UNIVERSITY OF TARTU

School of Law

Department of Public Law

Mari-Liis Vähi

RESPONSIBILITY FOR CYBERTERRORISM UNDER INTERNATIONAL LAW

MA thesis

Supervisor: prof. dr. iur. Lauri Mälksoo

Tartu, Estonia

2021

TABLE OF CONTENTS

INTRODUCTION 3
1. CHAPTER 1 - DEFINING CYBERTERRORISM 6
1.1. Terrorism 6
1. 1.1. Terrorism - the roots of the conundrum 6
1.1.2. Mainstream definitions 7
1.1.3. Characteristics of terrorism 8
1.2. Cyberterrorism 11
1.3. Legal definitions 16
2. CHAPTER 2: LEGAL FRAMEWORK ON CYBERTERRORISM 22
2.1. International law on terrorism 22
2.1.1. General instruments 22
2.1.2. Sectoral instruments 25
2.1.3. Regional instruments 26
2.2. International law on cyberterrorism 27
2.3. *Ius ad bellum* 31
2.4. *Ius in bello* 35
2.5. Customary International Law 38
2.6. State Responsibility 39
2.7. International Human Rights Law 41
2.8. International Criminal Law 43
2.8.1. Crimes applicable to terrorism 43
2.8.2. Individual responsibility 46
2.9. Responsibility of private entities 46
3. CHAPTER 3: WAYS FORWARD 50
CONCLUSION 56
RESÜMEE 58
LITERATURE 62

INTRODUCTION

Cyberspace is a global domain (also regarded as a 5th military domain[1]), involving private and public, civilian and military sectors. It is also a domain where ideologies and national, economic and geopolitical interests and positions clash. As digitalization has transformed every aspect of our society, improved our businesses and everyday lives, information and communication technologies (abbr. ICTs) have also caused an emergence of new security vulnerabilities. At interconnected and -dependent times of such increasingly wide range that the technology has provided to the world, the peace and security of the world is threatened by the malicious actions of states and non-state actors, including violent extremist groups or terrorists. Unscrupulous state and non-state actors have found new channels to spread misinformation and propaganda, to assemble and collect resources and conduct cyberattacks and -operations.

As cyberspace has created new challenges in interstate relations, so have various non-state actors, such as terrorists, with new means imposed new threats to health and safety of peoples, functioning of businesses and states, to political stability, and ultimately, to our democracies in general. With such a global domain that we all are so dependent on, the consequences of possible terror attacks are more significant than ever.

Both terrorism and cyber security threats are, besides the proliferation of weapons of mass destruction, state failure and organised crime, main threats and challenges to national security.[2] In 2010, the United Kingdom referred to international terrorism and "*cyber attack, including by other States, and by organised crime and terrorist*" as two of four "*Tier One*" threats to British national security.[3] In 2016, the Obama administration released the Cybersecurity National Action Plan that addressed the challenge of malicious actors, including terrorists, operating in cyberspace. It was also acknowledged that "*attacking us online is often easier than attacking us in person*".[4] According to the World Economic Forum's Global Risks Report 2020, cyberattacks constitute a major global risk considering both their likelihood and impact.[5]

---

[1] European Defence Agency. Cyber Defence. Available at: https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence

[2] G. Lindstrom, E. Luiijf. National Cyber Security: Framework Manual. Political Aims and Policy Methods. Gen. ed. A Klimburg. NATO CCD COE. Tallinn. 2012, pp. 47-48.

[3] HM Government. A strong Britain in an Age of Uncertainty: The National Security Strategy. 2010, p. 27. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[4] The White House. President Barack Obama. Office of the Press Secretary. Fact Sheet: Cybersecurity National Action Plan. 2016. Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

[5] The World Economic Forum. The Global Risks Report. 2020. Available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

According to the 2021 report, the threats posed by technologies remain high and misinformation, cyberattacks, targeted strikes and resource grabs are only on the rise.[6] Notably, terrorist attacks are one of the most imminent global risks.[7] In December 2020, the European Commission released a new EU Cybersecurity Strategy in which Ylva Johansson, the European Commissioner for Home Affairs, addressed the need to secure key infrastructure against (*inter alia*) terrorist attacks. She stated: "*To ensure the smooth functioning of the internal market and the livelihoods of those living in Europe, our key infrastructure must be resilient against risks such as natural disasters, terrorist attacks, accidents and pandemics like the one we are experiencing today".*[8]

The EU's Counter-Terrorism Agenda 2020 also addressed the need to tackle the rising threat of terrorism in the EU. The Agenda marked that the nature of terrorist attacks is shifting and the EU needs to prepare for threats both rising from new technologies, *e.g.* malicious use of drones, artificial intelligence, chemical, biological, radiological and nuclear material, as well as the use of online propaganda. The latter often becomes the integral part of the attack itself.[9] With their own intrinsic features, both terrorism and digital technologies pose significant challenges to international peace and security.

While the new technologies have generated new opportunities for terrorists to operate, they have also created new ways for law enforcement to tackle the threat of terrorism.[10] The question is whether our legal system manages to keep up the run of rapid technological development and hold the individuals and institutions responsible for the acts of terrorism.

One of the crucial concerns when it comes to terrorist use of cyberspace is accountability. That also raises the concern as to whether the international law provides sufficient measures to hold cyberterrorist responsible for the acts of cyberterrorism.

---

[6] The World Economic Forum. The Global Risks Report. 16th Edition. 2021, p. 53. Available at: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

[7] *Ibid.* p. 7.

[8] European Commission. New EU Cybersecurity Strategy. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. 2020. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[9] European Commission. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. Brussels, 9.12.2020. COM(2020) 795 final. 2020, p. 1. Available at: https://ec.europa.eu/home-affairs/sites/default/files/pdf/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf

[10] See United Nations Office on Drugs and Crime (UNODC). Frequently Asked Questions on International Law Aspects of Countering Terrorism. Vienna: UNODC. 2009, pp. 11-13. Available at: https://www.unodc.org/documents/terrorism/Publications/FAQ/English.pdf

This thesis focuses on the role of international law in ensuring responsibility for the acts of cyberterrorism. It does so by first exploring the nature and the definition of cyberterrorism under international law. Secondly, the current international legal framework on cyberterrorism and legal means of ensuring responsibility will be examined. Thirdly, in case there are gaps in legal framework, this paper intends to find possible remedies to ensure responsibility (and thus increase the accountability) for such acts.

For that end, this paper utilizes qualitative dogmatic legal analysis and deductive analytical methods. The author analyses international legal framework in regards to cyberterrorism. For this analysis, primarily grammatic and comparative interpretation methods will be used. Based on this analysis, the author also uses a deductive method to propose possible ways forward to strengthen responsibility for the acts of cyberterrorism. For the analysis real life cases of terrorism, cyberattacks and cyberterrorism will be used to exemplify the dogmatic analysis. Main sources used for this thesis are international legal instruments (conventions, treaties), scholarly writings (articles, books, commentaries) and court rulings.

Keywords

Cyberterrorism; Cyber Security; International Crimes; Cyber Crimes; Cyber Warfare, Cyber War; Cyber Act of war; Use of force; Armed attack; Act of Terror; Act of Aggression; Act of Violence; Information Security; Accountability; Responsibility; Cyber; Cyber Attack; International Humanitarian Law; International Human Rights Law; International Criminal Law; International Law

1. CHAPTER 1 - DEFINING CYBERTERRORISM

1.1. Terrorism

1. 1.1. Terrorism - the roots of the conundrum

Cyberterrorism consists of two widely contested terms "cyber" and "terrorism". This subchapter explores the definition of terrorism, including its roots and the nuances related to it. Based on the findings of this subchapter, the next subchapter will analyse what terrorism means in cyberspace.

Walter Laqueur, an influential scholar on terrorism, counted more than 100 definitions of terrorism. The only common characteristic he found was that they all include violence or the threat of violence.[11]

The term has lived a double life through societies of the world, on the one hand it has been considered a political strategy, on the other hand, a monstrosity of a mankind. For example, in 1793, the Jacobin leader during the French Revolution, Maximilien F.M.I de Robespierre, when describing the actions of the Jacobin Club, said that "*Terror is nothing but justice, prompt, severe and inflexible.*"[12] During their two years in power they executed 17,000 opponents, the period which is known as *La Terreur* or Reign of Terror. The word "terror" was also proudly used by the Russian revolutionaries who assassinated Czar Alexander II in 1881.[13] German revolutionary Karl Heinzen, in his 1853 political pamphlet "*Mord und Freiheit*" ("Murder and Liberty"), also saw terrorism as a progressive tool of violence to bring political change and boost progress in society and coined the term terrorism with *Freiheitskämpfer* (or freedom fighter).[14] Over time, the term "terrorism" grew its universal stigma and was used rather as a condemnation. It was then increasingly associated with movements of national liberation and some so-called "terrorists" preferred the terms of freedom fighters, guerrillas or mujahedeen.[15]

One of the last groups to call themselves terrorists was a Zionist organization called Lehi (aka Stern Gang). The terrorists of Stern Gang killed 91 people in Jerusalem in 1946. As the stigma

---

[11] W. Laqueur. The new terrorism: fanaticism and the arms of mass destruction. New York, Oxford University Press. 1999, p. 12.
[12] G. Nunberg. HEAD GAMES / It All Started with Robespierre / "Terrorism": The history of a very frightening word. SFGATE. Opinion. 2001, updated 2012. Available at: https://www.sfgate.com/opinion/article/HEAD-GAMES-It-All-Started-with-Robespierre-2865759.php
[13] *Ibid.*
[14] UNODC. Counter-Terrorism Module 1. Key Issues: Terrorism in the 19th Century. Vienna. 2018. Available at: https://www.unodc.org/e4j/en/terrorism/module-1/key-issues/terrorism-in-19th-century.html;
D. Bessner, M. Stauch. Karl Heinzen and the Intellectual Origins of Modern Terror. Terrorism and Political Violence. Volume 22. 2010. Available at: https://www.tandfonline.com/doi/abs/10.1080/09546550903445209
[15] G. Nunberg. 2001, updated 2012.

spread, by the 1990s, "terrorism" was used in all kinds of intimidation or disruption. People who infected computers with viruses immediately became cyberterrorists in the eyes of the public and cult leaders were described as psychological terrorists.[16]

Exploring the roots of terrorism (which can go back to the 11th century[17], or, according to other sources the 19th century[18]) only confirms the double-headedness of the concept. The term has found a vast variety of interpretations by historians, scholars, politicians and the population in general. Qualifying acts of violence, *e.g.* political assassinations or violent uprisings, as unjustifiable criminal acts or, instead, justifiable movements of liberation, is often difficult as it is to draw the line between these concepts. Therefore, to this day, the world has no internationally binding definition of terrorism and the definitional issues around the concept continue.

Subsequently, terrorism has also been used as a pejorative term for acts, including both methods and ends of conduct, that fall below standards of acceptable ethical conduct.[19] People have used this term with included morality and for a long time it has been regarded as a foreign concept with a sense of otherness.[20] Thus the term has, in many cases, not been utilized as an impartial, value-neutral, tool for assessing activities and tactics of political actors.[21] Similarly, R. Värk describes terrorism as "*imperfect, emotionally charged and politically influenced*".[22]

1.1.2. Mainstream definitions

Popular dictionaries have still found a way to define this controversial concept. According to Oxford Dictionary terrorism is the unlawful use of violence and intimidation, especially against civilians in the pursuit of political aims. Cambridge Dictionary defines terrorism as "*(threats of) violent action for political purposes*".[23] Collins dictionary defines terrorism as "*the use of violence, especially murder and bombing, in order to achieve political aims or to force a government to do something*".[24] Encyclopedia Britannica defines terrorism as "*the calculated use of violence to create a general climate of fear in a population and thereby to bring about a*

[16] *Ibid.*
[17] M. Burgess. History of Terrorism. POGO. 2012. Available at: https://www.pogo.org/investigation/2015/02/brief-history-of-terrorism/
[18] B. Hoffman. Inside Terrorism. New York: Columbia University Press. 1998, p. 17.
[19] D. M. Jones, M.L.R. Smith, P. Schulte, C. Ungerer. Handbook of Terrorism and Counter Terrorism Post 9/11. USA. Edward Elgar Publishing Limited. 2019, p. 2.
[20] *Ibid.* p. 7.
[21] *Ibid.* p. 2.
[22] R. Värk. Terrorism, State Responsibility and the Use of Armed Force. ENDC Proceedings, Volume 14. 2011, p. 75.
[23] Cambridge Dictionary. Terrorism. Available at: https://dictionary.cambridge.org/dictionary/english/terrorism
[24] Collins Dictionary. Terrorism. Available at: https://www.collinsdictionary.com/dictionary/english/terrorism

particular political objective".[25] Similarly, the Macmillan Dictionary defines it as "*the use of violence to achieve political aims*".[26] Thus, according to all of these popular dictionaries, terrorism refers to violence with political motivation.

1.1.3. Characteristics of terrorism

Common themes embedded in the definitions of terrorism are the following:

1) **the use or threat of violence**

Terrorism involves tactics and strategies that use violence (or the threat of such). This violence could cause serious harm, death or serious damage to property.[27] Conventional attacks used by terrorists are, to name a few[28], assassinations, beheadings[29], bombings, arson, hostage-taking, hijacking, kidnapping, sabotage, biological weapons, the perpetration of hoaxes and suicide bombings. Unconventional terrorism could include nuclear terrorism (*e.g.* attacking a nuclear reactor)[30], cultural terrorism[31] (*e.g.* ISIL attacking ancient statues at the Mosul museum in 2015), ecological terrorism (*e.g.* the threat of destruction to the environment)[32], information warfare[33], high-tech terrorism[34] (for instance, simultaneously exploding a bomb at a train station, launching a cyberattack on the critical infrastructure, using Trojan horses, worms, viruses, denial of service attacks, and other information warfare tools).[35] Thus, the terrorist threat has a complex nature, as there is a broad spectrum of attack scenarios.[36]

2) **intention to create fear**

---

[25] J. P. Jenkins. Terrorism. Encyclopedia Britannica. Available at: https://www.britannica.com/topic/terrorism

[26] Macmillan Dictionary. Terrorism. Available at: https://www.macmillandictionary.com/dictionary/british/terrorism

[27] R. Värk. 2011, p. 81.

[28] See, for example, Global Terrorism Index 2017 by the Institute for Economics and Peace. Available at: https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%202017%20%284%29.pdf

[29] BBC News. Running for your life from terror in north-east Mozambique. 12 March 2021. Available at: https://www.bbc.com/news/av/world-africa-56373615

[30] Counter-Terrorism Module 1. Key Issues: United Nations and Terrorism. 2018.

[31] *Ibid.*

[32] *Ibid.*

[33] F. Ristoldo. Attacks against Cultural Property as a weapon of war: An exploratory case study. Institut Barcelona Estudis Internacionals. 2016-2017. Available at: https://www.ibei.org/ibei_studentpaper34_105354.pdf

[34] Counter-Terrorism Module 1. Key Issues: United Nations and Terrorism. 2018.

[35] World Academy of Science, Engineering and Technology. Status and Requirements of Counter-Cyberterrorism. Available at: https://publications.waset.org/11708/status-and-requirements-of-counter-cyberterrorism

[36] N. A. Makhutov, V. P. Petrov, and D. O. Reznikov. Countering Terrorism: Biological Agents, Transportation Networks, and Energy Systems: Summary of a U.S.-Russian Workshop. Chapter: 7 Characteristics of Technological Terrorism Scenarios and Impact Factors. 2009, p. 55.

Acts of terrorism are explicitly intended to create fear, not just among the direct victims but among a wide audience - usually with an underlying political aim.[37] The underlying goal could entail coercion of a government, an international organization or an individual.[38] In order to create fear, terrorists must engage in increasingly dramatic, violent, and high-profile attacks. These have included hijackings, hostage takings, kidnappings, mass shootings, car bombings, and, frequently, suicide bombings.

Depending on the overall goal, terrorists can be referred to as "separatist", "revolutionary", "ethnocentric", "nationalist" or "religious".[39] For example, terrorists that have revolutionary goals seek to tear down current political systems and replace it with one of their liking. Italian Red Brigades, the German Red Army Faction (Baader-Meinhof Gang), the Basque separatist group ETA, the Peruvian Shining Path (Sendero Luminoso), and ISIL (the Islamic State in Iraq and the Levant; also known as the Islamic State in Iraq and Syria (ISIS) could be regarded as revolutionary terrorists.[40]

Terrorism and its motivations are dependent on the current social and economic culture. This dependency can also be described with David Rapoport's concept of the "waves" of terrorism ('The Four Waves of Terrorism'), these are, for example, the anarchist wave which emerged in the late nineteenth century/early twentieth century, the anti-colonial wave (starting with the post-World War I political principle of self-determination, *e.g.* as mentioned in Tartu Peace Treaty of 02.02.1920[41]), as well as extreme left waves and religious waves (as what we have occurring nowadays).[42] Each wave describes the dominant strategic goals of terrorism during a specific time and space. [43] Parker and Sitter (2016), on the other hand, claim that terrorism and its motivations are rather dependent on four goal-oriented categories: socialism, nationalism,

[37] R. Värk. 2011, p. 81.
[38] *Ibid.*
[39] Counter-Terrorism Module. 1 Key Issues: United Nations and Terrorism. 2018.
[40] Britannica Encyclopedia. Types of Terrorism. Available at: https://www.britannica.com/topic/terrorism/Types-of-terrorism
[41] It states the following: "*In consequence of the right of all peoples to self-determination, to the point of seceding completely from the State of which they form part, a right proclaimed by the Socialist and Federal Russian Republic of the Soviets, Russia unreservedly recognises the independence and sovereignty of the State of Estonia, and renounces voluntarily and forever all sovereign rights possessed by Russia over the Estonian people and territory whether these rights be based on the juridical position that formerly existed in public law, or in the international treaties which, in the sense here indicated, lose their validity in future.*" From: Article 2 of Peace Treaty of Tartu. Tartu, Estonia, 02.02.1920. Available at: https://hub.xpub.nl/termsofservice/peace-treaty-of-tartu.html
[42] D. Rappoport. The Four Waves of Modern Terrorism. A. Cronin, J. Ludes, eds. Attacking Terrorism: Elements of a Grand Strategy. Washington, DC: Georgetown University Press. 2004, pp. 46–73.
[43] Counter-Terrorism Module 1. Key Issues: Brief History of Terrorism. 2018.

religious extremism or exclusionism which do not necessarily rise and fall but can also occur in parallel and work as underlying motivators for different terrorist movements.[44]

The acts of terrorism could also be seen, on the one side, as the political martydoms, beautification and sacralization of violence, a personal commitment to a *"cause that could inspire others, and epitomised the revolutionary 'code of honour' by sparing innocent citizens".*[45]

3) location of attack:

To cause fear in the population, terrorists tend to choose high profile, increased shock value, attack locations that have high intensity of civilian population (schools[46], shopping centres[47], bus and train stations[48], restaurants and nightclubs[49], airports[50], concerts[51]) and buildings and other locations that are important economic or political symbols (embassies, military installations, churches).[52] Thus, terrorist threats are also global in nature as they are characterized by widespread distribution of the attacking locations.[53]

4) indiscriminate targeting

The modern acts of terrorism tend to be indiscriminate in their target selection. That means that terrorists do not make a distinction between civilians and military objectives, as humanitarian law prescribes. The industrialized and indiscriminate means and methods of warfare utilized during the world wars taught post-war revolutionary terrorists to disregard the principle of distinction and to adopt more irregular weapons and forms of fighting, such as urban guerrilla

---

[44] *Ibid.*;
T. Parker, N. Sitter. The Four Horsemen of Terrorism: It's Not Waves, It's Strains. Routledge. 2016, p. 199. Available at:
https://www.tandfonline.com/doi/pdf/10.1080/09546553.2015.1112277
[45] Counter-Terrorism Module 1 Key Issues: Terrorism in the 19th Century. 2018.
[46] Encyclopedia Britannica. Peshawar school massacre. Available at:
https://www.britannica.com/event/Peshawar-school-massacre
[47] See, for example, BBC News. Westgate attack: Two jailed over Kenyan shopping mall attack. 2020. Available at:
https://www.bbc.com/news/world-africa-54748341
[48] See, for example, BBC News. 7 July London bombings: What happened that day? 2015. Available at:
https://www.bbc.com/news/uk-33253598
[49] The New York Times. Realizing It's a Small, Terrifying World After All. Orlando Shooting. 2016. Available at:
https://www.nytimes.com/2016/06/21/us/orlando-shooting-america.html
[50] See, for example, South China Morning Post. Istanbul airport bombers planned to take hostages during attack. Available at: https://www.scmp.com/news/world/middle-east/article/1984157/istanbul-airport-bombers-planned-take-hostages-during-attack
[51] See, for example, BBC News. Ariana Grande reflects on Manchester bombing ahead of anniversary. 2020 Available at:
https://www.bbc.com/news/entertainment-arts-52752383
[52] J. P. Jenkins. Terrorism. Encyclopedia Britannica.
[53] N. A. Makhutov, V. P. Petrov, and D. O. Reznikov. 2009, p. 55.

warfare.[54] Indiscriminate weapons (*e.g.*, high-level bombing capacities, weapons of mass destruction) is a recurring feature in the modern threat landscape.[55] Due to the features of cyberspace, attacks through cyberspace could be even more indiscriminate against its targets.

