' désignent des 'soldats ou les forces armées' ; 'convoi', 'un groupe de véhicules ou de navires voyageant ensemble pour des raisons de sécurité, principalement avec une escorte armée' [OED]; les 'munitions de guerre' n'incluent 'pas seulement les obus, munitions et les autres matériaux intéressant directement la conduite de la guerre, mais aussi tout ce qui peut contribuer à sa continuation, tels que les stocks militaires de toutes natures et les denrées alimentaires' [OED]; 'approvisionnement' désigne 'l'ensemble des fournitures, des produits destinés à approvisionner' [Larousse].
La Suisse estime par conséquent que l'Etat neutre ne peut alors accepter que des belligérants utilisent ses réseaux militaires. Ce choix de la Suisse est curieux, car c'est précisément l'objet de l'article 3.
La thèse estime en l'occurrence que l'article 3 est applicable au cyberspace. En effet, le terme 'tout appareil destiné à servir comme moyen de communication' est assez large pour donner lieu à une interprétation evolutive, et ainsi englober internet.

Quant à l'article 4, il instaure une forme de *due diligence* dans le cyberespace. Toutefois, seuls les Pays-Bas se sont exprimés à son sujet, l'estimant applicable. Mais leur interprétation ne va pas à l'encontre de l'espionnage, bien au contraire : ils estiment en effet que cela requiert une 'vigilance constante', un 'renseignement fiable' et un 'processus permanent d'analyse'.

L'article 8 répond bien aux exigences d'Internet, car il est impossible pour un Etat de savoir quelles informations passent par ses infrastructures. Sur le réseau, l'information est en effet divisée en paquets, circulent par des voies différentes avant d'être reconstituée en parvenant au destinataire. L'applicabilité de cet article semble validée par la pratique étatique, car les Etats-Unis, les Pays-Bas et la Suisse ont pris position en sa faveur.

La thèse conclue que le raisonnement analogique utilisé par la doctrine repose sur une présomption erronée : la similitude entre territoire et cyberespace. La thèse rejette la validité de cette analogie, puisque le territoire et le cyberespace sont deux domaines différents, et estime que les règles régissant les relations entre belligérants sont inapplicables. Seuls les articles 3, 5 et 8 de la Convention V semblent ensuite encadrer les droits de la puissance neutre dans le cyberespace, mais ces articles ne vont pas à l'encontre du cyber-espionnage.

SECONDE PARTIE – LES REGLES DECONNECTEES DE L'INTEGRITE TERRITORIALE

I – LA CONVENTION DE VIENNE SUR LES RELATIONS DIPLOMATIQUES

1. Etat de la Doctrine

1.1. L'espionnage par les ambassades

En ce qui concerne l'espionnage par les ambassades, la doctrine adopte généralement trois postures différentes.
La première consiste à invoquer les articles 3(1) (d) et 41(1) de la Convention de Vienne sur les Relations Diplomatiques, afin de soutenir que l'espionnage est illégal. Selon le premier article, '[l]es fonctions d'une mission diplomatique consistent notamment à: […] s'informer par tous les moyens licites des conditions et de l'évolution des événements dans l'Etat accréditaire et faire rapport à ce sujet au gouvernement de l'Etat accréditant […]. Selon le second, '[s]ans préjudice de leurs privilèges et immunités, toutes les personnes qui bénéficient de ces privilèges et immunités ont le devoir de respecter les lois et règlements de l'Etat accréditaire. Elles ont également le devoir de ne pas s'immiscer dans les affaires intérieures de cet Etat'. Dans la mesure où

l'espionnage est interdit par les législations nationales de nombreuses Etats, il est alors considéré par beaucoup comme une violation du droit des relations diplomatiques. Le raisonnement a été utilisé pour l'espionnage [Ward ; Lafouasse], l'interception des télécommunications et le cyber-espionnage [Duquet et Wouters ; Forcese ; Talmon ; Peters].
D'autres auteurs estiment que l'espionnage par les diplomates fait l'objet d'une pratique si répandue que tant l'espionnage traditionnel [McDougal, Lasswell and Reisman ; Grzybowski ;Murty], que le cyber-espionnage sont des activités légales [Deeks ; Sharp].
Au vu de ces tensions, de nombreux auteurs pensent que l'espionnage se situe dans une zone grise : il n'est pas expressément interdit mais l'Etat d'accueil dispose de moyens pour se débarrasser des espions, à l'instar de la déclaration *persona non grata* [Chesterman ; Murty ; Delahunty ; Nahlik ; Lafouasse ; Kish and Witiw].

1.2. L'espionnage sur les ambassades

En ce qui concerne l'espionnage sur les ambassades, on retrouve de nouveau trois courants doctrinaux. Le premier consiste à invoquer les articles 22, 24 et 27(2) de la Convention de Vienne pour soutenir l'illégalité de cette forme d'espionnage [Forcese ; Quigley]. L'article 22(1) affirme en effet que '[l]es locaux de la mission sont inviolables. Il n'est pas permis aux agents de l'Etat accréditaire d'y pénétrer, sauf avec le consentement du chef de la mission'. L'alinéa 2 mentionne aussi que '[l]'Etat accréditaire a l'obligation spéciale de prendre toutes mesures appropriées afin d'empêcher que les locaux de la mission ne soient envahis ou endommagés, la paix de la mission troublée ou sa dignité amoindrie'. Quant à l'alinéa 3, il mentionne que les 'locaux de la mission, leur ameublement et les autres objets qui s'y trouvent, ainsi que les moyens de transport de la mission, ne peuvent faire l'objet d'aucune perquisition, réquisition, saisie ou mesure d'exécution'. L'article 24 mentionne que '[l]es archives et documents de la mission sont inviolables à tout moment et en quelque lieu qu'ils se trouvent' et l'article 27(2) que '[l]a correspondance officielle de la mission est inviolable. L'expression « correspondance officielle » s'entend de toute la correspondance relative à la mission et à ses fonctions'.
A l'opposé, certains auteurs estiment que l'espionnage sur les ambassades est si répandu qu'il est toléré en droit international [Smith].
L'argument de la zone grise existe également, puisque la mission peut décider de fermer ses locaux si l'espionnage nuit à sa mission [Murty].