5) Non-state actor:

Terrorism in general refers to acts committed by nonstate actors. However, including state or state-sponsored terrorism under the definition has also been suggested (and debated upon). In practise, the term "terrorism" has also been used to refer to the acts committed by the state. For example, Iran has referred to the attack on the 11th of April 2021 against Natanz nuclear facility as an act of "nuclear terrorism" and attributed the attack to Israel.[56] As well, there has been state-supported terrorism, for example, Iran and Syria have allegedly provided logistical and financial aid to Islamic revolutionary groups engaged in campaigns against Israel, the United States, and some Muslim countries in the late 20th and early 21st centuries.[57]

1.2. Cyberterrorism

Terrorists, as well as other malicious actors have gained many advantages with the utilization of different technological means (such as automatic weapons or compact, electrically detonated explosives). It gives terrorists new methods and opportunities that provide greater mobility and increased lethality and spread of the attacks.[58] Cyber means are also attractive options for modern terrorists, as they can provide anonymity, and have the potential to inflict massive damage, cause serious psychological impact, and inflict media appeal.[59]

The United Nations Office on Drugs and Crime (abbr. UNODC) report outlines the means by which the Internet is utilized for terrorist purposes, these are: propaganda (including recruitment, incitement, radicalization), financing, training, planning (including preparatory secret communication and publicly available information), execution (inducing fear, fabricating or circulating threat over Internet), cyberattacks (including disrupting the functioning of target's computer systems, servers or underlying infrastructure).[60]

---

[54] Counter-Terrorism Module 1 Key Issues: Brief History of Terrorism. 2018.
[55] *Ibid.*
[56] The New York Times. Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage. Available at: https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html
[57] Encyclopedia Britannica. Types of Terrorism. Available at: https://www.britannica.com/topic/terrorism/Types-of-terrorism
[58] *Ibid.*
[59] G. Weimann. Cyberterrorism: How Real Is the Threat? United Nations Institute of Peace. Special Report. Washington. 2004, p. 6. Available at: https://www.usip.org/sites/default/files/sr119.pdf
[60] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009, pp. 3-11.

In addition to the use of the Internet, cyberterrorism can go even beyond, covering the use of hardware, software, information systems, but also people, content, social interactions within these networks.[61] Cyberterrorism is, thus, a terrorist's use of cyberspace. Cyberspace can be a tool, target, or a space of a crime (including cyberterrorism).[62] The International Telecommunications Union (abbr. ITU) uses the term "cyberspace" to describe the "*systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks*".[63]

Therefore, terrorists could use open source media for spreading disinformation, sophisticated use of media for recruitment and radicalization, encrypted applications for communications, conducting ransomware attacks and using phishing to spread malware, attacking IoT devices, *etc*.

Cyberterrorism is the convergence of cyberspace and terrorism, terms that both create discussions about their essence.[64] Cambridge Dictionary defines cyberterrorism as "*the use of the internet to damage or destroy computer systems for political or other reasons*".[65] According to Encyclopedia Britannica, cyberterrorism is "*the use of the Internet to cause public disturbances and even death*" and leaves political aim out of the definition.[66] Collins dictionary ties the definition more directly with human consequences, as it states "*cyberterrorism is the use of computers and the internet to attack or frighten large numbers of people, usually in order to achieve political aims or to force a government to do something*".[67]

Mark M. Pollit defines cyberterrorism as *"the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents."* In this case, cyberspace (including, for example, computer systems) is a target rather than a tool. Pollit's

---

[61] M. E. Hathaway, A. Klimburg. National Cyber Security: Framework Manual. Cyber Terms and Definitions. Gen. ed. A. Klimburg. NATO CCD COE. Tallinn. 2012, p. 8.
[62] ISO/IEC 27032:2012. Information technology - Security techniques - Guidelines for cybersecurity. 2012, para. 4.18. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en
[63] ITU. ITU National Cybersecurity Strategy Guide. Geneva. 2011, p. 5. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf
[64] D. Denning. Articles, testimony on the subject before the House Armed Services Committee in May 2000;
Also: Mark M. Pollitt's article 'Cyberterrorism: Fact or Fancy?,' published in Computer Fraud and Security in 1998
[65] Cambridge Dictionary. Cyberterrorism. Available at: https://dictionary.cambridge.org/dictionary/english/cyberterrorism
[66] Encyclopedia Britannica. Cybercrime. Types of Cybercrime. Available at: https://www.britannica.com/topic/cybercrime#ref1285671
[67] Collins Dictionary. Cybererrorism. Available at: https://www.collinsdictionary.com/dictionary/english/cyberterrorism

definition is utilized by the Federal Bureau of Investigation (FBI) of the United States.[68] Dorothy Denning similarly defines cyberterrorism as "*the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."*[69] Nelson *et al.* define cyberterrorism as follows: *"Cyberterrorism is the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological."* These definitions focus on defining cyberterrorism as an attack against ICTs, however, the term has also been used more broadly referring to cyberspace as a tool or a space of cyberterrorism (in addition to being a target of an attack).[70] In parallel, the term "technological terrorism" that includes cyberterrorism but also electromagnetic, biological, chemical, radiological terrorism, is also used by some authors. Technological terrorism has been defined as "*actions directed against infrastructure elements critically important for national security or committed with the use of specially hazardous technologies, technical means, and materials*".[71] This definition, however, leaves out political motivation or social objectives, does not define attacker or target people but adds that the attack must be against critical infrastructure.

Therefore, the difference between kinetic terrorism versus cyberterrorism is that cyberterrorism involves the use of digital means or digital targets.[72] Additionally to the elements of conventional terrorism, *i.e.* political or ideological motive, fear as an outcome and presumably a non-state actor, cyberterrorism has also a digital element related to the crime.[73] Cyberterrorism has the capability to cause damage of an unpredictable amount or level and spread enormously.[74] Cyberterrorism could be appealing to terrorists as it is much cheaper,

---

[68] L. MacKinnon, D. Gan, L. Bacon, G. Loukas. D. Chadwick, D. Frangiskatos. Strategic Intelligence Management. Book Chapter 20: Cyber Security Countermeasures to Combat Cyber Terrorism. 2013, p. 234. Available at: https://www.researchgate.net/publication/285181525_Cyber_Security_Countermeasures_to_Combat_Cyber_Terrorism

[69] D. Denning. Articles, testimony on the subject before the House Armed Services Committee in May 2000; D.E. Denning. Cyberterrorism.Global Dialogue, 2000.

[70] ISO/IEC 27032:2012. Information technology - Security techniques - Guidelines for cybersecurity. 2012, para. 4.18. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

[71] N. A. Makhutov, V. P. Petrov, and D. O. Reznikov. 2009, p. 53.

[72] T. Stevens. Handbook of Terrorism and Counter Terrorism post 9/11. Strategic cyberterrorism: problems of ends, ways and means. 2019, p. 43.

[73] J. Jarvis, S. Macdonald. What is cyberterrorism? Findings from a survey of researchers. Terrorism and Political Violence 27, no. 4. 2017, pp. 657-78.

[74] J.-T. Kim, T. Hyun. Status and Requirements of Counter-Cyberterrorism. World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering. Vol:1, No:6, 2007. Available at: https://publications.waset.org/11708/status-and-requirements-of-counter-cyberterrorism

more anonymous than traditional methods, the variety and number of targets is very large and it can be conducted remotely.[75] Costs to launch a grave malicious cyber operation are much lower than the costs of kinetic operations whilst the consequences of a cyber operation could be much worse.

It is important to bear in mind that all malicious operations through networks should not automatically be classified as acts of cyberterrorism. For an act to be qualified as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear of such violence or damage. Acts of cyberterrorism would be, for example, attacks that lead to death or bodily injury, explosions, or severe economic loss. Attacks with significant impact, for example, against critical infrastructures could be acts of cyberterrorism. Attacks that merely disrupt nonessential services or that are just costly disturbances without a significant impact would not qualify as cyberterrorism.[76]

Although perhaps the feared threat of cyberterrorism has not yet fully materialized, there have been several early warnings (especially after the 9/11 attacks in 2001). Already in 1977, Robert Kupperman, then Chief Scientist of the US Arms Control and Disarmament Agency, stated: *"Commercial aircraft, natural gas pipelines, the electric power grid, offshore oil rigs, and computers storing government and corporate records are examples of sabotage-prone targets whose destruction would have derivative effects of far higher intensity than their primary losses would suggest. Thirty years ago terrorists could not have obtained extraordinary leverage. Today, however, the foci of communications, production and distribution are relatively small in number and highly vulnerable."* [77] The 1991 published book "Computers at Risk" starts as follows *"We are at risk. America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable – to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more*

[75] G. Weimann. 2004, p. 6.
[76] D. E. Denning. Testimony before the Special Oversight Panel on Terrorism. U.S. House of Representatives. Committee on Armed Services. 2000. Available at http://commdocs.house.gov/committees/security/has144240.000/has144240_0f.htm;
D. E. Denning. Cyberterrorism. Global Dialogue. 2000. Available at: http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf
[77] M. G. Devost, B. K. Houghton, N. A. Pollard. Information Terrorism: Political Violence in the Information Age. 1997, p. 76.

with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[78]

Major malicious cyber operations that have caught great media appeal, such as, I LOVE YOU virus[79], Estonia 2007 cyber attack[80], NotPetya[81], WannaCry[82], SolarWinds cyber attack[83], Stuxnet worm[84], have shown the significance of cyberattacks, and thus acts of potential cyberterrorism. On the other hand, major terrorism incidents, *e.g.* 1993 World Trade Center bombing[85], 9/11 attacks[86], 2005 London bombings[87], 2011 Norway attacks[88] or Charlie Hebdo attack in 2015[89], Sri Lanka Easter bombings[90], to name few, have demonstrated the world the significance of the threat of terrorism. According to GTA in 2019 there were approximately 8500 terrorist attacks around the world which killed more than 20300 people.[91]

---

[78] National Research Council, Computers at Risk: Safe Computing in the Information Age. Washington DC: National Academy Press. 1991, p. 7. Available at: http://www.nap.edu/books/0309043883/html/index.html

[79] J. Griffiths. 'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on. CNN Business. 2020. Available at: https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html

[80] J. Davis. Hackers Take Down the Most Wired Country in Europe. The Wired. 2007. Available at: https://www.wired.com/2007/08/ff-estonia/

[81] A. Greenberg. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. The Wired. 2018. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[82] Z. Whittaker. Two Years after WannaCry, a million computers remain at risk. TechCrunch. 2019. Available at: https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1

[83] I. Jibilian, K. Canales. The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. Business Insider. 2021. Available at: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[84] E. Nakashima, J. Warrick. Stuxnet was the work of U.S. and Israeli experts, officials say. The Washington Post. 2012. Available at: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

[85] U.S. Department of State. 1993 World Trade Center Bombing. 2019. Available at: https://www.state.gov/1993-world-trade-center-bombing/

[86] National Commission on Terrorist Attacks Upon the United States. The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks Upon the United States. Available at: https://govinfo.library.unt.edu/911/report/911Report_Exec.htm

[87] BBC News. 7 July London bombings: What happened that day? 2015. Available at: https://www.bbc.com/news/uk-33253598

[88] The New York Times. Anders Behring Breivik, Killer in 2011 Norway Massacre, Says Prison Conditions Violate His Rights. 2016. Available at: https://www.nytimes.com/2016/03/16/world/europe/anders-breivik-nazi-prison-lawsuit.html

[89] The Guardian. Charlie Hebdo trial: French court convicts 14 over 2015 terror attacks. 2020. Available at: https://www.theguardian.com/world/2020/dec/16/charlie-hebdo-trial-french-court-convicts-14-over-2015-terror-attacks

[90] BBC News. Sri Lanka attacks: Easter Sunday bombings marked one year on. 2020. Available at: https://www.bbc.com/news/world-asia-52357200

[91] National Consortium for the Study of Terrorism and Responses to Terrorism. Global Terrorism Overview: Terrorism in 2019. Background Report. University of Maryland. 2020. Available at: https://www.start.umd.edu/pubs/START_GTD_GlobalTerrorismOverview2019_July2020.pdf

The threats of cyberterrorism have also been illustrated with some incidents occurred. For example, in 2000, the Japanese Aum Shinryko cult's, the same group that was behind the 1995 Tokyo subway attack[92], software was used in 150 police vehicles which enabled the cult to receive classified tracking data on 115 vehicles. The Cult had also developed software for at least 80 Japanese firms and 10 government agencies and could have installed Trojan horses to launch or facilitate cyber terrorist attacks.[93]

As well, after the 9/11 attacks, Osama bin Laden allegedly stated that *"hundreds of Muslim scientists were with him who would use their knowledge [...] ranging from computers to electronics against the infidels."* Frank Cilluffo of the Office of Homeland Security has famously commented that *"[w]hile bin Laden may have his finger on the trigger, his grandchildren may have their fingers on the computer mouse".*[94]

Thus, cyberterrorism is an increasingly worrisome issue. Nevertheless the realness and the significance of the threat of cyberterrorism, the world is still lacking a comprehensive definition of cyberterrorism. The term is often overused or misused by popular media but a good operational definition is still lacking. The lack of common sense in the definition of cyberterrorism risks the threat, once fully materialized, to emerge into major horror to humanity. A main obstacle for creating a definition of cyberterrorism is, consequently, the lack of an agreed-upon definition of terrorism.[95]

1.3. Legal definitions

The only global treaty on terrorism that contains the definition of terrorism is the 1937 League of Nations Convention on the Prevention and Punishment of Terrorism. Article 1(2) of the 1937 Convention defines *"acts of terrorism"* as *"criminal acts directed against a state"* that must be *"intended or calculated to create a state of terror in the minds of particular persons, or a group of persons or the general public".*[96] The Convention includes a psychological element to the definition but does not define the purpose of the state of terror or fear generated.[97] Nor did the Convention address the issue of people's self determination and independence movements not

[92] BBC News. Aum Shinrikyo: The Japanese cult behind the Tokyo Sarin attack. 2018. Available at: https://www.bbc.com/news/world-asia-35975069
[93] G. Weimann. 2004, p. 12.
[94] *Ibid.*
[95] M. Conway. Cyberterrorism: Hype and Reality. Dublin City University. 2007, p.5. Available at: https://core.ac.uk/download/pdf/11308376.pdf
[96] UNODC. Introduction to international terrorism. Vienna. 2018. Available at: https://www.unodc.org/e4j/en/terrorism/module-1/key-issues/league-of-nations-and-terrorism.html
[97] E. Chadwick. Self-Determination, Terrorism and the International Humanitarian Law of Armed Conflict. 1996. Available at: https://www.unodc.org/e4j/en/terrorism/module-1/key-issues/league-of-nations-and-terrorism.html

to be qualified as terrorism. This treaty never entered into force because it received only one ratification, however, this definition laid the foundation for the definitions used in subsequent instruments.

In the 1991 Resolution, the United Nations General Assembly significantly reaffirmed "*the inalienable right to self-determination and independence of peoples under colonial and racist and other forms of alien domination*" and recognized that the fight against terrorism could be enhanced with the definition of terrorism. Preceding resolutions adopted by the General Assembly focused on measures to eliminate international terrorism and study of its underlying causes, but did not aim to define the phenomen itself. In the 1994 Declaration on Measures to Eliminate International Terrorism, the General Assembly qualified terrorism as a grave violation of the purpose and principles of the United Nations and characterized terrorism as unjustifiable (not justifiable on the basis of a political, philosophical, ideological, racial, ethnic, religious or any other nature) criminal acts intended to provoke a state of terror in general public. This was the same language used in the 1937 Convention.[98]

The 1996 ILC Draft Code defined international terrorism as "*undertaking, organizing, facilitating, financing, encouraging or tolerating acts of violence against another State directed at persons or property and of such nature as to create a state of terror (fear or dread) in the minds of the public figures, groups of persons or the general public in order to compel the aforesaid State to grant advantages or to act in a specific way*".[99]

The 1999 Convention for the Suppression of the Financing of Terrorism refers to terrorism as acts listed in the sectoral instruments or, referring to the context of armed conflict, as "*[a]ny other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act*".[100]

These international instruments, although officially interpreted the concept, did not provide comprehensive definition of international terrorism nor solved the issue with the struggle of peoples for national liberation and independence not falling under the scope of terrorism.