2. Etat du droit

2.1. L'espionnage par les ambassades

La thèse valide la théorie de la zone grise, et estime que l'Etat d'accueil dispose de moyens de protection à deux stades : durant l'accréditation et la réalisation de la mission diplomatique.

Alors que l'Etat accréditant nomme librement les membres du personnel de la mission, l'Etat accréditaire peut, '[e]n ce qui concerne les attachés militaires, navals ou de l'air', 'exiger que leurs noms lui soient soumis à l'avance aux fins d'approbation' (article 7). De plus, 'l'Etat accréditaire peut exiger que' l'effectif de la mission 'soit maintenu dans les limites de ce qu'il considère comme raisonnable et normal' et 'refuser d'admettre des fonctionnaires d'une certaine catégorie' (article 11). Les Britanniques ont notamment invoqué l'article pour lutter contre l'espionnage soviétique en 1971.

Les articles 3(1) (b) et 3(1) (d) montrent que la collecte de renseignement est inhérente à fonction diplomatique. Elle doit en effet 'protéger dans l'Etat accréditaire les intérêts de l'Etat accréditant et de ses ressortissants, dans les limites admises par le droit international' et 's'informer par tous les moyens licites des conditions et de l'évolution des événements dans l'Etat accréditaire et faire rapport à ce sujet au gouvernement de l'Etat accréditant'. Les Etats d'accueil sont de plus parfaitement conscients quant à la présence d'espions dans les ambassades, comme le montrent certaines publications de la Finlande et de la Lituanie. Cependant, ceux-ci disposent bel et bien de garanties. Certaines reposent sur le droit national, comme le montre l'article 41(1) : '[s]ans préjudice de leurs privilèges et immunités, toutes les personnes qui bénéficient de ces privilèges et immunités ont le devoir de respecter les lois et règlements de l'Etat accréditaire'. Mais c'est également le cas de l'article 3(1) (d). En effet, la pratique étatique montre que ces 'moyens licites' doivent en fait être évalués vis-à-vis du droit national de l'Etat d'accueil : le Japon, les Pays-Bas et la Suisse l'ont expressément affirmé. L'article 41(1) fait également appel au droit international, en mentionnant que les diplomates 'ont également le devoir de ne pas s'immiscer dans les affaires intérieures de cet Etat'. Seuls l'Allemagne et le Brésil ont–en des termes très flous–estimé que l'utilisation d'ambassades pour mener des activités d'espionnage électronique était contraire à la Convention.
La réponse définitive vient finalement de la CIJ, dans l'affaires des *Otages*. En effet, '[l]es conventions de Vienne de 1961 et de 1963 renferment des dispositions expresses pour le cas où des membres d'une mission diplomatique, sous le couvert des privilèges et immunités diplomatiques, se livrent à des abus de fonctions tels que l'espionnage ou l'immixtion dans les affaires intérieures de l'Etat accréditaire'. Les article 41(1) et 41(3) sont expressément cités. D'ailleurs, c'est 'afin précisément de fournir un remède à de tels abus éventuels des fonctions diplomatiques que l'article 9 de la convention de 1961 sur les relations diplomatiques' a été mis en place, et permet les déclarations *persona non grata*. L'article tient donc 'compte de la difficulté qu'il peut y avoir en pratique à prouver de tels abus dans chaque cas ou même à déterminer exactement quand

l'exercice de la fonction diplomatique, expressément visée à l'article 3, paragraphe 1 d), de la convention de 1961 […] peut être considéré comme se traduisant par des actes d' « espionnage », ou d' « ingérence dans les affaires intérieures ». Pour faire face à cette difficulté, l'article 9, paragraphe 1, prévoit expressément dans sa première phrase que 1'Etat accréditaire peut « à tout moment et sans avoir à motiver sa décision » informer l'Etat accréditant qu'un membre de sa mission diplomatique est « persona non grata » ou « n'est pas acceptable » […] Ces moyens sont par nature d'une efficacité totale' (Personnel diplomatique et consulaire des Etats-Unis à Téhéran (Etats-Unis d'Amérique c. Iran) (arrêt) [84]).

2.2. L'espionnage sur les ambassades

L'état du droit se penche tout d'abord sur la protection de la mission en elle-même, à commencer par l'inviolabilité des locaux diplomatiques (article 22(1)). Les locaux pouvant se définir comme 'pièces, partie de bâtiment servant de siège aux activités d'une profession' [Larousse], le terme désigne quelque chose d'intrinsèquement physique, et cette protection s'étend donc difficilement à des données virtuelles. Il en va de même pour l'alinéa 2, 'envahir' signifiant '[p]énétrer quelque part en nombre, de manière abusive ou non autorisée ; occuper, faire irruption dans un lieu' [Larousse]. Cette impossible extension au cyber-espionnage se confirme. D'ailleurs, la Suisse confirme que l'article 22 visait à prévenir des interférences dans les affaires intérieures d'un Etat, auxquelles le cyber-espionnage n'est pas équivalent.
Ensuite, cette activité ne trouble pas la paix ou la dignité de la mission, comme le confirme la pratique étatique. Selon la Cour Fédérale australienne, ces troubles concernent le fait de diffuser de façon prolongée–et à haut volume–des discours ou de musique, de scander des slogans, de brûler des drapeaux, de simuler des exécutions sur effigies de dirigeants, le passage répété de personnes hors des locaux diplomatiques, de façon à en prévenir l'accès, les comportements injurieux, le dépôt de substances nauséabondes [FCA 566, 1992]. Le comité des affaires étrangères au Parlement britannique adopte une approche similaire, tolérant certaines formes de manifestation mais considérant que le travail de la mission ne doit pas être perturbé, le personnel, intimidé, tandis que le libre accès du personnel et des visiteurs doit être maintenu.
L'alinéa 3, quant à lui, ne permet non plus de prévenir le cyber-espionnage. 'Ameublement' se définit comme l'"ensemble des meubles et objets qui garnissent ou ornent un logement, une pièce' [Larousse]. Si le terme 'objet' - '[c]hose solide considérée comme un tout, fabriquée par l'homme et destinée à un certain usage' [Larousse]–interdit probablement à des agents ayant pénétré dans les locaux sans autorisation de fouiller un ordinateur, il ne peut en aucun cas s'appliquer à des actes de cyber-espionnage menés à distance.

C'est ensuite l'inviolabilité des correspondances, documents et archives qui est analysée. La Convention de Vienne ayant été faite pour une période continue– et les termes 'archives' et 'documents' étant génériques–il est possible de recourir à une interprétation évolutive. 'Archives' peut se définir comme '[p]ièce, document d'archives' ou '[e]nsemble de fichiers qui ont été sauvegardés sur un support de stockage, sous forme compressée ou non' [Larousse]. Document se définit comme '[u]nité d'information correspondant à un contenu singulier'. Ces définitions peuvent clairement s'étendre à des données électroniques, et prévenir le cyber-espionnage.
La thèse estime que le terme 'correspondance' est plus problématique. En français, le terme se définit comme une 'communication par échange de lettres, de messages', alors que les définitions anglaises se concentrent sur le terme de '*letter*' ('lettre'). Or, ce terme fait généralement référence à un document écrit, et pas à une communication électronique ou vocale. Bien qu'aux Etats-Unis, la loi FISA permettent la surveillance des communications entre des 'puissances étrangères' ('*foreign powers*') et leurs agents, lorsqu'ils des intérêts américains sont en jeu, la pratique des Etats infirme en fait une interprétation en faveur de l'espionnage. Tout d'abord, l'adoption du FISA a fait l'objet d'âpres discussions, certains parlementaires dénonçant expressément une contradiction avec la Convention de Vienne. Ensuite, la Suisse mentionne explicitement que l'inviolabilité 'de la personne, des biens, archives, documents et correspondance ou encore de la valise diplomatique' doit prévenir 'l'Etat hôte' de 's'arroger le droit de surveiller les informations à disposition des bénéficiaires institutionnels et des personnes appelées en qualité officielle auprès d'eux'. Ensuite, les activités d'espionnage diplomatique de la NSA ont soulevé d'unanimes réactions : le Parlement européen, le Brésil, le Costa-Rica et les autres Etats membres du CELAC, ainsi que la résolution de l'AG des Nations Unies 69/121 ont tous dénoncé la contrariété de l'espionnage avec l'inviolabilité des archives, communications et documents des missions diplomatiques et consulaires.

La thèse conclue que la Convention de Vienne a créé un système à plusieurs vitesses. Les articles 24 et 27(2) assure l'inviolabilité les archives et documents électroniques, ainsi que les formes de correspondance électroniques et vocales. Leur surveillance est donc illégale. Pour le reste, la Convention de Vienne se contente de déléguer aux Etats le soin de s'occuper des espions, sans l'interdire par elle-même.

II – L'ACCORD SUR LES ASPECTS DES DROITS DE PROPRIETE INTELLECTUELLE QUI TOUCHENT AU COMMERCE

Trois articles de l'ADPIC sont d'intérêt en matière de cyber-espionnage, tant pour l'étude de la doctrine que du droit.
Selon l'article 3(1)–intitulé *traitement national*–'[c]haque Membre accordera aux ressortissants des autres Membres un traitement non moins favorable que celui

qu'il accorde à ses propres ressortissants en ce qui concerne la protection de la propriété intellectuelle, sous réserve des exceptions déjà prévues dans, respectivement, la Convention de Paris (1967), la Convention de Berne (1971), la Convention de Rome ou le Traité sur la propriété intellectuelle en matière de circuits intégrés […]'.

L'article 39(1) mentionne ensuite que, '[e]n assurant une protection effective contre la concurrence déloyale conformément à l'article 10bis de la Convention de Paris (1967), les Membres protégeront les renseignements non divulgués conformément au paragraphe 2 et les données communiquées aux pouvoirs publics ou à leurs organismes conformément au paragraphe 3'. L'article 39(2) mentionne ensuite que '[l]es personnes physiques et morales auront la possibilité d'empêcher que des renseignements licitement sous leur contrôle ne soient divulgués à des tiers ou acquis ou utilisés par eux sans leur consentement et d'une manière contraire aux usages commerciaux honnêtes [note 10], sous réserve que ces renseignements: a) soient secrets en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, ils ne sont pas généralement connus de personnes appartenant aux milieux qui s'occupent normalement du genre de renseignements en question ou ne leur sont pas aisément accessibles; b) aient une valeur commerciale parce qu'ils sont secrets; et c) aient fait l'objet, de la part de la personne qui en a licitement le contrôle, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrets'. Cette note 10 précise ensuite que, '[a]ux fins de cette disposition, l'expression "d'une manière contraire aux usages commerciaux honnêtes" s'entendra au moins des pratiques telles que la rupture de contrat, l'abus de confiance et l'incitation au délit, et comprend l'acquisition de renseignements non divulgués par des tiers qui savaient que ladite acquisition impliquait de telles pratiques ou qui ont fait preuve d'une grave négligence en l'ignorant'.

Enfin, son article 73 traite des *Exceptions concernant la sécurité*. 'Aucune disposition du présent accord ne sera interprétée: a) comme imposant à un Membre l'obligation de fournir des renseignements dont la divulgation serait, à son avis, contraire aux intérêts essentiels de sa sécurité; b) ou comme empêchant un Membre de prendre toutes mesures qu'il estimera nécessaires à la protection des intérêts essentiels de sa sécurité: i) se rapportant aux matières fissiles ou aux matières qui servent à leur fabrication; ii) se rapportant au trafic d'armes, de munitions et de matériel de guerre et à tout commerce d'autres articles et matériel destinés directement ou indirectement à assurer l'approvisionnement des forces armées; iii) appliquées en temps de guerre ou en cas de grave tension internationale; c) ou comme empêchant un Membre de prendre des mesures en application de ses engagements au titre de la Charte des Nations Unies, en vue du maintien de la paix et de la sécurité internationales'.