[98] A. Cassese, P. Gaeta, J. R. W. D Jones. The Rome Statute of the International Criminal Court: A Commentary. Volume 1. Oxford University Press. 2002, pp. 510-519.
[99] *Ibid.* p. 514.
[100] United Nations. International Convention for the Suppression of the Financing of Terrorism. 1999. Available at:
https://www.un.org/law/cod/finterr.htm

Nevertheless, international community has adopted a long list of sectoral instruments on terrorism, which could feed to the generic definition. These instruments provide workable and pragmatic solutions to the specific acts of terrorism, like hijacking or nuclear terrorism.[101]

Without an universal definition, regional organisations and national governments have adopted different approaches to fight against terrorism. In 2002, with framework decision 2002/475/JHA of 13 June 2002 on combating terrorism, all EU Member States agreed on the common definition of terrorism that would be used in national legislations.[102] That definition is also enshrined in the 2005 Council of Europe Convention on the Prevention of Terrorism.[103] Notably, the decision also included incitement (including indirect incitement) to commit a terrorist offence under the scope of terrorism which was the first attempt by international law to define incitement to terrorism.[104] The decision was amended in 2008 with the decision 2008/919/JHA[105], in response to the growing terrorist threat and the use of new technologies (such as the Internet), and added provisions on public provocation and incitement (with reference to the Security Council resolution 1624). The definition leaves the scope of terrorism still open, but requires member states to implement the offence in a way that it respectable of human rights (including the right to freedom of expression).[106]

The UK and the US have passed legislation to specifically fight against cyberterrorism. Pursuant to the US's and the UK's legal framework, cyberterrorism is treated as an act of terrorism, as a special kind of cyber crime. Title 22 of the United States Code, Section 2656f(d) contains the following definition: "*The term 'terrorism' means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience.*" The latter definition of terrorism does not distinguish means or tools used to conduct the act of terrorism, thus covers cyberterrorism under its provision. [107] In 2001, the US passed a Patriot Act that encompasses

[101] R. Värk. 2011, pp. 79-80.
[102] UNODC. The use of the Internet for terrorist purposes. New York. 2012, p. 22. Available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf;
V. Ekstedt, T. Parkhouse, D. Clemente. National Cyber Security: Framework Manual. Commitments, Mechanisms and Governance. Gen. ed. A Klimburg. NATO CCD COE. Tallinn. 2012, p. 157.
[103] V. Ekstedt, T. Parkhouse, D. Clemente. National Cyber Security: Framework Manual. 2012, p. 157.
[104] *Ibid*, p. 157.
[105] The use of the Internet for terrorist purposes. 2012, p. 23.
[106] V. Ekstedt, T. Parkhouse, D. Clemente. National Cyber Security: Framework Manual. 2012, p. 157.
[107] M. Conway. 2007, p. 16.

acts of cyberterrorism.[108] According to the UK's updated (in February 2001) Terrorism Act an act of terrorism includes "*the use of or threat of action that is designed to seriously interfere with or seriously disrupt an electronic system*".[109]

According to the Japanese national approach cyberterrorism aims at *"seriously affecting information systems of private companies and government ministries and agencies by gaining illegal access to their computer networks and destroying data."*[110] Moscow-based ITAR-TASS news agency states that, in Russia, cyberterrorism is perceived as *"the use of computer technologies for terrorist purposes."*[111] Yael Shahar, Web master at the International Policy Institute for Counter-Terrorism, located in Israel, differentiates between a number of different types of information terrorism, these are: (1) electronic warfare that occurs when hardware is the target; (2) psychological warfare that has the goal of inflammatory content; (3) hacker warfare that degenerates into cyberterrorism.[112]

Leaving it up to national governments to define and criminalise terrorism, means that countries have very different approaches to this international crime and it is challenging to distinguish the crime among different political and legal systems. Thus it is difficult to distinguish which violent attacks against a government may be legitimate (*i.e.* national liberation, independence and self-determination movements against colonial and racist or other forms of alien domination and occupational regimes or systems), or to simply fight against international terrorism in an effective way. Applying this approach means that, for example, the African National Congress that conducted violent actions against South Africa's apartheid government but commanded broad sympathy in the international community, could be considered terrorists. Another example that could, with applying this approach, fall under the category of terrorism is the Resistance movement against the Nazi occupation of France during World War II.[113] Up to this day, the international community has not found a way to differentiate these two with an universal definition and has, thus, failed to provide a comprehensive global definition of terrorism.

---

[108] U.S. Congress. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. Public Law 107-56-OCT. 26, 2001. Authenticated U.S. Government Information. 2001. Available at: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

[109] M. Conway. 2007, p. 5.

[110] *Ibid*, p. 8.

[111] Foreign Broadcast Information Service (FBIS). Russia Cracks Down on 'Cyberterrorism'. ITAR-TASS. FBIS-SOV-2002-0208. 8 February, 2002.

[112] M. Conway. 2007, p. 8.

[113] J. P. Jenkins. Terrorism. Encyclopedia Britannica.

Although terrorism has been of great concern to international peace and security, the international community has struggled to come to a consensus on how to define the term "terrorism". Terrorism is a widely contested phenomena. Nevertheless, some general agreements have been reached on the definition of terrorism during peace time, but in times of armed conflict a significant dissensions among international community persist (such as whether freedom fighters that attack civilians should be labelled as terrorist, instead of war criminals, whether a state actions could be classified as terrorism).[114] The main obstacle for reaching a consensus on the definition is best described with the oft-cited phrase "*one person's terrorist is another person's freedom fighter*". Thus, many countries have been unwilling to establish such a universal definition as it might go against their national interests. The absence of universally agreed upon definition of terrorism also contributes to legal uncertainty and undermines "*the states' credibility and the legitimacy of their conduct in the war on terror"*.[115] Another dimension of confusion is then added with the cyber realm. In other words, as the term "terrorism" is widely contested, it is even more unclear how to define cyberterrorism. There is no international convention that would define and proscribe cyberterrorism.[116]

Without a globally agreed upon definition of terrorism, it is even more difficult to say what would be an exhaustive list of terror acts in cyberspace, which acts of cyberterrorism amount to use of armed force, which acts bring upon an responsibility. Cyberterrorism could refer to cyber attacks with certain characteristics to terrorism, or even more broadly, cyberterrorism could be any terroristic use of cyberspace. The latter includes also spreading false information, propaganda, radicalization, networking, recruiting, online training, financing, command and control of attacks, psychological warfare, and cyberattacks[117] which can be described as a "tool-oriented" cyberterrorism".[118] For the purpose of this paper the former approach will be preferred as cyber attacks of terrorism raise up vital questions about applicability of international law and to also limit the scope of this research.

[114] A. Cassese, G. Acquaviva, M. Fan, A. Whiting. International Criminal Law. Cases and Commentary. Terrorism. Oxford University Press. 2011, p. 288.
[115] R. Värk. 2011, p. 77.
[116] V. Ekstedt, T. Parkhouse, D. Clemente. National Cyber Security: Framework Manual. 2012, p. 156.
[117] D.Mair. #Westgate: A Case Study: How al-Shabaab used Twitter during an Ongoing Attack, Studies in Conflict & Terrorism. Available at: https://www.tandfonline.com/doi/pdf/10.1080/1057610X.2016.1157404?casa_token=0NzngSf4tisAAAAA:hajQRdhfivqtRzSdPEZgdjdZxhv4VZEMRmqb9ZPx5QyOblTaUNOXq_z54mGlKqfM5ww5WYm8mN6BxA
[118] A.-M. Talihärm. Cyberterrorism: in Theory or in Practice? Defence against terrorism review. 2010, p. 69.

Nietzsche has stated that ***"****[...] it is only that which has no history which can be defined".*[119] Nietzsche argues that any concept, such as terrorism, that has a long history of its own defies definition, it simply does not have just one precise meaning. Controversially, the international community has also struggled to define operations in cyberspace exactly because it is such a new concept and a lot is unclear on how to address issues related to cyberspace, or perhaps people do not even want to bind their hands with clear boundaries. In regards to terrorism, it is difficult to define it be it due to historical, national, cultural, ethnic standpoints. Geoffrey Levitt has said that "*the search for legal definition of terrorism is the holy grail*" and "*periodically, eager souls set out, full of purpose, energy and self-confidence, to succeed where many others have tried and failed."* Perhaps, then, trying to globally define cyberterrorism, is even more holy, and even more doomed to fail. However, international efforts and commitments are essential for fighting against this international crime. And through this common fight, perhaps even, the international community would develop a more harmonized approach that would subsequently seed the global definition on cyberterrorism. Without a universally agreed definition of cyberterrorism, international (cyber)terrorism has, nevertheless, still been addressed and tackled by international instruments. The next chapter will analyse the legal framework regulating cyberterrorism.

[119] F. Nietzsche. On the Genealogy of morals. 1887, II:13.

2. CHAPTER 2: LEGAL FRAMEWORK ON CYBERTERRORISM

Acts of terrorism could be the most grave forms of violence and can indiscriminately target all people. The terrorist acts in cyberspace could do the same, or even more so, as the world societies are highly and increasingly dependent on ICT infrastructures and the cyber tools are convenient tools for terrorists (see Chapter 1, para 1.2.), thus could become increasingly preferred means. It is then the most concerning that the legal status of terrorism and cyberterrorism in international law stays unclear. To fight against terrorism, effectively prosecute terrorists, ensure rule of law and accountability for the acts of terrorism, the international community needs to outlaw these acts with comprehensive and effective up-to-date regulations. Yet there is no binding international legal instrument that would regulate and proscribe international cyberterrorism. Nevertheless, acts of cyberterrorism could be encompassed by other existing legal instruments. Acts of cyberterrorism can be encompassed with specific regulations on cyberterrorism, or a combination of cybercrime and counter-terrorism legislation (*e.g.* applying existing cybercrime legislation to the terrorist use of ICTs or applying existing counter-terrorism legislation to the acts related to ICT-s), or, counter-terrorism or criminal acts without differentiating means of conduct (*i.e.* Internet or ICTs are regarded as tools or mediums and not as an individual element of a crime), depending on the approach.[120] In general, various acts of terrorism are prohibited under international humanitarian law, international criminal law, international human rights law and, debatably, under customary international law.[121] This chapter analyses the current legal framework in regards to responsibility of cyberterrorism.

2.1. International law on terrorism

2.1.1. General instruments

Although there is no universally accepted binding definition of terrorism, many legal instruments regulate and outlaw specific acts of terror (including terrorist acts in cyberspace). However, there is no overarching general convention on terrorism, let alone cyberterrorism.

Already by the 1930s, many bilateral agreements referred to the suppression of terrorism and many extradition treaties addressed assassination attempts against Chiefs of State (*e.g.*

[120] Counter-Terrorism Implementation Task Force (CTITF). Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects. CTITF Working Group Compendium. 2011. Available at: https://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf

[121] H. Edwards. International law and terrorism: the case of ISIS. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019. p. 28.

Convention on Extradition 1933, article 3 (e)).[122] By 1937, a Committee of Experts, established by the League Council, drafted a Convention on Terrorism that outlined acts of terrorism that State Parties were obliged to criminalize within their domestic laws. The 1937 Convention did not enter into force.[123]

Since 1972, the United Nations General Assembly (abbr. UNGA) has adopted several (non-binding) resolutions aimed at eliminating international terrorism, *e.g.* resolutions in 1972, 1985, 1987 and 1991. The 1991 resolution confirmed "*inalienable right to self-determination and independence of peoples under colonial and racist or other forms of alien domination and foreign occupation* [...]".[124] In 1994 and 1996, the General Assembly adopted the declaration on Measures to Eliminate International terrorism, which characterized terrorist acts.[125] In 1994, the General Assembly reaffirmed that the acts of terrorism are "*criminal and unjustifiable, wherever and by whomever committed* [...]" and stated that "*criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them*".[126]

In 2005, a Draft Comprehensive Convention against International Terrorism was presented to the UNGA. The draft convention regulates the acts of terrorism by stating the following:

"Any person commits an offence within the meaning of the present Convention if that person, by any means, unlawfully and intentionally, causes:
(a) Death or serious bodily injury to any person; or
(b) Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or to the environment; or
(c) Damage to property, places, facilities or systems referred to in paragraph 1 (b) of the present article resulting or likely to result in major economic loss;

[122] Introduction to international terrorism. 2018.
[123] *Ibid.*
[124] A. Cassese, P. Gaeta, J. R. W. D Jones. 2002, pp. 510-511.
[125] *Ibid.* p. 512.
[126] United Nations General Assembly resolution 49/60 of 9 December 1994. Declaration on Measures to Eliminate International Terrorism. A/RES/49/60.

when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act."[127]

Although this definition is an important achievement in trying to establish a general definition of terrorism, states still disagree whose actions would be covered by this regulation.[128] Nevertheless, this convention has not been adopted yet, thus its effect is limited with a normative value but not a forcible binding effect.

In 2006, the UN General Assembly adopted a resolution called the Global Counter-Terrorism Strategy which includes the Plan of Action and provides Member States with a common strategic approach to fight terrorism.[129] Pursuant to the Plan of Action, Member States decided, *inter alia*: "[t]*o consistently, unequivocally and strongly condemn terrorism in all its forms and manifestations, committed by whomever, wherever and for whatever purposes, as it constitutes one of the most serious threats to international peace and security*" and, notably, "[t]*o work with the United Nations with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to "(a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; (b) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard".* [130]

A new era in the fight against terrorism started with the attacks of 11 September 2001 on the USA, after which the Security Council adopted Resolution 1373[131] that, *inter alia*, called up states to ban and prevent financing and supporting terrorists. The United Nations Security Council has also adopted several key resolutions to further international cooperation in the investigation, detection, arrest, extradition and prosecution of those involved in terrorist acts, and to take necessary legislative and other measures to combat terrorism by all Member States.[132] In its resolution 1624 (2005)[133], the Security Council also condemns incitement and glorification or justification of terrorist acts, and calls upon all States to prohibit by law. The

[127] UNGA. Letter dated 3 August 2005 from the Chairman of the Sixth Committee addressed to the President of the General Assembly. A/59/894. Available at: https://undocs.org/en/A/59/894
[128] R. Värk. 2011, p. 79.
[129] UNGA. The United Nations Global Counter-Terrorism Strategy. A/RES/60/288. New York: United Nations. 2006. Available at: https://undocs.org/en/A/RES/60/288
[130] *Ibid.*
[131] United Nations Security Council. Resolution 1373 (2001). S/RES/1373. 2001. Available at: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf
[132] In particular, resolutions 1373 (2001), 1267 (1999) and 1566 (2004)
[133] United Nations Security Council. Resolution 1624 (2005). S/RES/1624. 2005. Available at: https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1624%282005%29

Security Council resolutions do not provide clear definition of terrorism but condemn some acts of terrorism.

2.1.2. Sectoral instruments

As there is no overarching regulation on terrorism, notably, the means used for the acts of terrorism have an effect on the applicable law.[134] Since the 1960s various treaties have banned specific acts related to terrorism (*e.g.* Conventions on the safety of civil aviation, the Hostages Convention). A number of different sectoral conventions[135], the United Nations auspices and specialized agencies, *i.e.* the International Civil Aviation Organization and the International Maritime Organization, and the International Atomic Energy Agency provide guidance, and address and regulate specific acts of terrorism on the sectoral level. These international instruments cover the following terrorist acts: acts of aviation sabotage, acts of violence at airports, hijacking of aircrafts, acts against the safety of maritime navigation, acts against the safety of fixed platforms located on the continental shelf, crimes against internationally

[134] V. Ekstedt, T. Parkhouse, D. Clemente. National Cyber Security: Framework Manual. 2012, p. 156.
[135] 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft (Aircraft Convention) (deposited with the International Civil Aviation Organization);
1970 Convention for the Suppression of Unlawful Seizure of Aircraft (Unlawful Seizure Convention) (deposited with the International Civil Aviation Organization);
1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Civil Aviation Convention) (deposited with the International Civil Aviation Organization);
1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons (Diplomatic agents Convention);
1979 International Convention against the Taking of Hostages (Hostages Convention) (deposited with the Secretary-General of the United Nations);
1980 Convention on the Physical Protection of Nuclear Material (Nuclear Materials Convention) (deposited with the International Atomic Energy Agency);
1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (extends and supplements the Montreal Convention on Air Safety) (Airport Protocol) (deposited with the International Civil Aviation Organization);
1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Maritime Convention) (deposited with the International Maritime Organization);
1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf (Fixed Platform Protocol) (deposited with the International Maritime Organization);
1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection (Plastic Explosives Convention) (deposited with the International Civil Aviation Organization);
1997 International Convention for the Suppression of Terrorist Bombings (Terrorist Bombing Convention);
1998 International Convention for the Suppression of Terrorist Bombings;
1999 International Convention for the Suppression of Terrorist Financing (Terrorist Financing Convention);
2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (deposited with the International Maritime Organization)
2005 Protocol to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (deposited with the International Maritime Organization);
2005 International Convention for the Suppression of Acts of Nuclear Terrorism;
2005 Amendments to the Convention on the Physical Protection of Nuclear Material (deposited with the International Atomic Energy Agency).

protected persons (such as the kidnapping of diplomats), acts of unlawful taking and possession of nuclear material, acts of hostage-taking, acts of terrorist bombings and acts of funding the commission of terrorist acts and terrorist organizations. These instruments are legally binding only to the signatories[136] as the member states have to enforce provisions of the conventions through national jurisdictions.[137]

2.1.3. Regional instruments

In addition to international instruments, regional conventions on terrorism have been adopted in Latin America, Europe, by the South Asian Association for Regional Cooperation (abbr. the SAARC), and by the Arab States.[138] These regional legal instruments aiming to combat terrorism are, for instance, the 1971 Organization of American States' Convention to Prevent and Punish Acts of Terrorism Taking the Form of Crimes against Persons and Related Extortion that are of International Significance, 1977 European Convention on the Suppression of Terrorism, 1987 South Asian Association for Regional Cooperation (SAARC) Regional Convention on Suppression of Terrorism, 1998 Arab Convention on the Suppression of Terrorism, 1999 Treaty on Cooperation among States Members of the Commonwealth of Independent States in Combating Terrorism, 1999 Convention of the Organization of the Islamic Conference on Combating International Terrorism, 1999 Convention of the Organization of the Islamic Conference on Combating International Terrorism, 2007 Association of South East Asian Nations (ASEAN) Convention on Counter Terrorism, 2005 Council of Europe Convention on the Prevention of Terrorism. These regional instruments complement and provide useful legal frameworks, yet they do not replace international instruments that can be utilized outside a particular geographical region and provide means to cooperate internationally.[139]

As there is no universally agreed upon definition of terrorism, there is also no comprehensive United Nations instrument on terrorism with an exhaustive list of the manifestations of terrorism. Thus, the international legal framework on terrorism is scattered and has developed along sectoral (or regional) lines, criminalizing specific acts of terrorism without searching for consensus on the broader concept of terrorism. The crimes outlined by these instruments do not, however, constitute crimes under international law. These are crimes under domestic laws as the member states will incorporate these crimes under national legislation. These instruments

[136] For a list of the current ratification status of these universal legal instruments, please see www.unodc.org/tldb/ universal_instruments_NEW.html.
[137] The use of the Internet for terrorist purposes. 2012.
[138] A. Cassese, P. Gaeta, J. R. W. D Jones. 2002, p. 513.
[139] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009, p. 34-35.

support cooperation to enable States parties to either prosecute and extradite the alleged offenders.[140]

2.2. International law on cyberterrorism

No universal convention has been adopted specifically relating to the terrorist use of cyberspace. Furthermore, international law that regulates and addresses traditional attacks, targets, weapons, and effects, does not explicitly mention *"cyber".* Thus, an analogy is primarily used to apply international law in the cyber context.[141] However, due to the spread of technology, cyberspace has also been used for malicious acts.