1. Etat de la doctrine

La doctrine compte deux courants doctrinaux principaux, et le premier applique directement les articles susmentionnés au cyber-espionnage. En ce qui concerne l'article 3, Fidler considèrent que les obligations imposées au gouvernement n'ont de pertinence que sur leur propre territoire, et ne prohibe en aucun cas le cyber-espionnage à l'étranger [Fidler]. A l'opposé, d'autres auteurs considèrent que donner aux entreprises de son pays des secrets volés à l'étranger leur accordent bien un traitement favorable [Malawer ; Lotrionte ; Parajon-Skinner]. Pour l'article 39, Blood considère que deux éléments préviennent l'application de l'article au cyber-espionnage. L'alinéa 1, d'abord : sa construction laisse entendre qu'il n'accorde pas plus de protection que la Convention de Paris. L'alinéa 2 et sa note 10, ensuite : l'obtention illégale de renseignements commerciaux n'y est pas mentionnée dans la définition des pratiques 'contraires aux usages commerciaux uniques' [Blood]. Ce dernier point est partagé par Danielson [Danielson]. Strawbridge insiste quant à lui sur le terme 'possibilité', présent dans l'alinéa 2 ('Les personnes physiques et morales auront la possibilité d'empêcher que des renseignements licitement sous leur contrôle ne soient divulgués à des tiers ou acquis ou utilisés par eux sans leur consentement et d'une manière contraire aux usages commerciaux honnêtes'). Selon lui, la disposition permet simplement à ces personnes d'entreprendre des poursuites judiciaires [Strawbridge]. Brenner estime que les limites aux *exceptions de sécurité* de l'article 73 compliquent une prévention du cyber-espionnage [Brenner]. *A contrario*, certains auteurs estiment compliqué pour un Etat de prétendre qu'espionner relève de ses intérêts essentiels de sécurité [Malawer], ou proposent de s'en servir pour combattre le cyber-espionnage [Lewis].

Ensuite, la doctrine tend à appliquer des modes non-officiels d'interprétation.
Dans la mesure où l'ADPIC incorpore la Convention de Paris–qui impose le traitement national (article 2) et la protection contre la concurrence déloyale (article 10bis)–avant de protéger les renseignements non-divulgués (article 39), les dessins et modèles industriels (articles 25-26), les droits d'auteurs et connexes (articles 9-10), et les brevets (articles 27-34), Parajon-Skinner estime qu' « ensemble », ces articles ont deux effets. Le premier, c'est de protéger les innovations développées par des acteurs non-étatiques ; le second, c'est de s'abstenir de pratiquer des activités entravant les droits de propriété intellectuelle [Parajon-Skinner].
Par ailleurs, certains auteurs considèrent qu'il ressort tant du *Mémorandum d'Accord sur les Règles et Procédures Régissant le Règlement des Différends* de l'OMC (article 3.2) et de la jurisprudence de l'OMC (affaire dite *Essence* et *Hormones*) que les règles de l'ADPIC doivent être interprétés en fonction des règles de droit international coutumier. Ils estiment donc que–dans la mesure où la souveraineté et la non-intervention relèvent du droit international coutumier–le cyber-espionnage constitue une violation de l'ADPIC [Parajon-Skinner ; Lotrionte].

Enfin, certains auteurs estiment que le cyber-espionnage serait contraire à l'esprit et à la lettre de l'ADPIC [Parajon-Skinner ; Lotrionte ; Brenner].

2. Etat du droit

Après ce panorama de la doctrine existante, c'est au tour de l'état du droit d'être étudié, à commencer par l'article 3. Bien que le préambule de l'ADPIC reconnaisse qu'il faille tenir 'compte de la nécessité de promouvoir une protection efficace et suffisante des droits de propriété intellectuelle', une interprétation textuelle de 'chaque Membre accordera aux ressortissants des autres Membres un traitement non moins favorable que celui qu'il accorde à ses propres ressortissants' ne révèle pas vraiment une application extraterritoriale. De plus, la définition du principe donnée par l'OMC elle-prévient une extension de l'article aux secrets industriels. Ainsi, '[l]es produits importés et les produits de fabrication locale doivent être traités de manière égale, du moins une fois que le produit importé a été admis sur le marché. Il doit en aller de même pour les services, les marques de commerce, les droits d'auteur et les brevets étrangers et nationaux […] Le traitement national s'applique uniquement une fois qu'un produit, service ou élément de propriété intellectuelle a été admis sur le marché' [www.wto.org/french/thewto_f/whatis_f/tif_f/fact2_f.htm]. La jurisprudence de l'OMC confirme le fait que l'article n'a pas vocation à s'appliquer de manière extraterritoriale, puisque toutes les demandes faites sur la base de l'article 3 concernent des restrictions ayant supposément lieu sur le territoire de l'Etat défendeur. Par conséquent, l'article 3 n'a pas vocation à prévenir le cyber-espionnage extraterritorial.

Quant à l'article 39, l'expression 'd'une manière contraire aux usages commerciaux honnêtes' ne fait pas appel à une définition externe. Comme le notait Blood, la note 10 inclue déjà des standards minimums, incluant 'au moins des pratiques telles que la rupture de contrat, l'abus de confiance et l'incitation au délit', et comprenant 'l'acquisition de renseignements non divulgués par des tiers qui savaient que ladite acquisition impliquait de telles pratiques ou qui ont fait preuve d'une grave négligence en l'ignorant'.
L'étape suivante consiste donc à déterminer si cette notion de 'tiers' peut inclure un Etat. Le contexte est décisif ici, et permet de répondre par la négative ; en effet–et tout au long de l'accord–les Etats sont désignés sous le nom de 'Membres' ou de 'gouvernements', tandis que le mot 'tiers' concerne à l'évidence des acteurs non-étatiques. L'article 31 en est un exemple : '[d]ans les cas où la législation d'un Membre permet d'autres utilisations de l'objet d'un brevet sans l'autorisation du détenteur du droit, y compris l'utilisation par les pouvoirs publics ou des tiers autorisés par ceux-ci […]'. La seule obligation qu'a l'Etat dans le cadre de l'article 39 est au paragraphe 1 : protéger 'les renseignements non divulgués conformément au paragraphe 2 et les données communiquées aux pouvoirs publics ou à leurs organismes conformément au paragraphe 3'. En fait,

les Etats n'ont qu'une obligation positive : donner à des personnes privées le moyen de protéger les renseignements non-divulgués des 'tiers' (paragraphe 2), et protéger les renseignements en leur possession (paragraphe 3). Il n'en résulte en aucun cas une obligation négative, qui obligerait les Etats à ne pas espionner. De plus, l'objet et le but de l'ADPIC est que les Etats adoptent des mécanismes de protection sur le plan national, ce qui résulte du préambule et de l'article 1.
Ensuite, la pratique subséquente va dans le sens de cette interprétation. Des membres du Congrès ont bien demandé au Représentant américain au Commerce de saisir l'OMC au sujet des activités de cyber-espionnage menées par la Chine, mais ces requêtes sont demeurées lettre morte. Il n'existe d'ailleurs pas de jurisprudence de l'OMC ayant pour base l'article 39. Il y a enfin une tendance récente à conclure des accords ou produire des déclarations non-contraignantes traitant du cyber-espionnage économique (Etats-Unis/Chine, Etats-Unis/Danemark/Finlande/Islande/Norvège/Suède, G20, G7), ce qui confirme le manque actuel de régulation.

L'article 73 et ses exceptions de sécurité est le dernier article de l'ADPIC à être analysé. Globalement, les auteurs doutent du possible rattachement du cyber-espionnage à un 'intérêt essentiel' de 'sécurité'. Toutefois, cette approche ignore totalement une différence de culture économique entre Pékin et Washington. En effet, la distinction entre acteurs publics et privés et soit floue, soit inexistante dans l'Empire du Milieu.

La thèse conclue donc que l'ADPIC n'interdit pas le cyber-espionnage.

PARTIE III – L'EXISTENCE DE REGLES COUTUMIERES SPECIFIQUES AU CYBER-ESPIONNAGE

1. Etat de la doctrine

Comme évoqué dans l'introduction, on considère généralement qu'une règle de droit international coutumier a deux composantes : la pratique et l'*opinio juris*.
Les positions de certains auteurs reflètent ces deux éléments. Ceux-ci peuvent alors mentionner la tolérance du droit international coutumier vis-à-vis de l'espionnage traditionnel, en mentionnant la pratique massive de l'espionnage [Lotrionte ; Smith], l'échange d'espions [Kish], une prise en charge exclusive par les juridictions domestiques [Lafouasse ; Cohen-Jonathan et Kovar], le refus de réguler cette activité de manière conventionnelle [Adams]. Cet argumentaire s'étend maintenant au cyber-espionnage [Beard ; Joyner]. A l'opposé, ce double test peut être utilisé pour soutenir la prohibition du cyber-espionnage, dans la mesure où l'espionnage et secret et que les Etats protestent lorsqu'ils en ont fait l'objet [Buchan]. Un grand nombre d'auteurs considère par ailleurs qu'aucune règle coutumière ne gouverne ni l'espionnage, ni le cyber-espionnage, en faisant

une activité exclusivement politique [Khalil ; Radsan ; Edmondson; Yoo; Navarette; Chesterman].
D'autres auteurs insistent davantage sur la pratique, généralement afin de démontrer la légalité de l'espionnage, puisque 'tout le monde le fait' [Lotrionte ; Deeks ; Williams ; Scott ; Sharp].
A l'inverse, certains auteurs insistent davantage sur l'*opinio juris* (déni des Etats lorsqu'ils sont soupçonnés d'espionnage) et ce, afin de défendre l'illégalité de l'espionnage [Shull].

2. Etat du droit

2.1. La pratique

Comme mentionné dans l'introduction, ce sont les actes législatifs, exécutifs et judiciaires qui permettent d'établir la pratique.
L'examen des actes législatifs comprend deux types de législation étatique : les législations pénales, et les lois relatives aux activités des services secrets.

En matière de droit pénal, il se trouve que l'espionnage constitue une infraction sur tous les continents, et est universellement réprimé. Tel est le cas en Europe (Allemagne, Autriche, Belgique, Espagne, Estonie, France, Royaume-Uni, Russie, Suisse), Asie (Chine, Corée du Sud, Inde, Philippines, Turquie), Afrique (Algérie, Cameroun, Erythrée, Kenya, Nigéria, Tchad), Amérique (Argentine, Bolivie, Chili, Colombie, Equateur, Etats-Unis, Mexique, Pérou), Océanie (Australie, Nouvelle-Zélande, Papouasie Nouvelle Guinée). Certains Etats ont par ailleurs défini des infractions spécifiques aux cyber-intrusions (Afrique du Sud, Allemagne, Argentine, Bolivie, Chine, Colombie, Corée du Sud, Equateur, France, Luxembourg, Malaisie, Mexique, Nigéria, Pays-Bas, Pérou, Philippines, Royaume-Uni, Russie, Singapour, Suisse, Tchad, Thaïlande, Turquie, Venezuela).

Paradoxalement, les lois relatives aux activités des services secrets montrent qu'en parallèle, l'ensemble des Etats s'arroge le droit d'espionner sur les autres. La devise '*ne fais pas aux autres ce que tu ne voudrais pas qu'on te fasse'* n'existe donc en aucun cas dans le monde de l'espionnage !
Ainsi, les Etats prévoyant explicitement, dans leur législation, leurs activités de renseignement à l'étranger incluent la Bosnie-Herzégovine, l'Espagne, la France, la Géorgie, la Grèce, l'Italie, le Kazakhstan, le Kenya, la Papouasie-Nouvelle-Guinée. Certains font d'ailleurs directement référence au cyber-espionnage et à l'interception de télécommunications (Allemagne, Belgique, Canada, France, Nouvelle Zélande, Pays-Bas, Royaume-Uni, Suisse). Les Etats-Unis y font aussi référence, mais dans un acte exécutif.