Although not explicitly through international law *per se,* the international community has still addressed the issue of cyberterrorism through different channels. Since 1990, the United Nations General Assembly has addressed the issue of cybercrime and has adopted respective resolutions (1990 resolution dealing with computer crime legislation and 2000 and again in 2002 resolutions dealing with criminal misuse of ICT. These resolutions encouraged countries to revise their penal codes - *e.g.* in 1997, Russia updated its penal code by addressing cyber crime, IT crime, and cyberterrorism. [142]

United Nations reports and resolutions following the 2001 General Assembly resolution 1373, have specifically addressed the importance of countering terrorist use of the Internet. In the UNGA Global Counter-Terrorism Strategy, member states were encouraged to explore the means and ways the Internet is used by terrorists and also how to use the tools of the Internet for countering the spread of terrorism. In 2001, Security Council labelled international terrorism as a threat to peace.[143] 2010 resolution 1923[144], the Security Council has expressed "*concern at the increased use, in a globalized society, by terrorists of new information and communications technologies, in particular the Internet, for the purposes of the recruitment and incitement as well as for the financing, planning and preparation of their activities*".

While the current international law does not provide sufficient guidance and clarity for cyberterrorism, the existing legal framework of international law is applicable to acts committed in and through cyberspace as international law is written broad enough to

[140] The use of the Internet for terrorist purposes. 2012.
[141] The Global Campaign for Ratification and Implementation of the Kampala Amendments on the Crime of Aggression. The Council of Advisers on the Application of the Rome Statute to Cyberwarfare. Available at: https://crimeofaggression.info/the-campaign/the-council-of-advisers-on-the-application-of-the-rome-statute-to-cyberwarfare/
[142] M. E. Hathaway, A. Klimburg. National Cyber Security: Framework Manual. 2012, p. 13-14.
[143] United Nations Security Council. Resolution 1373.
[144] United Nations Security Council.Resolution 1923 (2010). S/RES/1923. 2010. Available at: http://unscr.com/en/resolutions/doc/1923

incorporate new concepts, technology, and terminology.[145] The applicability of international law to cyberspace was confirmed with a 2013 UN Group of Governmental Experts (abbr. UN GGE) landmark report[146] (and further elaborated with the 2015 report[147]). These reports elaborate on how international law applies to cyberspace, propose norms, rules and principles for the responsible behaviour of States and suggest capacity and confidence building measures. In the 2015 report, UN GGE also warned that "*The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.*" The 2015 report provides 11 voluntary, non-binding norms of responsible State behaviour, including the rules such as "*States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs*", states "*should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public*", and states "*should take appropriate measures to protect their critical infrastructure from ICT threats*", as well as rules on cooperation, assistance and prosecuting terrorists.[148] UN GGE will release a new report in 2021.

In parallel, the General Assembly has also established The Open-Ended Working Group (abbr. OEWG) to also provide guidance on the application of international law on cyberspace, including to develop the rules, norms, and principles of responsible behaviour of states, discuss ways for their implementation, and, in addition, to study the possibility of establishing a regular institutional dialogue with broad participation under the auspices of the UN.[149] In March, the OEWG released its third substantive report.[150] In the third report the OEWG, *inter alia*, addressed the potential threat of cyberterrorism, stating that "*[t]he continuing increase in*

---

[145] United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2013. Available at:
https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf
(hereinafter cited as UN GGE. 2013.);
United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. 2015. Available at:
https://undocs.org/A/70/174 (hereinafter cited as UN GGE. 2015.)

[146] UN GGE. 2013.

[147] UN GGE. 2015.

[148] *Ibid.*

[149] GIP Digital Watch. UN GGE and OEWG. Available at:
https://dig.watch/processes/un-gge

[150] United Nations General Assembly. Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. A/AC.290/2021/CRP.2. 2021.
https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States."

Although the international community has agreed that international law applies to cyberspace, it remains unclear how exactly it applies. For example, what kind of cyber operations constitute an armed attack, how does the LOAC apply to cyber operations against civilian data, can malware be seen as a weapon, and what are legal and illegal cyber weapons. There are significant differences between the countries, but also within countries' different agencies, in how a cyber attack is defined.[151] In a 2020 statement to the UN Security Council, the ICRC President Peter Maurer emphasized on the need for greater clarity on how international law applies to cyber operations against critical infrastructure.[152] To this end, for example, an academic guidance, the Cyber Law Toolkit has been established to provide guidance on the uncertainty about the application of international law in cyberspace.[153]

In 1998, The Council of Europe (abbr. EC) released guidelines on cyber crime which included a policy to counter computer crime and terrorism and the mechanisms necessary to achieve this without constraining the fast development of e-commerce in the EU or affecting the right to privacy. The guideline calls up for a harmonization of member states' laws.[154] On the 23rd of November 2001, the Council of Europe adopted the Convention on Cybercrime which came into effect in 2004.[155] The Council of Europe's Convention on Cybercrime (aka Budapest Convention) is the first and only multilateral binding instrument to regulate cybercrime. Crimes regulated under the treaty are ones in which targeted ICTs. The Budapest Convention, *inter alia*, requires parties to criminalize certain acts under domestic law that may lead to the commission of terrorist offenses, such as public provocation, recruitment and training, all of which may be committed through the Internet.[156]

The Organization for Economic Cooperation and Development (abbr. OECD) has also released Guidelines for the Security of Information Systems and Networks. These Guidelines consist of

[151] A. Klimburg, J. Healey. National Cyber Security: Framework Manual. Strategic Goals and Stakeholders. Gen. ed. A Klimburg. NATO CCD COE. Tallinn. 2012, p. 75.
[152] K. Mačák, T. Jančárková, T. Minárik. 2020. The right tool for the job: how does international law apply to cyber operations? Humanitarian Law & Policy. ICRC blogs. Available at: https://blogs.icrc.org/law-and-policy/2020/10/06/international-law-cyber-operations/
[153] *Ibid.*
[154] J.-T. Kim, T. Hyun. 2007.
[155] Council of Europe. Convention on Cybercrime. 2001. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[156] The use of the Internet for terrorist purposes. 2012, p. 21.

nine principles that aim to increase public awareness, education, information sharing and training to enhance understanding of online security and the adoption of best practices.[157]

Asia-Pacific Economic Cooperation (APEC) has promoted cybersecurity within the Asia-Pacific region and addressed the threats posed by cyber crimes and terrorism. In their Statement on Fighting Terrorism and Promoting Growth, APEC Leaders collectively committed to: endeavour to enact a comprehensive set of laws relating to cyber security and cyber crime that are consistent with the provisions of international legal instruments.[158]

In 2006, the ASEAN Regional Forum released a statement that called up its members to adopt cybercrime and cyber security laws "*in accordance with their national conditions and should collaborate in addressing criminal and terrorist misuse of the Internet*". In 2009 were these recommendations codified within the Shanghai Cooperation Organization (ASEAN-China Framework Agreement) on information security.[159]

The International Telecommunication Union (ITU), a United Nations specialized agency for information and communication technologies, Constitution Article 33 recognizes the right of the public to use the International Telecommunication Service, Article 45 prohibits harmful interference of services mentioned in the article, but the Constitution also provides the right for a member state to stop telecommunications pursuant to Article 34 or suspend services pursuant to Article 34.[160] ITU has released the Toolkit for Cybercrime Legislation (2010) to promote harmonized national cybercrime legislation and procedural rules, including with respect to acts of terrorism committed by using the Internet or the transmission of malware with the intent of furthering terrorism. While the Toolkit mainly focuses on cybersecurity issues, it also contains several provisions for the criminalization of specific acts of terrorism involving the use of the Internet, such as section 3 (f) which addresses unauthorized access to computer programs and the transmission of malware for purposes of terrorism.*[161]*

The Council of European Union framework decision 2002/475/JHA[162] of 13 June 2002 on combating terrorism requires Member States to ensure that terrorist offenses are effectively

[157] J.-T. Kim, T. Hyun. 2007.
[158] *Ibid*.
[159] M. E. Hathaway, A. Klimburg. National Cyber Security: Framework Manual. 2012, p. 15;
G. Austin. China's Cybersecurity and Pre-emptive Cyber War. New Europe. 2011.
[160] ITU. Collection of the basic texts adopted by the Plenipotentiary Conference. 2019. Available at: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.22.61.en.100.pdf
[161] The use of the Internet for terrorist purposes. 2012.
[162] The Council of the European Union. Council of the European Union Framework Decision 2008/919/JHA of 28 November 2008 amending Framework 22 Decision 2002/475/JHA on combating terrorism. 2008/919/JHA. 2008. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0919

prosecuted, and outlines specific measures with regard to victims of terrorist offenses. The Council of Europe Convention on the Prevention of Terrorism has similar provisions on terrorism offenses. The 2008 decision provides a basis for prosecuting the intentional dissemination of terrorist propaganda and bomb-making expertise through the Internet. The decision 2008/919/JHA, similar to the Council of Europe Convention on the Prevention of Terrorism, while not being an Internet-specific instrument, the offenses covered with the instrument also cover activities conducted by means of the Internet.[163] Since 2013 the EU has issued documents on EU strategy on cybersecurity which have *inter alia* addressed concerns about terrorist threats on essential services.[164]

Internationally, the cybersecurity strategy is a very scattered topic. Even in the EU, countries have developed diverse national cybersecurity strategies and have quite different views on a variety of matters, including how to apply international law to cyberspace. The ambiguity is even greater in regards to cyberterrorism. The contextual unclarity and scatteredness in the legal framework might affect the accountability of cyberterrorism and undermine the efforts to tackle modern terrorism and hold the new generation of terrorists responsible. Thus, the international community is not only lacking a coherent and operative security strategy, but also a comprehensive and effective legal framework and a common sense on the topic of cyberterrorism to support the efforts. One of the main obstacles of the international approach on cyberterrorism is, yet again, an absence of a universally agreed definition of terrorism. Thus states have adopted different judicial and strategic approaches on the issue.

2.3. *Ius ad bellum*

The 1945 Charter of the United Nations articles and principles regulate acts of cyberterrorism. The Charter is found to be applicable to the new features and dynamics posed by cyberspace, however the precise scope and content is up for interpretation.[165] One of the fundamental principles of international law is sovereignty pursuant to Article 2 (1) of the United Nations Charter. The Permanent Court of Arbitration in the 1928 Island of Palmas case stated that „*Sovereignty 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*

[163] The use of the Internet for terrorist purposes. 2012, p. 21.
[164] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN/2013/01. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001
[165] V. Ekstedt, T. Parkhouse, D. Clemente. National Cyber Security: Framework Manual. 2012, pp. 151-152.

functions of a state".[166] UN GGE 2013 report (and reiterated in the 2015 report) confirms that sovereignty applies to cyberspace: „*State sovereignty and International norms and principles that flow from sovereignty apply to state conduct of ICT-related activities* [...]" and adding that „*in the use of ICTs, States must observe, among other principles of International law, State sovereignty, sovereign equality* [...]".[167] The second pre-draft of the OEWG Report (May 2020) reiterates that „*[s]pecific principles of the UN Charter highlighted include state sovereignty; sovereign equality* [...]".[168]

Rule 1 of the Tallinn Manual (first edition) interprets the principle of sovereignty in regards to cyberspace by stating that "[a] *State may exercise control over cyber infrastructure and activities within its sovereign territory*".[169] Rule 4 of the Tallinn Manuals also touches upon the principle of sovereignty. Rule 4 of the Tallinn Manual (first edition) states that any interference with cyber infrastructure that enjoys sovereign immunity, constitutes a violation of sovereignty.[170] Rule 4 of the Tallinn Manual 2.0 states that a State must not conduct cyber operations that violate the sovereignty of another State.[171] The acts of cyberterrorism could violate sovereignty by, for example, attacking essential services of the state or interfering into election systems.

According to the UN GGE 2013[172] and 2015 reports[173] and OEWG 2020 report[174], due diligence also applies to cyberspace. The International Court of Justice (ICJ) in the 1949 Corfu channel case, explained due diligence of states by stating that it is *"every state's obligation not to allow*

[166] United Nations. Reports of International Arbitral Awards. Island of Palmas case (Netherlands, USA). 1928, p. 838. Available at: https://legal.un.org/riaa/cases/vol_II/829-871.pdf
[167] UN GGE. 2013.
UN GGE. 2015.
[168] OEWG. Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 2020. Available at: https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf
[169] M. N. Schmitt. Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press. 2013, p. 15. Available at: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf
[170] *Ibid*, pp. 23, 26.
[171] M. N. Schmitt. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. 2017, p. 17.
[172] UNGA. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98*. 2013. Available at: https://eucyberdirect.eu/wp-content/uploads/2019/10/ungge-2013.pdf
[173] UNGA. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. 2015. Available at: https://undocs.org/A/70/174
[174] OEWG. 2020.

knowingly its territory to be used for acts contrary to the rights of other states".[175] According to the UN GGE 2015 report[176], "*states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs*" and the 2020 OEWG report[177] elaborated further that "*states must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts"*. In the cyber context, due diligence means that a state must not allow its territory, or territory or cyber infrastructure under its control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for other states.[178] Rule 5 of the Tallinn Manual states that States shall not knowingly allow their cyber infrastructure to be used for acts that adversely and unlawfully affect other States.[179] Thus, state have a due diligence obligation not to let their infrastructure to be used also by cyberterrorists.

A derivative principle of sovereignty, non-intervention (enshrined in Article 2(7) of the Charter), is also applicable to cyberspace and to cyberterrorism. The ICJ, in the 1986 Nicaragua case, explained the principle as „*a prohibited intervention must accordingly be one bearing on matters in which each state is permitted, by the principle of state sovereignty, to decide freely".*[180] There are two elements of the principle of non-intervention: 1) *domain reservé*, *i.e.* matters the state is permitted to decide freely are choice of the political, economic, social and cultural system, formulation of foreign policy (elections, language policy, the structure of governance, the terms of treaties); 2) coercion, *i.e.* acts that deprive another state of freedom of choice causing another state to act in a way it otherwise would not or refraining from acting in a way that it otherwise would act (threaten treaty violation to achieve election result).

Another derivative principle of international law is prohibition of use of force. The prohibition of the use of force in international law, as set out in Article 2(4) of the UN Charter, operates exclusively between states. According to Article 2(4) "*all 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*

[175] ICJ. 1949. The Corfu Channel case. Reports of judgments, advisory opinions and orders. Available at: https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf
[176] UN GGE. 2015.
[177] OEWG. 2020.
[178] M. N. Schmitt. Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press. 2013. Available at: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf
[179] M. N. Schmitt. Tallinn Manual on the International Law Applicable to Cyber Warfare. 2013, p. 15.
[180] ICJ. Nicaragua v. United States of America. Case concerning military and paramilitary activities in and against Nicaragua. Reports of judgments, advisory opinions and orders. 1986. Available at: https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Nations." In the cyber context, it is not the target or tool used that determines whether the use of force threshold has been crossed, but rather, the consequences of the operation and its surrounding circumstances and whether the consequences are comparable with those of a conventional armed attack (*e.g*. has physical damage or loss of life, or serious disruption to the functioning or stability of the state occurred).[181] Cyberattack and whether it is considered a use of force (as defined by the Law of Armed Conflict) and a *casus belli*, has different interpretations around the world with some countries being more ambiguous of the term's scope than others.[182]

This general prohibition of the use of force has two exceptions, *i.e.* the use of force in self-defence (Article 51 of the United Nations Charter) and a Security Council authorization of force (Article 42 of the United Nations Charter), in a case when the use of force is necessary for the maintenance or restoration of international peace and security (Chapter VII of the United Nations Charter). Article 51 requires an "armed attack" to be attributable to a state, thereby engaging its responsibility. The use of force is permitted only in case of self-defence of a state, or the UN Security Council declares a situation as a threat to international peace and security.[183] How international (cyber)terrorism violates the international prohibition of the use of force, remains a debatable topic. The UN Security Council has never officially authorized a use of force against terrorist threat, although the Council has classified terrorism as a threat to international peace and security and thus, could then possibly evoke the right of self-defence against terrorist threat.[184]

In this regard, the US took a position that customary international law to use self-defence exception may be extended to military operations against non-state actors (like ones in Syria and Iraq). However, some states disagree with extending customary international law to non-state actors in such a way.[185]

In terms of cyberspace, there is a broad agreement that cyber operations that cause similar effects as conventional kinetic actions that constitute as uses of force, *i.e.* death, injury, destructions, damage, qualify also as uses of force.*[186].* However, in matters where it is not so

[181] E. Luiijf, J. Healey. National Cyber Security: Framework Manual. Organisational Structures and Considerations. Gen. ed. A. Klimburg. NATO CCD COE. Tallinn. 2012, p. 117.
[182] M. E. Hathaway, A. Klimburg. National Cyber Security: Framework Manual. 2012, p. 18;
See also Rule 11 in the Tallinn Manual on the International Law Applicable to the Cyber Warfare, gen. ed Michael N. Schmitt. Cambridge University Press. 2013.
[183] B. Ahlhaus. Public international law, terrorism and insurgency post 9/11. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 16.
[184] *Ibid.* p. 15.
[185] T. Stevens. Handbook of terrorism and counter terrorism post 9/11. 2019, pp. 36-37.
[186] M. N. Schmitt. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2017, rule 82, para. 16.

apparent whether it could cross the threshold of armed conflict, for example, prolonged denial of service attack that does not cause direct consequences to civilians, qualifying cyber operations remain unclear.

Thus sovereignty, including principles of non-intervention, non use of force and due diligence, apply to cyberspace. However, it presents an ongoing difficulty to determine how and to what extent these principles apply to cyberspace and if and to what extent they are applicable to the acts of non-state actors, such as terrorists.