En revanche, certains Etats font référence à leurs activités de renseignement de manière plus subtile ; ainsi, la Russie, la Slovaquie et la Suisse ont des dispositions leur permettant de porter assistance à leurs agents déployés à l'étranger.
De nombreux Etats recourent toutefois à des formules ambiguës : reconnaitre que des informations sont cherchées 'au sujet de l'étranger', 'hors du pays', 'en rapport avec des Etats étrangers', ou 'sur le plan interne et international' en est une première manifestation. Les Etats ayant recours à ce type de disposition incluent l'Allemagne, le Royaume-Uni et la Slovaquie, l'Australie, la Croatie, le Chili, le Ghana, le Kenya, le Nigeria, la Norvège, le Paraguay, le Pérou, la Slovaquie, et la Turquie. Une seconde manifestation est la présence de dispositions permettant de prévenir la déclassification d'informations si cela venait à endommager la relation avec d'autres Etats, comme en Norvège ou aux Pays-Bas.

Les motifs justifiant la collecte de renseignement incluent systématiquement la protection de la sécurité nationale. C'est de cas de l'Allemagne, de la Bosnie-Herzégovine, du Canada, du Chili, du Mexique, du Monténégro, du Nigéria, de la Norvège, de la Turquie. Toutefois, un nombre encore plus important d'Etats rajoute à cet impératif la protection du bien-être économique, scientifique ou de ses relations étrangères. C'est le cas de l'Australie, de la Belgique, de la France, de l'Espagne, de la Géorgie, du Ghana, de la Grèce, de l'Italie, du Kazakhstan, du Kenya, de la Nouvelle-Zélande, de la Papouasie-Nouvelle-Guinée, du Royaume-Uni, de la Russie, de la Slovaquie, la Suisse. Les Etats-Unis, par le biais d'un ordre exécutif, sont également dans cette situation.

Les juridictions nationales ont parfois rendu des jugements liés à l'espionnage. Mais, à l'exception de la Convention de Vienne sur les Relations Diplomatiques– lorsqu'il s'agit de l'immunité d'un agent–ou des Conventions de La Haye, c'est en toujours en vertu du droit national que des espions ont été condamnés.

2.2. L'*opinio juris*

Ce sont ensuite les déclarations publiques des Etats, les publications officielles, et les avis juridiques des gouvernements qui permettent d'établir l'*opinio juris*.

De nombreux Etats ont ouvertement reconnu, par le biais de déclarations publiques, mener des activités de renseignement à l'étranger : Australie, Canada, Cuba, Espagne, Etats-Unis, France. Parmi les justifications invoquées, on retrouve le fait que 'tout le monde le fait' ou que cela est nécessaire pour se protéger. Par ailleurs, le TPIY avait demandé au Canada et aux Etats-Unis de fournir les 'enregistrements, synthèses, notes et textes de toute communication interceptée (électronique, vocale et écrite)' ainsi que les sources travaillant pour eux. Que ces informations 'existent ou non', ces deux Etats avaient refusé de s'exécuter ; ils estimaient que des impératifs de sécurité nationale étaient en jeu.

Un avis juridique du gouvernement suisse estime par ailleurs que l'espionnage est toléré par le droit international coutumier.

L'absence de prohibition directe de l'espionnage dans le droit conventionnel–à l'exception de la Convention de Vienne sur les Relations Diplomatiques–a été régulièrement soulignée tout au long de la thèse. Des propositions en vue de limiter l'espionnage de manière conventionnelle ont été faites–et refusées–à trois reprises. Proposition du Viêt-Nam à la Chine en faveur d'un traité prohibant les activités d'espionnage et de reconnaissance (1970), de l'Indonésie à l'Australie en faveur d'un Code d'Ethique (2013), de l'Allemagne aux Etats-Unis concernant un 'accord de non espionnage' (2014).

Comme le montre la CDI, 'la pratique pertinente doit être générale, c'est-à-dire suffisamment répandue et représentative, ainsi que constante'. Et en effet, la prohibition de l'espionnage dans les codes pénaux nationaux satisfait bien cette exigence. Toutefois, l'auto-autorisation d'espionner dans les législations relatives aux activités de renseignement est aussi répandue, représentative et constante. De plus, 'la pratique en question doit être menée avec le sentiment de l'existence d'une obligation juridique ou d'un droit'. Si de nombreux Etats estiment qu'ils ont le droit d'espionner, les exemples de protestation contre une telle activité sont au moins aussi nombreux. Mise dans situation similaire, la CIJ avait autrefois estimé que '[l]es faits soumis à la Cour révèlent tant d'incertitude et de contradictions, tant de fluctuations et de discordances […] il y a eu un tel manque de consistance dans la succession rapide des textes conventionnels […] ratifiés par certains États et rejetés par d'autres, et la pratique a été influencée à tel point par des considérations d'opportunité politique dans les divers cas, qu'il n'est pas possible de dégager de tout cela une coutume constante et uniforme acceptée comme étant le droit' [*Affaire du droit d'asile* (Colombie/Pérou) (arrêt) 277]. C'est la conclusion à laquelle parvient la thèse concernant le cyber-espionnage.

CONCLUSION GENERALE

1. Synthèse

Durant des décennies, les Etats se sont satisfait du contrôle indirect–et ambiguë–qu'offrait la présence physique de l'espion sur son territoire. S'il avait la qualité de diplomate, il pouvait être expulsé. Dans le cas contraire–et si son Etat d'allégeance reconnait son envoi–alors l'Etat victime pouvait dénoncer une violation de souveraineté et procéder à des échanges d'espions. En l'absence d'une telle reconnaissance–ou en temps de guerre–l'espion pouvait être jugé, conformément à la législation nationale. Cet équilibre est rompu par la dématérialisation et la déterritorialisation de l'espionnage, et l'inapplicabilité de certaines règles réside directement dans cet élément.

Tel est le cas pour la violation de souveraineté. L'illégalité de l'espionnage traditionnel réside en effet exclusivement dans l'intrusion non-consensuelle d'un agent étranger sur le territoire d'un autre Etat. En effet, l'activité d'espionnage elle-même ne va pas à l'encontre du principe de souveraineté territoriale. Cette conclusion est *a fortiori* confirmée par la pratique étatique.
Tel est aussi le cas pour l'article 22(1) de la Convention de Vienne sur les Relations Diplomatiques. S'introduire dans une ambassade pour y installer des dispositifs d'espionnage est évidemment contraire à l'article. En revanche, il n'en va pas de même pour le cyber-espionnage, ou même les interceptions de télécommunications. La seule intrusion physique dans les locaux diplomatiques est en effet prohibée par la disposition. Quant à l'article 22(3), il ne peut s'appliquer au cyber-espionnage ou aux interceptions de télécommunications pour les mêmes raisons. 'Locaux', 'ameublement', 'objets' désignent des concepts éminemment physiques.
Alors que les Conventions de La Haye II (1899), IV (1907) et le Protocole Additionnel I autorisent l'espionnage entre belligérants, ils ne peuvent être transposés au cyber-espionnage. Ces règles ont en effet été conçues vis-à-vis d'environnements spécifiques : la terre, la mer, l'air. Dans la mesure où le cyberespace est un domaine différent–ce qui est confirmé par les Etats–ces règles ne peuvent pas être intégralement et automatiquement transposées.

En revanche, la migration de l'espionnage sur Internet n'a rien changé par rapport à certaines règles. Le *jus ad bellum* était muet quant à l'espionnage, et le demeure pour le cyber-espionnage. Ni l'un ni l'autre n'implique une arme et, en réduisant les incertitudes quant aux intentions des autres Etats, servent en fin de compte l'objet de la Charte des Nations Unies. La validité des méta-principes d'interprétation est, de plus, controversée.
Cette transition est également sans effet sur le principe de non-intervention, puisque l'espionnage per se n'est pas coercitif. De plus–et bien qu'ils puissent être dirigés contre les systèmes politiques, économiques, sociaux et culturels d'un Etat–peu de domaines demeurent sous sa juridiction exclusive.
Ni l'espionnage traditionnel, ni le cyber-espionnage ne sont régulés par l'ADPIC. L'article 3 n'a en effet pas vocation à s'appliquer extra-territorialement, tandis que l'article 39 n'interdit pas aux Etats d'espionner des entreprises basées à l'étranger. Le premier oblige simplement les Etats à garantir le respect du traitement national sur leur propre territoire. Le second protège les entreprises des activités menées par d'autres acteurs non-étatiques ('tiers'), et oblige les Etats ('Membres') à assurer la protection des renseignements non divulgués qui leur sont confiés. Les exceptions concernant la sécurité de l'article 73 ne suffisent pas non plus à décourager le cyber-espionnage.
En matière d'espionnage diplomatique, les notions d' « envahis », « endommagés », « paix de la mission troublée » ou « dignité amoindrie » définies par l'article 22(2) de la Convention de Vienne sur les Relations diplomatiques est

sans effet sur l'espionnage et le cyber-espionnage. Ils visent en effet à limiter les excès pouvant se produire lors de protestations. Quant aux activités de renseignement menées par les ambassades, la Convention de Vienne délègue aux Etats parties le pouvoir de prendre des mesures contre les espions, sans prohiber l'espionnage par elle-même.

En fin de compte, deux corps de règles sont à la fois applicables au cyberspace et pertinentes pour le cyber-espionnage.
Tout l'abord, l'article 8 de la Convention V de La Haye permet à l'Etat neutre de tolérer certaines activités de cyber-espionnage passant par ses infrastructures. Toutefois, cette convention ne s'applique qu'en temps de guerre. Ensuite, une interprétation textuelle révèle bien l'applicabilité de l'article 3 de la Convention de La Haye. Toutefois, cela n'affecte qu'indirectement le cyber-espionnage, en prévenant la construction d'infrastructures sur le territoire d'un Etat neutre en vue de communiquer avec des belligérants, ainsi que l'usage de 'toute installation de ce genre' n'ayant 'pas été ouverte au service de la correspondance publique'.
Ensuite, une interprétation textuelle et évolutive de ses articles 24 et 27(2) révèle que seule la Convention de Vienne sur les Relations Diplomatiques prohibe le cyber-espionnage. Il n'en résulte toutefois pas une prohibition générale : seul l'espionnage dirigé contre la correspondance officielle électronique et vocale, ainsi que les archives et documents numériques de la mission diplomatique est prohibé.

En droit international, le régime juridique du cyber-espionnage n'est pas uniforme, mais fragmenté. Il n'y a en effet pas de prohibition ou d'autorisation générale de l'activité. La seule restriction concerne une forme spécifique–l'espionnage sur les ambassades–et provient d'un instrument particulier–la Convention de Vienne sur les Relations Diplomatiques. En dehors de ca cadre, le cyber-espionnage se caractérise par une absence de droit. Tous les Etats s'espionnent, et souhaitent en profiter.

2. Perspectives

2.1. Etat de la doctrine : une approche managérialiste du cyber-espionnage

La nature et la doctrine ont un élément en commun : elles ont horreur du vide. En dépit d'un désintérêt centenaire des Etat pour une régulation de l'espionnage à travers des règles de droit international, la doctrine a essayé d'étendre le cadre juridique existant au cyber-espionnage. Ce phénomène de *managérialisme* avait déjà été dénoncé par certains auteurs, pour d'autres problématiques [d'Aspremont ; Koskenniemi ; Kennedy].