2.4. *Ius in bello*

Acts of terrorism the world has seen conflict with many rules of International Humanitarian Law (abbr. IHL, also known as *ius in bello* or the Law of Armed Conflict), such as the prohibition of torture and abuse, prohibition to attack cultural objects and places of worship, non-distinction of civilians and military objectives, attacking civilians. In and through cyberspace, the acts of terrorism could be even more indiscriminate as the distinction between civilian and military objectives is less clear-cut. In the Nuclear Advisory Opinion, the ICJ stated that "*the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to al1 forms of warfare and to al1 kinds of weapons, those of the past, those of the present and those of the future*".[187] Thus, all established principles and rules of International Humanitarian Law apply to all forms of lawfare and weapons, including cyber warfare and cyber weapons. This, however, raises more questions for interpretations. For example, according to the fourth Geneva Convention, it is prohibited to attack civilian populations and civilian facilities (such as dams, electric grids, places of worship) - the international community has yet to agree on issues such as what are considered civilian objects in cyberspace that are subject to the same protection or whether cyber operations that disrupt, but do not physically damage systems amount to an attack as defined in IHL.[188]

According to the International Humanitarian Law, attacks that utilize means or methods of warfare not directed against a specific military objective, or the effects of attacks are not limited

[187] International Court of Justice. Legality of the Threat or Use of Nuclear Weapons. Advisory Opinion. ICJ Reports 1996. ICJ 266. 1996, para 86.
[188] H. Durham. Cyber operations during armed conflict: 7 essential law and policy questions. ICRC blogs. Humanitarian law & Policy. 2020. Available at: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/?utm_campaign=DP_FORUM%20Cyber%20operations%20during%20armed%20conflict%3A%207%20essential%20law%20and%20policy%20questions&utm_source=hs_email&utm_medium=email&utm_content=85308521&_hsenc=p2ANqtz-8-XJ_x1tNb-Vspuc2CoVbalosrTb-w3h7ifr-e1wNzMCocsKxsJtggq6uHCfXnhk3hM-EPHnRxHDbh1TPGigkT7MqUVQ&_hsmi=85308521

in a lawful manner, are unlawful.[189] In regards to cyberspace, this means that cyber tools that spread and cause damage indiscriminately are prohibited.[190] Thus, basic rules of IHL apply to cyberspace. These rules are, for example, prohibition to target civilians and civilian objects is forbidden; using indiscriminate weapons and attacks; prohibition of disproportionate attack; attacking medical services.[191]

International Humanitarian Law applies during the international and non-international armed conflict (abbr. IAC and NIAC). IAC applies to conflicts between states, whereas NIAC applies to conflicts between state and non-state actors. There is a broad agreement that conflicts in Syria and Iraq constitute NIAC, thus IHL applies to a non-state actor (ISIS).[192] For NIACs, only Common Article 3 of the (1949) Geneva Conventions and Additional Protocol II are applicable. The Common Article 3 lays down minimum prohibitions, such as not attacking civilians or wounded and sick, and applies to non-state actors directly (regardless of whether the state is a signatory).[193] Article 13 of Additional Protocol II to the Geneva Conventions for non-international armed conflicts, specifically outlaws "*acts or threats of violence the primary purpose of which is to spread terror among the civilian population*".[194] For international armed conflicts Article 51 section 2 of Additional Protocol I is applicable.[195] In order to apply these articles, on the one hand, a state has to be a signatory to the protocol and, on the other hand, the non-state actors have to satisfy the following criteria: (a) they are organized; (2) they are "*under responsible command*"; (3) they "*exercise such control over a part of (the state's) territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol*".[196] Thus, IHL would not apply to just any non-state terrorist but the one that has some state-like characteristics (like control over some territory, organization, command system).

---

[189] See Article 51(4) of Additional Protocol I and rule 11 of ICRC Customary IHL Study. Available at: https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf
[190] H. Durham. 2020.
[191] ICRC. International Humanitarian Law and Cyber Operations during Armed Conflicts. ICRC Position Paper. 2019. Available at: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts
[192] H. Edwards. International law and terrorism: the case of ISIS. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 28.
[193] See the full wording of the Article 3 here: https://ihl-databases.icrc.org/ihl/WebART/375-590006
[194] ICRC. Treaties, States Parties and Commentaries. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977. Article 13: Protection of the civilian population. Available at: https://ihl-databases.icrc.org/ihl/WebART/475-760019?OpenDocument
[195] ICRC. Treaties, State parties, and Commentaries. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 51: Protection of the civilian population. Available at: https://ihl-databases.icrc.org/ihl/WebART/470-750065
[196] H. Edwards. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, pp. 28-29.

IHL prohibits all acts aimed at spreading terror among the civilian population (art. 51, para. 2, Protocol I; and art. 13, para. 2, Protocol II). IHL also proscribes the following acts, which could also be considered as terrorist attacks: attacks on civilians and civilian objects (arts. 51, para. 2, and 52, Protocol I; and art. 13, Protocol II); indiscriminate attacks (art. 51, para. 4, Protocol I); attacks on places of worship (art. 53, Protocol I; and art. 16, Protocol II); attacks on works and installations containing dangerous forces (art. 56, Protocol I; and art. 15, Protocol II); the taking of hostages (art. 75, Protocol I; art. 3 common to the four Conventions; and art. 4, para. 2b, Protocol II); murder of persons not or no longer taking part in hostilities (art. 75, Protocol I; art. 3 common to the four Conventions; and art. 4, para. 2a, Protocol II). [197]

There is a widespread agreement that cyber operations that have comparable effects to classic kinetic operations are governed by IHL applicable in IAC (Tallinn Manual 2.0, rule 82, paragraph 16). For example, the destruction of civilian or military assets, or actions that cause the death or injury of soldiers or civilians is prohibited both through cyber and conventional methods. However, it is uncertain whether cyber operations that do not physically destroy or damage military or civilian infrastructure could be considered an armed force governed by IHL in the absence of kinetic hostilities. Thus, it remains unclear which cyber operations constitute an armed force under IHL.[198]

There are several challenges in applying International Humanitarian Law to cyberterrorism, or terrorism in general. One is that IHL requires precise classification of conflicts. In practice, it is not always easy to make a distinction between IAC and NIAC. Moreover, Sassoli has noted that "*the law of non-international armed conflicts may appear in certain respects inappropriate for a transnational conflict between a state and a global non-state actor, since such law was designed for conflicts occurring within a territory"*.[199] As well, it may be difficult to say when the armed conflict has ceased and IHL is no longer applicable. Another troublesome issue in regards to applying IHL to (cyber) terrorist attacks, is the distinction between civilian and military objectives which in fact lies at the heart of humanitarian law.[200] Specifically in regards to cyberterrorism, it is unclear whether some cyber tools, targets and consequences are permitted or forbidden under IHL. Thus, although International Humanitarian Law does not provide a definition of terrorism, it regulates acts of terrorism. However, it remains unclear how and to what extent acts of cyberterrorism are covered under International Humanitarian Law.

[197] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009, p. 70.
[198] H. Durham. 2020.
[199] M. Sassoli. Transnational armed groups and international humanitarian law. Program on Humanitarian Policy and Conflict Research. Occasional Paper Series. No. 6, February 2006, 22.
[200] H. Edwards. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 35.

2.5. Customary International Law

Customary International Law is a framework of unwritten international law that refers to the rules and principles of international law established by state practice. Customary International Law, being dependent on state practice and changing reality, may adapt more easily to the changes in the global realm.[201] Customary International Law also addresses terrorist acts, for example, in the Galić case, the International Criminal Tribunal for the former Yugoslavia (abbr. ICTY), found "*that terrorization of civilian population, committed during an armed conflict, has crystallized into a war crime under customary international law*".[202] The Special Tribunal for Lebanon, the only tribunal that was created specifically to try terrorist cases, was to established to prosecute those suspected of assassinating former Lebanese Prime Minister Rafik Hariri[203], in fact found that a definition of terrorism exists under customary international law (based on UN Resolutions and the legislative and judicial practice of States).[204] The tribunal also provided an international definition of terrorism. Pursuant to the Appeals Chamber of the Special Tribunal for Lebanon, terrorism has three core elements: (1) the commission of a criminal conduct (like murder or hostage-taking); (2) the intent (*dolus specialis*) to spread fear in the population or influence decision making of national or international authority and the intent (*dolus*) of the underlying crime; (3) the act has a transnational element.[205] This decision has been widely criticized for broadening international law, thus, the existence of terrorism under customary international law remains a debatable matter.[206]

Although the UN treaties and resolutions do not constitute as customary international law, they indicate the state practice and consensus of the international community. Thus, for example, the UN Security Council resolution 1373 indicates prohibition of terrorism under customary international law. Special acts of terrorism, such as genocide or torture, would also be prohibited by the customary international law.[207] Presumably, customary international law is also

---

[201] *Ibid.*

[202] *Ibid.;*
International Criminal Tribunal for the former Yugoslavia (ICTY). Prosecutor v. Stanislav Galić. ICTY Appeals Chamber. Judgement. IT-98-29-A. 2006, para. 91-98. Available at: https://www.icty.org/x/cases/galic/acjug/en/gal-acjud061130.pdf

[203] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009.

[204] I. van den Herik, C. Rose, Y. Radi. n.d. para 2.

[205] M.P. Scharf. How the war against ISIS changed international law. Case Western Reserve Journal of International Law 48. 2016, pp. 1-54. Available at: scholarlycommons.law.case.edu/faculty_publications/1638;
A. Cohen. Prosecuting terrorists at the International Criminal Court: Re-evaluating an unused legal tool to combat terrorism: Michigan State International Law Review 20, no. 2 (2012):250. 2012.

[206] I. van den Herik, C. Rose, Y. Radi. n.d. para 2.

[207] H. Edwards. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, pp. 32-33.

applicable to non-state actors.[208] Although customary international law is susceptible to changing the world, it is also difficult to identify new rules of customary international law.[209]

Emergence of customary international law requires constant, uniform and general settled state practice, and a conviction by states that such practice shall be deemed obligatory (creates legal rights or obligations).[210] However, emergence of customary international law on terrorism and its definition, is unlikely, as global community continues to disagree as states have not been able to agree to adopt a generic treaty on international terrorism.[211]

Some rules of customary international law are less adaptable to changes, these are peremptory norms of international law or *ius cogens* norms. These norms, for example, prohibit genocide, torture, slavery and use of force contrary to the United Nations Charter.[212] The principles of customary international law that have also been codified in treaty law, are intervention, use of force, due diligence, state responsibility and these are principles that could also apply to the acts of cyberterrorism (see above).

2.6. State Responsibility

States have a positive obligation to protect, a responsibility for security, ensuring rights and freedoms of its citizens. One of the threats to those aims is terrorism. Apart from conventional kinetic attacks, government institutions and service providers are threatened by cyberattacks and disinformation campaigns intended to radicalize or shift the political narrative. Digital means and targets could keep terrorists from having to face accountability for their actions. If, for example, an jihadist terrorist would want to target a Western society, it would be beneficial for them to attack one of the weakness points, which could be some (essential) ICT systems the Western society is reliant on. The terrorist might be encouraged to launch such cyberattack with perceived impunity through the geographical and legal disconnect.[213] States may bear responsibility for cyberterrorism if it also has sufficient linkage (*e.g.* if a state directs an act of cyberterrorism) to the act itself.

---

[208] *Ibid.* p. 33.
[209] *Ibid*. p. 36.
[210] ICJ. North Sea Continental Shelf. Federal Republic of Germany/Denmark, Federal Republic of Germany/Netherlands. Judgement. ICJ Reports. 1969, para 77. Available at: https://www.icj-cij.org/public/files/case-related/52/052-19690220-JUD-01-00-EN.pdf;
ICJ. Continental Shelf. Libyan Arab Jamahiriya/Malta. Judgement. ICJ Reports. 1985, para. 27. Available at:
https://www.icj-cij.org/public/files/case-related/68/068-19840321-JUD-01-00-EN.pdf.
[211] R. Värk. 2011, p. 81.
[212] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009, p. 11.
[213] T. Stevens. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 44.

State responsibility (for cyberterrorism) is governed with Draft Articles on the Responsibility of States of Internationally Wrongful Acts (abbr. ARSIWA), a "*modern framework for State responsibility*"[214], which regulate when and how states are held responsible for breaches of an international obligation. These rules also establish in which cases an act of an official or an individual is attributed to the state. Thus, states that do not conduct but sufficiently support (through the concept of agency) terrorist activities may become responsible for the acts of terrorism.[215]

A state bears responsibility, if: (1) an internationally wrongful act has been committed (Article 1 of ARSIWA); (2) the conduct (action or omission) is attributable: (Article 2 of ARSIWA); (3) Conduct constitutes a breach of an international obligation of the State (Article 2 of ARSIWA).[216] Apart from wrongful actions, not fulfilling its due diligence obligation constitutes an internationally wrongful omission by a State.[217] In Bosinan Genocide case the breach of the obligation to prevent genocide constituted the wrongful act.[218] State should also not provide safe haven for cyberterrorists as the United Nations Security Council has insisted that states must "*deny safe haven to those who finance, plan, support, or commit terrorist acts*".[219] For the elaboration on due diligence obligations, see para. 2.3.

State involvement could constitute direction or control of an attack, support (*i.e.* financing, providing equipment, training, transportation), toleration or inaction, however, not any connection with terrorism involves responsibility.[220] According to the UN GGE 2013 report, *"States must meet their international obligations regarding internationally wrongful acts attributable to them".*[221] According to the UN GGE 2015 report *"States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise*

[214] J. Crawford. State Responsibility: The General Part. Cambridge Studies in international and comparative law. Cambridge University Press. 2013, p. 45.
[215] V. Ekstedt, T. Parkhouse, D. Clemente. National Cyber Security: Framework Manual. 2012, pp.153, 156.
[216] United Nations. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. 2008, p. 35. Available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
[217] M. Bergwick. Due Diligence in Cyberspace. An assessment of rule 6 in the Tallinn Manual 2.0. Uppsala Universitet. 2020, p. 23. Available at: https://www.diva-portal.org/smash/get/diva2:1417207/FULLTEXT01.pdf
[218] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, para 462. Available at: https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf
[219] United Nations Security Council. Resolution 1373. 2001, para. 2.
[220] *Ibid*. pp. 82-85.
[221] UN GGE. 2013, para 23.

originates from a State's territory or from its ICT infrastructure may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated".[222]

State involvement could also be more direct as a state may prefer (to take advantage of international legal loopholes, minimize the responsibility) to choose conduct an act of cyberterrorism instead of conducting a conventional armed attack.[223] To identify sufficient control or direction, an overall or effective control test shall be used.[224] The former requires a state to be involved in the planning, direction, support and execution of the terrorist act.[225] The latter requires a state to have an overall control over a terrorist action, thus the state does not have to issue specific orders or instructions to every specific act of terrorism.[226]

According to Article 11 of ARSIWA, the state could be responsible for the act of cyberterrorism, if it acknowledges and adopts the act as its own.

It is important to identify state involvement (one of the abovementioned) to justify the use of self-defence. According to Article 8 of ARSIWA, using self-defence (according to Article 39 of the UN Charter) in case of an attack (or a threat of such), there has to be an imminent threat from a state. That means that the act of cyberterrorism has to be linked to some state which is a difficult task for law enforcement.[227]

In the case of Stuxnet, a cyber operation against Iranian nuclear technologies (critical infrastructure), it is apparent that these kinds of cyber weapons are so sophisticated and linked to state actors and their proxies.[228] In this case, if a sufficient linkage has been identified between the state and the act of terrorism, state responsibility could be raised.

2.7. International Human Rights Law

Human rights obligations form an integral part of the international legal counter-terrorism framework, both through the obligation imposed on States to prevent terrorist attacks, which have the potential to significantly undermine human rights, and through the obligation to ensure

[222] UN GGE. 2015, para 28 f.
[223] R. Värk. 2011, p. 82.
[224] Ibid. pp. 87-89.
[225] Military and Paramilitary Activities in und against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, para. 115. Available at: https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf
[226] ICTY. Prosecutor v. Duško Tadić. Case No IT-94-1-A. Judgement of the Appeals Chamber. 15 July 1999, paras. 117, 122, 131, 132, 145. Available at: https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf
[227] B. Ahlhaus. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 15.
[228] T. Stevens. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 45.

that all counter-terrorism measures respect human rights. On the other hand International Human Rights Law (abbr. IHRL) could also be applied to the acts of terrorism, which have devastating effects on the enjoyment of individual human rights. However, according to ECHR, the acts of terrorism can only go against states as states have obligations to protect civilians against terrorists, compensate for terror acts, shall not engage in terror acts. The applicability of IHRL to non-state actors, is a debatable issue, as traditionally, it has been regulating the relationship between the state and individuals.[229] The UN Office on Drugs and Crime (abbr. UNODC), in the 2009 report, rejected the applicability of IHRL to terrorist, stating that "*international human rights instruments govern the responsibilities of States with regard to the individual, not the criminal responsibility of terrorist individuals and organizations*".[230] Bellal, a legal advisor at the humanitarian organization Geneva Call, on the contrary, suggests that IHRL applies to armed groups that have achieved *de facto* authority with state-like functions.[231] It is also debated whether IHRL is also applicable during armed conflict, whether IHRL complements IHL during armed conflicts or the applicability of IHL excludes the applicability of IHRL.[232] In case IHRL is applicable to non-state actors, IHRL would impose several legal obligations on terrorists.[233] This would mean enhancing terrorist organizations to state-like organizations, but would also provide greater means to hold terrorists accountable for the violations of human rights.[234]

States can be held responsible for violations of their international human rights obligations which include a duty to protect people from acts of terrorism (*e.g.* inadequate criminal legislation to govern the terrorism or failure to act to prevent the activities of terrorism). States, thus, have a positive obligation to, *inter alia*, establish an effective criminal justice system within the rule of law to combat impunity for terrorists.[235] States may also face responsibility for the acts of terrorism if it has some linkage to the acts[236]

As mentioned above, IHRL also prescribes that counter-terrorism measures respect human rights. This however raises many debates (see, for example, burqa and other face coverings

[229] H. Edwards. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 30.
[230] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009, p. 91.
[231] A. Bellal. Beyond the pale?; A. Bellal. Interview regarding international law and ISIS; interview by H. Edwards. Geneva. 2016.
[232] H. Edwards. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 31.
[233] *Ibid.*
[234] *Ibid*.
[235] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009, p. 92.
[236] *Ibid.* p. 91.

bans, such as in Switzerland[237], Sri Lanka[238], Case S.A.S v. France Judgment[239]), such as private versus collective rights, freedom of expression, freedom of thought, religion, conscience, association, discrimination, right to privacy versus right (and state's obligation) to security, debates on content regulations.[240] Fighting against terrorism, developing laws criminalizing the incitement of acts of terrorism and regulating cyberspace, whilst protecting human rights (such as the rights to freedom of expression and association, or religion) is a challenge for policymakers, legislators, law enforcement agencies and prosecutors.

2.8. International Criminal Law

2.8.1. Crimes applicable to terrorism

In 1937 the League of Nations adopted Convention that would establish International Criminal Court to try terrorist offences according to the 1937 Terrorism Convention, however this never came to force.[241] The successor of the League of Nations, the United Nations took a broader approach to establish a permanent international criminal court.[242] Subsequently, international terrorism was left out from the Statute of International Criminal Court. Establishment of the International Criminal Court (abbr. ICC) is the latest and the greatest development in the field of international criminal law, yet it has not been used for the purpose of trying cases of terrorism. The 1998 Rome Statute of the International Criminal Court, outlaws the most serious crimes, such as genocide, crimes against humanity, war crimes and crimes of aggression, yet it does not include terrorism, as a distinct, *sui generis* offence, within its jurisdiction.[243] However, the ICC may try cases of terrorism if they amount to war crimes, crimes against humanity, genocide, *i.e.* crimes the Court has jurisdiction over.[244] The International Law Commission (the UN agency responsible for codification of international law) itself has stated in the Draft Statute for an International Criminal Court that some acts of terrorism could qualify a crimes against humanity and genocide: "*A systematic campaign of terror committed by some groups against the civilian population would fall within the category of crimes under general international law*

[237] BBC News. Switzerland referendum: Voters support ban on face coverings in public. 2021. Available at:
https://www.bbc.com/news/world-europe-56314173
[238] BBC News. Sri Lanka to ban burka and other face coverings. 2021. Available at:
https://www.bbc.com/news/world-asia-56386426
[239] European Court of Human Rights. Case S.A.S v. France. Judgment. Grand Chamber. Strasbourg. 2014.
[240] *Ibid.*;
The use of the Internet for terrorist purposes. 2012.
[241] A. Cassese, P. Gaeta, J. R. W. D Jones. 2002, pp. 5, 9.
[242] *Ibid.* p. 9.
[243] H. Edwards. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 29.
[244] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009, p. 40.

in subparagraph (d), and if motivated on ethnic or racial grounds, also subparagraph (a)".[245] In the context of armed conflict, some acts of terrorism, could also be qualified as war crimes. Terrorism may fall under the category of war crime as unlawful attacks against civilians with the additional specific intent of spreading terror among the civilian population.

In cases before the ICTY (Galić and Milošević cases) and SCSL (Brima and Charles Taylor cases), terrorism has been considered a war crime, *i.e.* unlawful attacks against civilian population with the additional specific intent of spreading terror among civilians.[246] In Galić case, an international tribunal for the first time convicted an accused for the crime of "*acts or threats of violence the primary purpose of which is to spread terror among the civilian population*".[247] War crimes are serious violations of the laws applicable during (international or non-international) armed conflict that evoke individual criminal responsibility. [248] War crimes (and grave breaches of IHL) are governed under treaty-based and customary IHL, whereas terrorism is regulated by reference to a number of complex, sectoral, offence-based instruments (see above).[249] In order for an act of cyberterrorism to fall under category of war crimes, it has to take place in the context of armed conflict.

Specific acts of terrorism may also fall under category of crimes against humanity.*[250]* In Galić case, the accused was also found guilty of crimes against humanity.*[251]* Crimes against humanity constitute a serious attack on human dignity, grave humiliation or a degradation of people.[252] Crimes against humanity require an act of terrorism to be widespread or systematic attack against civilians, irrespective of time of war or peacetime.*[253]* These crimes include, for example, murder, torture or other inhumane acts (for example enslavement, rape, sexual slavery, or persecution against any identifiable group or collectivity on political, racial, national, ethnic, cultural, religious, gender).*[254]* Thus, for the act of terrorism to fall under category of crimes

[245] United Nations. Draft Statute for an International Criminal Court with commentaries. Report of the International Law Commission on the work of its forty-sixth session. 1994. Available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/7_4_1994.pdf
[246] A. Cassese, G. Acquaviva, M. Fan, A. Whiting. 2011, p. 286.
[247] *Ibid*.
[248] Geneva Call. Introduction to the Law of Armed Conflict (LOAC). 2013. Available at: http://www.genevacall.org/wp-content/uploads/dlm_uploads/2013/11/The-Law-of-Armed-Conflict.pdf
[249] Council of Europe. Committe of Experts on Terrorism (CODEXTER). Application of International Humanitarian Law and Criminal Law to Terrorism Cases in Connection with Armed Conflicts. Discussion Paper. 2017. Available at: https://rm.coe.int/16807025f9
[250] A. Cassese, G. Acquaviva, M. Fan, A. Whiting. 2011, p. 286.
[251] *Ibid.*
[252] Introduction to the Law of Armed Conflict (LOAC). 2013.
[253] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009, p. 42.
[254] *Ibid.*

against humanity it has to be sufficiently widespread or systematic conduct of violence listed under Article 7 of the Rome Statute.[255]

Cohen states that "*crimes against humanity are arguably the most suitable format to prosecute terrorist acts although they also require* [...] *a widespread or systematic attack and, thus, raise the threshold for the more common isolated terrorist acts*".[256]

Acts of terrorism could also fall under category of genocide when the terrorist acts has the *"intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such"* and a crime listed in the sections (a), (b), (c), (d) and (e) of the Article 6 of the Rome Statute has been conducted.[257]

International Criminal Law is applicable during armed conflicts and during peacetime.[258] Although in certain circumstances, acts of (cyber)terrorism could be tried as crimes under the Rome Statute, there is no international criminal jurisdiction of (cyber) terrorism.[259] "*Hence, under the current ICC list of crimes, the effects of terrorism can be prosecuted, but not the act of terror itself*".[260] Whether an act of terrorism constitutes a crime under the ICC statute depends on the criteria of these crimes lists, relevant aspects to consider are number of people affected (killed, injured, kidnapped), location of attacks, type of attack (armed assault, hijacking, the scale on an attack including gravity, character, lethality, spread, rapidly, duration, persistence of attack, geographic scope, *etc*. There has been unsuccessful attempts (in 1998 and 2010) to include terrorism as a separate distinct crime under the ICC Statute.[261] Although there is a gap in the legal framework to try terrorist cases, current existing legal framework is still used by the ICC to investigate, prosecute and try alleged offenders designated as terrorist.[262]

---

[255] *Ibid.*
[256] A. Cohen. Prosecuting terrorists at the International Criminal Court: Re-evaluating an unused legal tool to combat terrorism: Michigan State International Law Review 20, no. 2 (2012):250. 2012;
See also International Criminal Court (ICC). Understanding the International Criminal Court. The Hague: ICC. 2013. Available at:
https://www.icc-cpi.int/iccdocs/PIDS/publications/UICCEng.pdf
[257] Frequently Asked Questions on International Law Aspects of Countering Terrorism. 2009, p. 43.
[258] H. Edwards. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 39.
[259] R. Cryer, H. Friman, D. Robinson, E. Wilmshurst. An Introduction to International Criminal Law and Procedure. Other Crimes. Transnational Crimes, Terrorism and Torture. 2. ed. Cambr. 2010.
[260] I. van den Herik, C. Rose, Y. Radi. Towards an international terrorism tribunal? Universiteit Leiden. video tuition course. n.d. para 2. Available at:
https://www.coursera.org/lecture/international-law-in-action/towards-an-international-terrorism-tribunal-wNQY1
[261] *Ibid.*
[262] *Ibid.*

2.8.2. Individual responsibility

The International Criminal Court (abbr. ICC) may only prosecute individuals (not organisations or states), according to the principle of complementarity, the ICC may only prosecute if the state is unable or unwilling to genuinely investigate and prosecute its nationals. In order to prosecute nationals of a state, the state has to have ratified the Rome Statute or the UN Security Council has to give the jurisdiction to try the case to the ICC. Alternatively, international criminal law could also be applied at the national level by states.[263]

States may also prosecute individuals based on extraterritorial jurisdiction or universal jurisdiction.[264] The ICRC explains "*under the principle of universal jurisdiction, war crimes suspects may be criminally prosecuted not only by the state in which the crime occurred, but by all states".*[265] In regards to fighting terrorism, this expanded jurisdiction under international law is controversial and may undermine international law. For example, the US does not recognize the ICC's jurisdiction over its own nationals but can exercise jurisdiction over foreign individuals who have committed offences outside the US. Such selective approaches to international jurisdiction over terrorist may undermine international law.[266]

In practice, bringing terrorists to justice remains troublesome. In addition to difficulties in collecting admissible evidence and taking terrorists into custody, there are also some legal issues such as too vague international extradition regulations.[267] As explained above, terrorist cases could be tried in the ICC if all the elements of listed crimes are met. For example, in 2016, the ICC sentenced Ahmad al-Faqi al-Mahdi – an Islamic militant who destroyed ancient shrines in Timbuktu, and who was a member of Ansar Dine, an al-Qaeda-linked group that controlled northern Mali in 2012– to nine years in jail for war crimes against cultural property. [268]

2.9. Responsibility of private entities

As so-called Information Society seems to be in the constant change whilst the legal systems seem to be lacking behind, accepting a more multi-level, multi-stakeholder approach to security, governance and delegating some jurisdiction to global ICT-experts and industry (such

[263] H. Edwards. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 30.
[264] *Ibid.* p. 36.
[265] ICRC. International humanitarian law and terrorism: Questions and answers: What does IHL say about terrorism? 2011. Available at: https://www.icrc.org/data/rx/en/resources/documents/faq/terrorism-faq-050504.htm
[266] H. Edwards. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p. 36.
[267] *Ibid.* p. 35.
[268] M. Vlasic, H. Turku. Our cultural heritage is under attack. We must all join the fight to protect it. World Economic Forum (WEF). 2016. Available at: https://www.weforum.org/agenda/2016/10/our-cultural-heritage-is-under-attack-we-must-all-join-the-fight-to-protect-it/

as ISO, IEC, ITU) to put down general security standards and guidelines, is perhaps a modern way forward. Delegating responsibilities or increasing engagement with the industry and relevant stakeholders in the matters of Internet governance and cyber security could enhance the efforts of fighting international cyber crimes (against or with the use of ICTs). Private sector sector plays a crucial role in national cyber security matters, as it conducts research, designs, develops and manufactures the vast majority of software and hardware used in ICTs, provides online products and services, maintains most of the network infrastructure and often owns the critical infrastructure - all of which can be targeted or used to conduct cyberattacks.[269] Private sector plans and manages resources, provides reliable connectivity, and ensures delivery for traffic and services.[270] In terms of national cyber security, non-state and international actors are as involved as government entities.[271] As the private service providers are playing increasingly greater roles in Internet governance and security matters, it raises questions like if and what kind of responsibilities are they bearing.

One approach could be that, as private companies are already governing important matters to the peace and security, democracy, *etc*, governments could actively delegate some responsibilities to these service providers. Governments or international organisations could lay responsibilities for service providers to, for example, secure public spaces by setting minimum obligations for operators of public places to ensure the security of shopping malls, transport services, places of worship, *etc*. The authorities could also delegate the responsibility to monitor and take down propaganda or other terrorist content. In that sense internet service providers would be acting similarly to law enforcement.[272]

Depending on the national approach, service providers might play an essential role in regulating content and users of their services. In the article "*Terrorism and the Internet: should web sites that promote terrorism be shut down?*", Barbara Mantel notes that "*most Internet service providers, web hosting companies, file-sharing sites and social networking sites have terms-of-service agreements that prohibit certain content*". For example, she notes that Yahoo's Small Business Web hosting service specifically forbids users from utilizing the service to provide material support or resources to any organization(s) designated by the United States Government as a foreign terrorist organization. To that extent, there is an element of self-regulation within the information society. Self-regulation by these private sector stakeholders may also support countering terrorist communication, incitement, radicalization and training

[269] Gen. ed. A. Klimburg et al. National Cyber Security: Framework Manual. Tallinn. 2012, pp. 37, 96.
[270] *Ibid*, p. 37.
[271] A. Klimburg, J. Healey. National Cyber Security: Framework Manual. Tallinn. 2012, p. 67.
[272] The use of the Internet for terrorist purposes. 2012.

activities conducted on these platforms. In addition, the service providers play a role in timely identification of Internet activity that may promote acts of terrorism.[273]

However, a regulatory "techlash", the monopolization and applying a more authoritarian approach in cyberspace with governments making service providers responsible and imposing fines on them when not providing sufficient security and possibly breaking them up, could contribute to digital inequality as it would be very difficult for smaller companies to operate.[274]

E. Macron has in regards to the increased role of private entities in Internet governance, pointed out that the world has given sovereignty to (telecom) companies.[275] A lot of control over critical digital infrastructure has shifted to the private sector and some governments are now aware and alarmed this as this becomes especially problematic if the industry does not deliver what governments want in terms of security. Therefore, policymakers should put down requirements to follow and standardization (including international standardization) should be revalued as a matter of strategic autonomy. To reflect the reality and for the laws, rules and standards to be up-to-date and relevant, governments should to that end, cooperate with companies and technology experts, and private companies, on the other hand, should cooperate with governments to address their concerns.[276] However, some governments have taken a more dominant approach in regards to Internet Governance. For matters of international concern and that have significant differences in approaches between governments, a greater harmonization and common understanding should be pursued. This includes content control and regulation in terms of terrorism as regulating terrorism-related content on the Internet is highly contentious. Some states apply strict regulatory controls on the Internet and other related service providers (including using technologies to filter or block access to some content) while other states have adopted a softer regulatory approach, relying to a greater extent on self-regulation by the information sector.[277]

Another solution could be strengthening the role of the international community in the areas of Internet governance. While the level of government regulation of the Internet varies greatly

---

[273] *Ibid.*

[274] World Economic Forum. The Global Risks Report 2021. 2021. Available at: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf#page=29&zoom=100,58,569

[275] The Economist. "On the edge of a precipice": Macron's stark warning to Europe. 9. November 2019. Available at: https://www.economist.com/weeklyedition/2019-11-09

[276] Strategic Autonomy and Cybersecurity in the Netherlands. Cyber Security Council. 2021. Available at: https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands

[277] The use of the Internet for terrorist purposes. 2012, p. 50.

around the world, in the absence of a global authority responsible for Internet regulation, private stakeholders continue to dominate a domain that has become essential to all states and by controlling the availability of terrorism-related content disseminated via the Internet.[278]

Policies and governance play a vital role in mitigating risks and speeding response to cyber incidents, however, governance is not always present in information security. The matters of cyberterrorism are not limited by national boundaries. In considering effective actions to fight against international cyberterrorism, there is a need for concerted and consistent international legislation.[279] This means increased cooperation between academia, ICT companies, state and nonstate actors, to, *inter alia*, ensure compliance of nonstate actors in situations of national danger, the resilience of the private sector to ensure continuity of its operations.[280]

Although, unlike combat in air or at sea, the internet as a domain of conflict is controlled overwhelmingly by the private sector, as to this day, the responsibility for countering the use of the cyber means for terrorist purposes ultimately lies with member states. To capture threats like cyberterrorism that operate in an immersively multi-stakeholder environment, a holistic comprehensive approach is needed to effectively fight against such threats. Some international efforts have been made to formalize information sharing and cooperation with private entities (*e.g.* NIS Directive, EU Directive 2006/24/EC).

[278] *Ibid.* p. 123.
[279] L. MacKinnon, D. Gan, L. Bacon, G. Loukas. D. Chadwick, D. Frangiskatos. Strategic Intelligence Management. 2013.
[280] A. Klimburg, J. Healey. National Cyber Security Framework Manual. 2012, p. 97.

3. CHAPTER 3: WAYS FORWARD

As it was shown in the previous chapters, international law encompasses many acts of terrorism by different instruments, yet it remains ill-equipped to ensure responsibility for the acts of terrorism, or, furthermore, acts of cyberterrorism. There is no explicit *delictum juris gentium* of cyberterrorism. The fragmentation of law and issues with applying international law to the acts of cyberterrorism (due to shortcomings with legal definitions, jurisdictional scope and procedures for prosecution[281]), undermines its potential benefits and effectiveness of ensuring responsibility for such horrors. In fact, terrorists have taken advantage of legal gaps and the lack of international cooperation.[282] Thus, international law must be improved to address modern global threats and provide a legal framework to effectively bring contemporary terrorists to justice. This Chapter purposes some ways forward to ensure responsibility of acts of cyberterrorism.

Greater and clearer understandings of international law in the context of cyberterrorism

Although the international community has been unable or unwilling to agree on the global definition of terrorism, greater clarity could be brought to, in addition to the acts of terrorism, outlaw acts of cyberterrorism. Even if the world is yet unwilling to agree on a legal comprehensive global definition of cyberterrorism, much can be done to prepare and fight against cyberterrorism. As well, efforts could be made to create greater common understandings and interpretations of international law in regards to cyberspace and crimes committed against and through the use of ICTs. International community could interpret the international principles, laws and norms further to ensure resilience, stability and accountability, and enhance fight against modern terrorism. Global and regional efforts to harmonize laws of terrorism are important to overcome legal scatteredness and gaps in the regulations on cyberterrorism. In order to bring wrongdoers to justice, the international community needs a political and legal clarification for the possible acts of cyberterrorism, prohibit certain cyber operations (including terrorist acts in cyberspace), propose possible countermeasures (such as punishment or reprisal attack to the cyberterrorism) and responses (diplomatic response, coordinating attribution, judiciary), but also clarify the interpretation of cyber attack and armed response to it, what constitutes a legal target in cyberspace, but also on matters like content regulations.[283] Significant progress that has been made by the UN GGE, OEWG, or Tallinn Manual processes are essential in seeking to elaborate on the applicability of international law on cyberspace and

[281] T. Stevens. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, p 39
[282] R. Värk. 2011, p. 75.
[283] M. E. Hathaway, A. Klimburg. National Cyber Security: Framework Manual. 2012, p. 19.

on cyberterrorism, and subsequently, to overcome the existing legal loopholes and uncertainty and to fight against impunity. Nevertheless the important steps that have been taken, the international legal framework should still be further elaborated on.

International counter-terrorism convention

For the legal framework to be more efficient, the international community could build up from the scattered sectoral instruments an international counter-terrorism convention that would, *inter alia*, elaborate the acts of terrorism further in the context of the fifth, global domain (*i.e.* cyber domain). A crucial milestone would also be when the global community would adopt the Comprehensive Convention on International Terrorism (abbr. CCIT). The draft convention would be a pragmatic solution to enhance the international fight against terrorism. It, *inter alia*, includes causing serious damage to telecommunications and information networks as a terrorist offence. However, the convention does not specifically elaborate on cyberterrorism and thus would have to be still further interpreted. Nevertheless, the acts of cyberterrorism would fall under the scope of the draft convention.[284]

As terrorism can be disrespectful of national boundaries, in case of cyberterrorism national boundaries play even lesser role. Thus, international cyberterrorism is a global threat affecting all countries and people and therefore needs a global comprehensive approach. International terrorism convention could provide an effective framework to fight against this global threat. The international community could also establish a new court, an International Counter-Terrorism Court to enhance evidence sharing, cooperation and global efforts to ensure accountability for these international crimes. The international court, operating based on an international convention of terrorism, could therefore overcome the paradox that one person's terrorist is another person's freedom fighter and ensure accountability for the grave and global crimes.[285]

The author is in the opinion that the creation of an international court and convention on terrorism, that should address modern threats posed by cyberspace, would, indeed, improve the fight against terrorism and impunity. However, since the international community still faces some obstacles in, for example, reaching consensus on pragmatic workable comprehensive definition on cyberspace, this is unlikely to happen any time soon.

New laws regulating cyberspace

[284] United Nations General Assembly. Draft comprehensive convention on international terrorism : working document. A/C.6/55/1. 2000. Available at: https://digitallibrary.un.org/record/422477

[285] T. Stevens. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019, pp. 37-38.