2.2. Etat du droit : vers un triomphe du droit national ?

A la lumière de la recherche, trois tendances sont plausibles.

Premièrement, il est improbable qu'un traité prohibant le cyber-espionnage connaisse bientôt le jour. Il n'en va pas autrement dans le cas du cyber-espionnage économique. De plus amples déclarations et code de conduite apparaitront probablement sur les plans bilatéraux et régionaux. Les Etats mènent depuis toujours un double jeu ; même les Etats-Unis, qui dénoncent avec vigueur cette activité, pratiquent l'espionnage industriel.

Toutefois–et deuxièmement–des traités internationaux relatifs à la cybercriminalité vont se développer. Paradoxalement, donc, le droit international va promouvoir l'adoption de règles nationales prohibant les 'accès', 'interceptions', 'intrusions', ou des atteintes à la 'confidentialité' des données. En substance, des incriminations affectant le cyber-espionnage, mais qui se concentrent sur l'individu sans toucher l'Etat responsable.

Enfin, les droits de l'Homme pourraient également être pertinents. Dans la mesure où le cyber-espionnage implique une violation de données, le droit au respect de la vie privée pourrait être impliqué dans certains cas de cyber-espionnage. Toutefois, certaines incertitudes demeurent quant à l'application extraterritoriale de ces instruments et le degré de contrôle requis. Confronté à 'certaines administrations publiques' qui feraient 'systématiquement effectuer les tâches de collecte et d'analyse des données dans le cadre de juridictions offrant des garanties plus faibles en matière de protection de la vie privée', administrant 'un réseau transnational de services du renseignement en jonglant avec divers vides juridiques et en coordonnant la pratique de la surveillance pour contourner les protections offertes par les régimes juridiques nationaux', le Comité des Droits de l'Homme réagit. Il estime que 'cette pratique ne remplit pas les conditions voulues pour être légale', car 'la prévisibilité du fonctionnement du régime de surveillance aux personnes qui y sont soumises' n'est pas assurée'. Les articles 17 et 4 du Pacte sont mentionnés. Par ailleurs, '[l]es États n'ont pas pris non plus de mesures effectives pour protéger les individus relevant de leur compétence contre les pratiques de surveillance illégale suivies par d'autres États ou entreprises, en violation de leurs propres obligations en matière de droits de l'homme' [para 30]. Il estime 'qu'un État ne peut pas se soustraire à ses obligations internationales en matière de droits de l'homme en prenant en dehors de son territoire des mesures qui lui seraient interdites « chez lui »' [para 33]. Ensuite, '[l]es 'notions de « pouvoir » et de « contrôle effectif » permettent de reconnaître qu'un État exerce une « compétence » ou des pouvoirs publics, dont les mesures de protection des droits de l'homme sont destinées à freiner les abus' [para 33]. 'Il s'ensuit que la surveillance numérique peut donc mettre en cause les obligations d'un État en matière de droits de l'homme si elle fait intervenir l'exercice du pouvoir ou le contrôle effectif dudit État à l'échelle de l'infrastructure des communications numériques, où que cela se produise, par exemple sous la forme d'écoutes directes ou d'une pénétration de l'infrastructure

en place' [para 34]. Si ces droits bénéficient clairement aux individus, si et comment ils peuvent s'étendre à des personnes morales–Etats et entreprises– reste à déterminer.

RESUME

Les Etats s'espionnent depuis des siècles, soulevant des tensions. Toutefois, une régulation expresse ne peut être trouvée que dans le droit des conflits armés. Alors que les espions peuvent être capturés et punis, il est paradoxalement admis que leur envoi en temps de guerre n'est pas contraire au droit international. En revanche, aucune règle expresse ne vient réglementer l'espionnage en temps de paix. Une appréhension indirecte n'existe que par le biais de la souveraineté territoriale. En effet, en l'absence de son consentement, l'envoi d'un agent sur le sol d'un territoire étranger est illégal. Cela fait écho à la position ambivalente des Etats sur la scène internationale, qui ont toujours envoyé des espions en territoire étranger. Quand ces agents sont capturés, l'Etat peut les punir conformément à sa législation pénale, protester ou les échanger. Toutefois, l'applicabilité de ce cadre juridique est remise en question par l'émergence du cyber-espionnage, dans la mesure où la présence physique d'un agent n'est plus requise. Le fil d'Ariane de cette thèse est donc de savoir si la dématérialisation et la déterritorialisation de l'espionnage prévient l'application des règles de droit international au cyber-espionnage.

La doctrine a tenté de faire face à ce manque de régulation expresse et ces changements. Les auteurs ont habituellement proposé d'appliquer les traités existants, d'examiner la légalité du cyber-espionnage à la lumière des règles de souveraineté et de non-intervention, ou essaient d'identifier de nouvelles règles coutumières. Toutefois, cette thèse perçoit de nombreux problèmes dans cette démarche. En effet, seules de rares références sont faites aux règles d'interprétation contenues dans la Convention de Vienne sur le Droit des Traités, les conclusions de la Commission de Droit International (CDI) sur l'identification du droit international coutumier, ainsi qu'à la pratique étatique. De plus, de nombreuses analogies reposent sur la supposition erronée que le territoire et le cyberespace sont similaires.

Huit instruments sont analysés dans cette thèse. Afin de déterminer ce qu'ils ont à dire au sujet du cyber-espionnage, cette recherche propose de recourir aux règles officielles d'interprétation contenue dans la Convention de Vienne, les conclusions de la CDI, et d'incorporer le montant maximum de pratique étatique. Cette thèse conclut finalement que le cyber-espionnage ne viole pas les règles de souveraineté, de non-intervention, la Charte des Nations Unies, l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce. Elle révèle également que la plupart des règles applicables en temps de guerre sont inapplicables, et que ni l'espionnage ni le cyber-espionnage ne sont interdits par le droit international coutumier. Seule la surveillance des archives et documents digitaux, ainsi que la correspondance électronique et vocale violent la Convention de Vienne sur les Relations Diplomatiques.