David T. Borgeois described the current situation of the rapid development of technologies as a "Wild West"-type of atmosphere caused by the fact that the policymakers haven't kept up with the new reality with appropriate laws.[286] In addition to applying existing international law to cybersecurity issues, the international community could propose new rules, laws and principles to fill the gaps that international law is yet lacking. This could be done by adopting a convention (see the previous paragraph) but also by adopting revised NIS, updated Budapest Convention[287], or revised EU's Cybersecurity Act[288], *etc.* that reflects the modern reality better and strengthens international commitments in the fight against (cyber)terrorism. That means that both sectoral and regional legal instruments that regulate terrorism, should also be reviewed in regards to cyberspace. In the absence of so-called hard-law, non-binding, guidance providing instruments such as Tallinn Manuals (including revised Tallinn Manual 3.0) play an important role in interpreting existing legal framework in a way that reflects modern reality and threats. In addition to new laws, measures and guidance, existing frameworks should also be further implemented, strengthened and promoted.

To ensure accountability of terrorism, national legal frameworks should, *inter alia*, criminalize unlawful acts carried out by terrorists over the Internet or related services, regulate Internet-related services (*e.g.* ISPs) and content, provide investigative powers for law enforcement agencies engaged in terrorism-related investigations, develop specialized judicial or evidential procedures and facilitate international cooperation, whilst maintaining standards of international human rights.[289] The legislative framework should cover general cybercrime legislation (including solicitation and criminal association that might be related to terrorism cases), general counter-terrorism legislation and internet-specific counter-terrorism legislation.[290]

Modernization of international law

The fight against terrorism must adapt to the new era, the so-called Information Society. In order to ensure accountability for acts of cyberterrorism, governments and law enforcement must understand the differences between physical terrorism and cyberterrorism and not

[286] D. T. Borgeois. Information Systems for Business and Beyond. The Saylor Academy. 2014.
[287] Convention on Cybercrime. 2001. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[288] The European Parliament and the Council of the European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). 2019. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj
[289] The use of the Internet for terrorist purposes. 2012
[290] *Ibid.*

undermine the latter. Governments must identify threats to their national security that will be enshrined in their national security strategies and counter-cyberterrorism plans.[291]

To address cyberterrorism, a multilateral response that respects international law and the Charter of the United Nations and is responsive to the realities of contemporary issues and a globalized world, is required. In order to respond to contemporary threats, a principled, inclusive, comprehensive and forward-looking (as provided by the United Nations Global Counter-Terrorism Strategy) strategy is needed. International cooperation can support the states with their responsibility responses to prevent and counter terrorism. [292]

As well, in terms of international criminal law, modernization if the Rome Statute could be sought to hold cyberterrorists accountable. Including terrorism as a distinct crime would enhance specifically the prosecution of terrorists. In addition, interpreting the existing Rome Statute and enhancing the ICC processes in a way that reflects the modern threat landscape, *i.e.* including cyberattacks and -threats, could also improve ensuring responsibility for the acts of cyberterrorism.

Enhancing cyber resilience against cyberterrorism

Improving cyber resilience in general contributes to the fight against cyberterrorism and the impunity of such. Terrorism is a phenomenon that seeks to divide, to fight against it we need to invest in deradicalization processes and unity through social cohesion and inclusion, education, multi-stakeholder cooperation, regional and international coordination and information sharing. In the context of cyber, there is a need for state institutions and private enterprises to increase their cyber resilience. The NATO Member States have in 2010, recognised malicious cyber operations "*can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability*".[293]

The most frequent targets of cyber operations are digital services and finance sector, but also public sector and manufacturing. However, cyber readiness and awareness among businesses and individuals are low.[294] As Specops Software cybersecurity expert Darren James said *"No*

[291] J.-T. Kim, T. Hyun. 2007.
[292] UNGA. Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy. A/75/729. 2021. Available at: https://undocs.org/A/75/729
[293] Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, adopted by Heads of State and Government at the NATO in Lisbon 19-20 November 2010, para. 12. Available at: http://www.nato.int/strategic-concept/pdf/ Strat_Concept_web_en_pdf.
[294] Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade. 2020. Available at: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

one can rest on their laurels when it comes to cybersecurity"[295], all companies are suggested to continually improve their cybersecurity strategy and modernize their systems in accordance with the changing threat landscape. Alongside, governments should adopt necessary cybersecurity standards and requirements in compliance with international guidelines and obligations. Non-state actors and cybercriminals are increasingly sophisticated in their methods, thus service providers and policy, law and decision makers should as well constantly enhance their cyber readiness, keep their cyber hygiene high and invest in cybersecurity to also address the cyber threats imposed by non-state actors. Protection of core infrastructure and essential services is utmost important, to this end revised NIS directive[296] could provide guidance. Capacity- and confidence building measures to tackle cyberthreats and the threat of terrorism should be kept up to date on private, national, regional and international level to effectively prevent, deter and respond to cyberterrorism. Law enforcement that fights against terrorism, might now in regards to cyber crimes also need a special type of investigative powers and cyber capacity specialized investigative techniques for law enforcement and prosecutors.

In addition, in terms of a global multistakeholder domain (cyberspace) and international crime (international terrorism), international multilevel (between governments, private entities, milCERTS, civCERTS, etc.) cooperation, information sharing (including in evidence collecting and prosecuting terrorists) is crucial. Thus, the international community should also formalize the information sharing between governments and private stakeholders.[297]

To that end, common understanding on the issues of cyberterrorism should be pursued. International action and policy dialogue in the field of cybersecurity has been sought through the international organisations such as the Council of Europe, the Organisation for Economic Co-operation and Development (OECD), the Organization for Security and Co-operation in Europe (OSCE), the North Atlantic Treaty Organization (NATO) and the United Nations (UN).[298]

Through the new Programme of Action for Advancing Responsible State Behaviour in Cyberspace, many of such legal and policy means are addressed. The Programme of Actions aims to enhance capacity building, develop confidence-building measures, improve

[295] N. Forrester. New report reveals countries most targeted by 'significant' cyberattacks. EU Security Brief. 2020. Available at: https://securitybrief.eu/story/new-report-reveals-countries-mosttargeted-by-significant-cyber-attacks
[296] European Commission. NIS directive. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis-directive
[297] The use of the Internet for terrorist purposes. 2012.
[298] EU Cybersecurity Initiatives. European Commission. 2017. Available at: https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

coordination among the relevant stakeholders, advancing norms of responsible behaviour and understanding how international law specifically applies to cyberspace.[299]

Thus, harmonized, clear and strengthened approach towards (cyber)terrorism, continuous efforts in the fight against terrorism and addressing new threats imposed by ICTs, are needed to hold modern terrorist accountable for their actions. However, there are significant challenges in tackling and regulating cyberterrorism - apart from technical attribution and evidential challenges, there are significant dissenting opinions and approaches to terrorism and cyber operations, including matters related to dual criminality, sharing intelligence based sensitive information[300], regulating content and the scope of applying international law to cyberspace.

[299] United Nations Office of Disarmament Affairs (UNODA). OEWG. Joint Contribution – Programme of Action. The future of discussions on ICTs and cyberspace at the UN last updated on the 2nd of December 2020. Available at: https://front.un-arm.org/wp-content/uploads/2020/12/joint-contribution-PoA-future-of-cyber-discussions-at-the-un-2-2-2020.pdf

[300] The use of the Internet for terrorist purposes. 2012.

CONCLUSION

Today's world is more interconnected than ever, mostly because of the widespread use of ICTs. We are highly dependent on something that has only come into existence within the last century. It has been a fast race somewhere unknown and unpredictable, and people have struggled to adapt their conventional laws, systems and thinking which subsequently has created some gaps and vulnerabilities in our systems. Perhaps even, the new technologies and spread of them have also changed our attitudes, values and ethics - something that changes our ways of interpreting conventional rules. New technologies, whether it is inventing aeroplane or gunpowder, or digital technologies, present both new opportunities and challenges.[301] Information and communication technologies can be used by criminals and terrorists to pursue their malicious intents, be it social, political or other aims. Global character and interconnectivity of cyberspace create a new vulnerability in regard to terrorist threat. It is true that terrorist attacks still mainly occur in the physical domain rather than in the cyber domain or against ICT targets and ICTs have rather a supporting role in terrorist activities (*e.g.* providing encrypted communication means). Thus, cyberterrorism remains to be a possibility than a proven reality.[302] Nevertheless, the threats of cyberterrorism persist real and serious.

Threats posed in cyberspace are of concern to all countries, thus strong commitments to international law are evermore important to strengthen the stability and to overcome so called Wild West what ICTs brought to the digital society. This thesis focused on the ways of holding cyberterrorists responsible and on the applicability of current international law on cyberterrorism. In order to do that, the definition of cyberterrorism was explored. Notably, there is no universal generic definition of terrorism nor cyberterrorism. In analysing applicable legal frameworks that are relevant in regards to cyberterrorism, several challenges to this end were identified. There were uncertainties identified in applying related norms of international law - sovereignty, use of force, non-intervention, due diligence, but also applying International Humanitarian law, Customary International Law, and International Criminal Law in regard to the acts of cyberterrorism, as well debates on human rights in regards to cyberterrorism were addressed. The nations of the world still have very different approaches to these matters. Opinions still dissent on what is meant by terrorism and the clash is increased in relation to the new domain and questions around how to regulate it. Thus, nevertheless the common will of countries to bring wrongdoers to justice, it is not a simple task. International law and ensuring responsibility for the acts of cyberterrorism is therefore bound by the political positions and

[301] Bert Koenders. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Gen. ed. M. N. Schmitt. 2017, XXV.
[302] T. Stevens. Handbook of Terrorism and Counter Terrorism Post 9/11. 2019.

inclinations. This is also due to the persisting challenges to define terrorism in general – thus, the legal framework on international terrorism works rather on a regional or sector-specific level. Global and regional efforts to overcome this obstacle were addressed. As well, possible remedies to overcome legal loopholes and ways to strengthen the framework of holding cyberterrorists responsible, were proposed.

Therefore, this thesis found that international law is, in fact, ill-equipped to ensure responsibility for cyberterrorism. International law should be further interpreted in regards to cyberterrorism. An international comprehensive convention on terrorism that reflects the modern threat landscape and means, would enhance the fight against terrorism and impunity. As the legal gaps were identified, the thesis also proposed ways forward in regard to strengthening responsibility.

Whether international law is such a call in the desert to provide clarity on the concept of cyberterrorism or the stability in cyberspace should be pursued through some other channels, remains in question as the views of various states differ drastically. However, international law is one of the channels in the holistic fight against (cyber)terrorism.

Therefore, the value of this thesis to the jurisprudence lies in the elaboration on the conventional norms of international law in regard to cyberterrorism and the proposed remedies to strengthen the responsibility for cyberterrorism.

As this thesis focuses on a more general and holistic approach to international law, covering all branches of international law, more specific research on the topic could be done with a more detailed focus on one branch - for example, on the topic of responsibility for cyberterrorism under international criminal law. As well, the definition of cyberterrorism but also legitimate weapons, targets, tools of cyberspace (under international humanitarian law) could be further researched. The topic of cyberterrorism and responsibility for the acts of cyberterrorism could also be opened up in a regional context. Legal loopholes and uncertainty could be overcome with academic research but also seeking the common understanding of the international community to tackle this international, real and significant threat.

Vastutus küberterrorismi eest rahvusvahelises õiguses

RESÜMEE

Nii terrorism kui ka küberrünnakud kujutavad endast olulist ohtu riiklikule ning rahvusvahelisele rahule, stabiilsusele ja julgeolekule. Info- ja kommunikatsioonitehnoloogiate levik on lisaks võimalustele loonud ka väljakutseid rahvusvahelisele kogukonnale, riikidele, organisatsioonidele ja indiviididele, sealhulgas õigusloojatele ja õiguskaitseasutustele. Samuti valmistab siiani väljakutseid rahvusvahelise terrorismi uurimine, menetlemine, (universaalne) defineerimine ja toimepanijate vastutusele võtmine. Rahvusvahelisel kogukonnal lasub uus väljakutse tagada, et ka uue globaalse viienda domeeni vahendusel ja/või vastu suunatud rünnete toimepanijad, sh terroristid, kannaksid vastutust. Vastutuse tagamine ning karistamatuse vastu võitlemine eeldab selget, toimivat ja efektiivset õigusraamistikku reguleerimaks küberterrorismi.

Sellest johtuvalt oli töö eesmärgiks läbi kehtiva rahvusvahelise õigusraamistiku analüüsimise leida vastus küsimusele, kas kehtiv rahvusvaheline õigus on piisav, et hoida potentsiaalsed küberterroristid vastutavana. Selleks on töös esmalt uuritud küberterrorismi olemust ja definitsiooni, teiseks on analüüsitud kehtivat rahvusvahelist õigusraamistikku küberterrorismi valguses, ja kolmandaks on töö viimases peatükis toodud ettepanekud meetoditest, mis tugevdaksid küberterroristide vastutusele võtmist ja vastava õigusliku raamistiku edendamist.

Magistritöö esimene peatükk otsib vastuseid küsimusele, kuidas defineerida küberterrorismi. Terrorism, küberterrorism, küberrünnak ja kübersõda (ja teised seotud terminid) on kõik rahvusvaheliselt vaieldatavad mõisted. Küberterrorismile puudub ühene rahvusvaheliselt tunnustatud definitsioon. Küberterrorism koosneb kahest elemendist: küber ja terrorism. Riikidel on küberruumile ja terrorismile (ja sellest tulenevalt küberterrorismile) väga erinev käsitlus. Töös on käsitletud põgusalt terrorismi kui definitsiooni kujunemislugu, seda, kuidas sellest on saanud hukkamõistuna kasutatav termin, aga ka peavoolu arusaama terrorismist ja küberterrorismist, samuti terrorismi ja küberterrorismi kirjeldavaid omadusi. Esimese peatüki viimases osas on kirjeldatud rahvusvahelise kogukonna püüdlusi ametlikult defineerida küberterrorismi. Maailmas puudub ühene definitsioon terrorismist ja seega ka küberterrorismist. Küberruumi reguleerimise ja defineerimise puhul on väljakutseteks nii selle uudsus, kui ka riiklikult erinev lähenemine sellega hõlmatud valdkondadele, sealhulgas Interneti reguleerimine, valitsemine ja turvamine, inimõiguste ja vabaduste piiramine, jne. Terrorismi defineerimise ebaõnnestumiste põhjused võtab edukalt kokku levinud aforism, et *"ühe mehe vabadusvõitleja on teise mehe terrorist"*. Kuigi rahvusvaheline kogukond ei ole

olnud piisavalt üksmeelne, et terrorismi defineerida, on siiski tehtud olulisi edusamme selle mõiste sisustamisel.

Töö teine peatükk keskendub küberterrorismi õiguslikule raamistikule, kus esmalt uuritakse terrorismi reguleerivat rahvusvahelist raamistikku. Kuna rahvusvaheline kogukond ei ole leidnud ühest definitsiooni terrorismile ja loonud üldist õiguslikku instrumenti (kuigi on seda üritanud), töötab praegune terrorismivastane võitlus põhiliselt riiklikul ja regionaalsel või sektoriaalsel (vastavalt konkreetsele terroriakti toimepanemisviisile ja vahendile) tasandil. Kuna efektiivne rahvusvahelise terrorismi vastane võitlus eeldab rahvusvahelist koostööd ja ühist raamistikku, jääb selline lähenemine poolikuks.

Seejärel uuriti töös rahvusvahelist õigust küberterrorismi valguses. Ka küberterrorismile ei ole rahvusvahelist konventsiooni. Küberterrorismi on käsitletud suunavate, soovituslike ja hukkamõistvate väärtustega väljaannetes (ÜRO Peaassamblee otsused, ÜRO Julgeolekunõukogu otsused, aga ka mitmetasandiliste foorumite nagu UN GGE, OEWG ja Tallinn Manual avaldised). Nendes allikates on küberterrorismi ja küberterroristlike tegusi ka tõlgendatud, et pakkuda akadeemilist selgust ja soovitusi rahvusvahelise õiguse tõlgendamisel. Samuti on rahvusvahelised platvormid nagu näiteks OECD, ITU või Euroopa Komisjoni Arvutikuritegevusvastase konventsiooni näol pakkunud reegleid küberruumi reguleerimiseks. Küberkuritegusi (sealhulgas terrorismi) on adresseeritud ka regionaalsel tasandil, nagu näiteks Aasia ja Vaikse Ookeani Majanduskoostöö (ehk APEC), Kagu-Aasia Maade Assotsiatsiooni (lüh ASEAN) ja Hiina koostöö, Euroopa Liidu Nõukogu raames.

Seejuures analüüsiti *ius ad bellum* ja sellega seotud põhimõtete (nagu suveräänsus, jõu kasutamise ja interventsiooni ehk mittesekkumise keeld, hoolsuskohustus) kohaldatavust küberterroristlikele tegudele. Üldiselt võib öelda, et need printsiibid kohalduvad ka küberterrorismile, kuid on selgusetu, kuidas ja mis ulatuses need kohalduvad.

Järgmises alapeatükis käsitleti *ius in bello* ehk rahvusvahelise humanitaarõiguse kohaldatavust küberterroristlikele tegudele. Kuna rahvusvaheline humanitaarõigus on kirjutatud piisavalt üldiselt ja laiaulatuslikult, siis see kohaldub ka küberruumis toimuvale. Samas esineb teatud ebaselgusi, millised küberrelvad ja -sihtmärgid, ning rünnaku tagajärjed on rahvusvahelise humanitaarõiguse reeglite ja põhimõtete järgi lubatud. Samuti pole selge, kuidas need reeglid (Genfi konventsioonide teisest protokollist tulenevad reeglid) kohalduvad mitteriiklikele rühmitustele.

Järgmisena analüüsitakse rahvusvahelise tavaõiguse kohaldatavust küberterrorismile. Kuigi osad allikad leiavad, et rahvusvaheline tavaõigus võiks kohalduda terrorismile, on pigem

kaheldav, kas terrorismi keeld on jõudnud rahvusvahelise tavaõiguse osaks saada. Seega on ebatõenäoline, et ka küberterrorism oleks rahvusvahelise tavaõiguse poolt reguleeritud. Samas rahvusvahelise õiguse printsiibid, mis on saanud tavaõiguse osaks (nagu näiteks jõu kasutamise keeld, hoolsuskohustus, riigivastutus) on rakendatavad ka küberterrorismi puhul.

Järgmises alapeatükis on käsitletud riigivastusega seonduvaid küsimusi küberterrorismi kontekstis. Riigivastutust võiks kohaldada, kui riik kas ise paneb küberterroristliku rünnaku toime (nn riiklik terrorism), läbi agendi kontrollib ja juhib rünnakut või teadvustab ja võtab küberterroristliku kuriteo omaks. Samas võiks riik vastutada ka juhul, kui ei hoia ära küberterroristlikku rünnakut ja/või laseb sellel juhtuda.

Seejärel analüüsitakse rahvusvahelise kriminaalõiguse kohaldatavust küberterrorismile ja üksikisiku vastutust. Terrorism ei ole eraldi kuritegu rahvusvahelise kriminaalõiguse raamistikus, kuid küberterroristlikud teod võiksid olla Rahvusvahelise Kriminaalkohtu Rooma statuudis reguleeritud sõjakuritegude, inimsusevastaste kuritegude ning genotsiidi regulatsioonidega hõlmatud, kui vastavate regulatsioonide kriteeriumid on samuti täidetud. Sellisel juhul võiks küberterroriste kui indiviide menetleda Rahvusvaheline Kriminaalkohus.

Järgmisena käsitletakse rahvusvaheliste inimõiguste kohaldatavust küberterrorismi vastu võitlemisel, aga ka kohaldatavust küberterroristlikele tegudele. Inimõigused kohalduvad nii meetmetele, mida kasutatakse küberterrorismi vastu võitlemisel, kui ka riikidele kohustusena ennetada küberterrorismi. Kuigi küberterroristlikud rünnakud võivad tõsiselt rikkuda isikute inimõigusi ja vabadusi, on inimõiguste ja sellest tulenevate kohustuste kohaldamine mitteriiklikele organisatsioonidele problemaatiline, sest traditsiooniliselt on inimõiguste raamistikku kohaldatud inimese ja riigi vahelistele suhetele. Inimõiguste kohaldamine sõjaolukorras on samuti küsitav. Riike saab aga hoida vastutavana inimõiguste rikkumise eest, kui seoses küberterrorismiga ei ole näiteks loodud adekvaatset kriminaalsüsteemi või riik laseb küberterrorismil juhtuda.

Töö kolmandas peatükis on toodud näiteid, kuidas rahvusvahelist raamistikku edendada, et küberterrorismi vastu võidelda ja küberterroriste vastutusele võtta. Selleks on pakutud praktilisi soovitusi, aga ka teoreetilisi väljavaateid. Soovituste hulgas pakuti välja näiteks rahvusvahelise õiguse edasine interpreteerimine küberterrorismi valguses, õiguse moderniseerimine, ühiste lähenemiste otsimine, õiguse harmoniseerimine, rahvusvaheline mitmetasandilise koostöö tugevdamine, aga ka uute regulatsioonide või uue konventsiooni vastuvõtmine, mis käsitleks küberterrorismi ja edendaks rahvusvahelist võitlust (küber)terrorismi ja süüdimatuse vastu.

Töös on kasutatud peamiselt rahvusvahelise õiguse allikaid, sh rahvusvahelised konventsioonid, kohtupraktika, üldpõhimõtted, aga ka (õigus)teadlaste artiklid. Töös on kasutatud kvalitatiivset dogmaatilist õigusanalüütilist meetodit, samuti deduktiivset analüütilist meetodit. Analüüsi käigus on terrorismi käsitlevaid definitsioone ja regulatsioone vaadeldud küberkontekstis. Analüüsi on ilmestatud näidetega terroristlikest rünnakutest, küberrünnakutest aga ka küberterroristlikest rünnakutest.

Analüüsi käigus leiti vastuseid uurimisprobleemile, kas rahvusvaheline õigus on piisav tagamaks vastutust küberterrorismi eest. Töö analüütilises osas leiti, et kuigi rahvusvaheline õigus kohaldub küberterrorismile, siis see ei ole piisav tagamaks küberterroristlike tegude eest vastutusele võtmist. Töös pakuti välja teoreetilisi ja praktilisi võimalusi vastutuse tugevdamiseks. Muuhulgas oleks tarvis rohkem tõlgendada rahvusvahelise õiguse norme küberkontekstis, sealhulgas seoses küberterrorismiga.

LITERATURE

LAWS AND TREATIES

1) European Commission. NIS directive. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis-directive
2) Council of Europe. Convention on Cybercrime. 2001. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
3) The European Parliament and the Council of the European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). 2019. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj
4) International Committee of the Red Cross (ICRC). Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949. Available at: https://ihl-databases.icrc.org/ihl/WebART/375-590006.
5) International Committee of the Red Cross (ICRC). Treaties, State parties, and Commentaries. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. Article 51: Protection of the civilian population. Available at: https://ihl-databases.icrc.org/ihl/WebART/470-750065
6) International Committee of Red Cross (ICRC). Treaties, States Parties and Commentaries. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977. Article 13: Protection of the civilian population. Available at: https://ihl-databases.icrc.org/ihl/WebART/475-760019?OpenDocument
7) International Telecommunications Union (ITU). Collection of the basic texts adopted by the Plenipotentiary Conference. 2019. Available at: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.22.61.en.100.pdf
8) United Nations. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. 2008. Available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf
9) United Nations (UN). International Convention for the Suppression of the Financing of Terrorism. 1999. Available at: https://www.un.org/law/cod/finterr.htm

10) Peace Treaty of Tartu. Tartu, Estonia, 02.02.1920. Available at: https://hub.xpub.nl/termsofservice/peace-treaty-of-tartu.html
11) U.S. Congress. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. Public Law 107-56-OCT. 26, 2001. Authenticated U.S. Government Information. 2001. Available at: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf
12) 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft (Aircraft Convention) (deposited with the International Civil Aviation Organization);
13) 1970 Convention for the Suppression of Unlawful Seizure of Aircraft (Unlawful Seizure Convention) (deposited with the International Civil Aviation Organization);
14) 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Civil Aviation Convention) (deposited with the International Civil Aviation Organization);
15) 1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons (Diplomatic agents Convention);
16) 1979 International Convention against the Taking of Hostages (Hostages Convention) (deposited with the Secretary-General of the United Nations);
17) 1980 Convention on the Physical Protection of Nuclear Material (Nuclear Materials Convention) (deposited with the International Atomic Energy Agency);
18) 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (extends and supplements the Montreal Convention on Air Safety) (Airport Protocol) (deposited with the International Civil Aviation Organization);
19) 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Maritime Convention) (deposited with the International Maritime Organization);
20) 1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf (Fixed Platform Protocol) (deposited with the International Maritime Organization);
21) 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection (Plastic Explosives Convention) (deposited with the International Civil Aviation Organization);
22) 1997 International Convention for the Suppression of Terrorist Bombings (Terrorist Bombing Convention);

23) 1998 International Convention for the Suppression of Terrorist Bombings;
24) 1999 International Convention for the Suppression of Terrorist Financing (Terrorist Financing Convention);
25) 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (deposited with the International Maritime Organization)
26) 2005 Protocol to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (deposited with the International Maritime Organization).
27) 2005 International Convention for the Suppression of Acts of Nuclear Terrorism;
28) 2005 Amendments to the Convention on the Physical Protection of Nuclear Material (deposited with the International Atomic Energy Agency).

UNITED NATIONS RESOLUTIONS

1) United Nations General Assembly resolution 49/60 of 9 December 1994. Declaration on Measures to Eliminate International Terrorism. A/RES/49/60.
2) United Nations General Assembly. The United Nations Global Counter-Terrorism Strategy. A/RES/60/288. New York: United Nations. 2006. Available at: https://undocs.org/en/A/RES/60/288
3) United Nations Security Council. Resolution 1373 (2001). S/RES/1373. 2001. Available at: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf
4) United Nations Security Council. Resolution 1624 (2005). S/RES/1624. 2005. Available at:
5) https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1624%282005%29
6) United Nations Security Council. Resolution 1923 (2010). S/RES/1923. 2010. Available at: http://unscr.com/en/resolutions/doc/1923

COURT PRACTICE

1) Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007. Available at: https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf
2) European Court of Human Rights. Case S.A.S v. France. Judgment. Grand Chamber. Strasbourg. 2014.

3) International Court of Justice (ICJ). Continental Shelf. Libyan Arab Jamahiriya/Malta. Judgement. ICJ Reports. 1985. Available at: https://www.icj-cij.org/public/files/case-related/68/068-19840321-JUD-01-00-EN.pdf.
4) International Court of Justice (ICJ). Legality of the Threat or Use of Nuclear Weapons. Advisory Opinion. ICJ Reports 1996. ICJ 266. 1996.
5) International Court of Justice (ICJ). Nicaragua v. United States of America. Case concerning military and paramilitary activities in and against Nicaragua. Reports of judgements, advisory opinions and orders. 1986. Available at: https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf
6) International Court of Justice (ICJ). North Sea Continental Shelf. Federal Republic of Germany/Denmark, Federal Republic of Germany/Netherlands. Judgement. ICJ Reports. 1969. Available at: https://www.icj-cij.org/public/files/case-related/52/052-19690220-JUD-01-00-EN.pd
7) International Court of Justice (ICJ). The Corfu Channel case. Reports of judgements, advisory opinions and orders. 1949. Available at: https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf
8) International Criminal Tribunal for the former Yugoslavia (ICTY). Prosecutor v. Duško Tadić. Case No IT-94-1-A. Judgement of the Appeals Chamber. 15 July 1999. Available at: https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf
9) International Criminal Tribunal for the former Yugoslavia (ICTY). Prosecutor v. Stanislav Galić. ICTY Appeals Chamber. Judgement. IT-98-29-A. 2006. Available at: https://www.icty.org/x/cases/galic/acjug/en/gal-acjud061130.pdf
10) United Nations. Reports of International Arbitral Awards. Island of Palmas case (Netherlands, USA). 1928. Available at: https://legal.un.org/riaa/cases/vol_II/829-871.pdf

GUIDELINES, STRATEGIES, REPORTS, STUDIES AND OTHER OFFICIAL MATERIALS

1) Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, adopted by Heads of State and Government at the NATO in Lisbon 19-20 November 2010. Available at: http://www.nato.int/strategic-concept/pdf/ Strat_Concept_web_en_pdf

2) Council of Europe. Committe of Experts on Terrorism (CODEXTER). Application of International Humanitarian Law and Criminal Law to Terrorism Cases in Connection with Armed Conflicts. Discussion Paper. 2017 Available at: https://rm.coe.int/16807025f9
3) Counter-Terrorism Implementation Task Force (CTITF). Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects. CTITF Working Group Compendium. 2011. Available at: https://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf
4) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN/2013/01. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001
5) D. E. Denning. Testimony before the Special Oversight Panel on Terrorism. U.S. House of Representatives. Committee on Armed Services. 2000. Available at http://commdocs.house.gov/committees/security/has144240.000/has144240_0f.htm
6) European Commission. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. Brussels, 9.12.2020. COM(2020) 795 final. 2020. Available at: https://ec.europa.eu/home-affairs/sites/default/files/pdf/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf
7) European Commission. EU cybersecurity initiatives: working towards a more secure online environment. 2017. Available at: https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.
8) European Commission. New EU Cybersecurity Strategy. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. 2020. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
9) European Defence Agency. Cyber Defence. Available at: https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence
10) Gen. ed. A Klimburg. National Cyber Security: Framework Manual. Political Aims and Policy Methods. NATO CCD COE. Tallinn. 2012.

11) M. N. Schmitt. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. 2017.
12) M. N. Schmitt. Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge University Press. 2013. Available at: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf
13) Geneva Call. Introduction to the Law of Armed Conflict (LOAC). 2013. Available at: http://www.genevacall.org/wp-content/uploads/dlm_uploads/2013/11/The-Law-of-Armed-Conflict.pdf
14) Global Terrorism Index 2017 by the Institute for Economics and Peace. Available at: https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%202017%20%284%29.pdf
15) HM Government. A strong Britain in an Age of Uncertainty: The National Security Strategy. 2010. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.
16) ICRC. Customary IHL Study. Available at: https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf
17) ICRC. International Humanitarian Law and Cyber Operations during Armed Conflicts. ICRC Position Paper. 2019. Available at: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts
18) ICRC. International humanitarian law and terrorism: Questions and answers: What does IHL say about terrorism? 2011. Available at: https://www.icrc.org/data/rx/en/resources/documents/faq/terrorism-faq-050504.htm
19) International Criminal Court (ICC). Understanding the International Criminal Court. The Hague: ICC. 2013. Available at: https://www.icc-cpi.int/iccdocs/PIDS/publications/UICCEng.pdf
20) ISO/IEC 27032:2012. Information technology - Security techniques - Guidelines for cybersecurity. 2012, para. 4.18. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en
21) International Telecommunications Union. ITU National Cybersecurity Strategy Guide. Geneva. 2011. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

22) Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade. 2020. Available at: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade
23) National Commission on Terrorist Attacks Upon the United States. The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks Upon the United States. Available at: https://govinfo.library.unt.edu/911/report/911Report_Exec.htm
24) National Consortium for the Study of Terrorism and Responses to Terrorism. Global Terrorism Overview: Terrorism in 2019. Background Report. University of Maryland. 2020. Available at: https://www.start.umd.edu/pubs/START_GTD_GlobalTerrorismOverview2019_July2020.pdf
25) OEWG. Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 2020. Available at: https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf
26) Strategic Autonomy and Cybersecurity in the Netherlands. Cyber Security Council. 2021. Available at: https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands
27) The Council of the European Union. Council of the European Union Framework Decision 2008/919/JHA of 28 November 2008 amending Framework 22 Decision 2002/475/JHA on combating terrorism. 2008/919/JHA. 2008. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0919
28) The Global Campaign for Ratification and Implementation of the Kampala Amendments on the Crime of Aggression. The Council of Advisers on the Application of the Rome Statute to Cyberwarfare. Available at: https://crimeofaggression.info/the-campaign/the-council-of-advisers-on-the-application-of-the-rome-statute-to-cyberwarfare/
29) The White House. President Barack Obama. Office of the Press Secretary. Fact Sheet: Cybersecurity National Action Plan. 2016. Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
30) The World Economic Forum. The Global Risks Report. 16th Edition. 2021. Available at: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

31) The World Economic Forum. The Global Risks Report. 2020. Available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
32) U.S. Department of State. 1993 World Trade Center Bombing. 2019. Available at: https://www.state.gov/1993-world-trade-center-bombing/
33) United Nations General Assembly. Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy. A/75/729. 2021. Available at: https://undocs.org/A/75/729
34) United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2013. Available at: https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf
35) United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. 2015. Available at: https://undocs.org/A/70/174
36) United Nations General Assembly. Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. A/AC.290/2021/CRP.2. 2021. Available at: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
37) United Nations General Assembly (UNGA). Letter dated 3 August 2005 from the Chairman of the Sixth Committee addressed to the President of the General Assembly. A/59/894. Available at: https://undocs.org/en/A/59/894
38) United Nations General Assembly. The United Nations Global Counter-Terrorism Strategy. A/RES/60/288. New York: United Nations. 2006. Available at: https://undocs.org/en/A/RES/60/288
39) United Nations Office of Disarmament Affairs (UNODA). OEWG. Joint Contribution – Programme of Action. The future of discussions on ICTs and cyberspace at the UN last updated on the 2nd of December 2020. Available at: https://front.un-arm.org/wp-content/uploads/2020/12/joint-contribution-PoA-future-of-cyber-discussions-at-the-un-2-2-2020.pdf

40) United Nations Office on Drugs and Crime. Frequently Asked Questions on International Law Aspects of Countering Terrorism. Vienna: UNODC. 2009. Available at: https://www.unodc.org/documents/terrorism/Publications/FAQ/English.pdf
41) United Nations. Draft Statute for an International Criminal Court with commentaries. Report of the International Law Commission on the work of its forty-sixth session. 1994. Available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/7_4_1994.pdf
42) United Nations. Draft Statute for an International Criminal Court with commentaries. Report of the International Law Commission on the work of its forty-sixth session. 1994. Available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/7_4_1994.pdf
43) United Nations Office on Drugs and Crime. Counter-Terrorism Module 1. Vienna. 2018. Available at: https://www.unodc.org/documents/e4j/18-04932_CT_Mod_01_ebook_FINALpdf.pdf
44) United Nations Office on Drugs and Crime. The use of the Internet for terrorist purposes. New York. 2012. Available at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

BOOKS, ARTICLES, AND OTHER LITERARY SOURCES

1) A. Bellal. Beyond the pale? A. Bellal. Interview regarding international law and ISIS. Interview by H. Edwards, Geneva, 2016.
2) A. Cassese, G. Acquaviva, M. Fan, A. Whiting. International Criminal Law. Cases and Commentary. Terrorism. Oxford University Press. 2011.
3) A. Cassese, P. Gaeta, J. R. W. D Jones. The Rome Statute of the International Criminal Court: A Commentary. Volume 1. Oxford University Press. 2002.
4) A. Cohen. Prosecuting terrorists at the International Criminal Court: Re-evaluating an unused legal tool to combat terrorism: Michigan State International Law Review 20, no. 2. 2012.
5) A.-M. Talihärm. Cyberterrorism: in Theory or in Practice? Defence against terrorism review. 2010.
6) B. Hoffman. Inside Terrorism. New York: Columbia University Press. 1998.

7) D. Bessner, M. Stauch. Karl Heinzen and the Intellectual Origins of Modern Terror. Terrorism and Political Violence. Volume 22. 2010. Available at: https://www.tandfonline.com/doi/abs/10.1080/09546550903445209
8) D. E. Denning. Cyberterrorism. Global Dialogue. 2000. Available at: http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf.
9) D. Rappoport. The Four Waves of Modern Terrorism. A. Cronin, J. Ludes, eds. Attacking Terrorism: Elements of a Grand Strategy. Washington, DC: Georgetown University Press. 2004.
10) D. T. Borgeois. Information Systems for Business and Beyond. The Saylor Academy. 2014.
11) E. Chadwick. Self-Determination, Terrorism and the International Humanitarian Law of Armed Conflict. 1996.
12) F. Nietzsche. On the Genealogy of morals. 1887, II:13.
13) F. Ristoldo. Attacks against Cultural Property as a weapon of war: An exploratory case study. Institut Barcelona Estudis Internacionals. 2016-2017. Available at: https://www.ibei.org/ibei_studentpaper34_105354.pdf
14) G. Austin. China's Cybersecurity and Pre-emptive Cyber War. NewEurope. 2011.
15) Gen. ed. D. M. Jones, P. Schulte, C. Ungerer, M. L. R. Smith. International law and terrorism: the case of ISIS. Handbook of Terrorism and Counter Terrorism Post 9/11. USA. Edward Elgar Publishing Limited. 2019.
16) G. Nunberg. HEAD GAMES / It All Started with Robespierre / "Terrorism": The history of a very frightening word. SFGATE. Opinion. 2001, updated 2012. Available at: https://www.sfgate.com/opinion/article/HEAD-GAMES-It-All-Started-with-Robespierre-2865759.php
17) G. Weimann. Cyberterrorism: How Real Is the Threat? United Nations Institute of Peace. Special Report. Washington. 2004. Available at: https://www.usip.org/sites/default/files/sr119.pdf
18) H. Durham. Cyber Operations During Armed Conflict: 7 Essential Law and Policy Questions. ICRC blogs. Humanitatian Law & Policy Blog. 2020. Available at: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/?utm_campaign=DP_FORUM%20Cyber%20operations%20during%20armed%20conflict%3A%207%20essential%20law%20and%20policy%20questions&utm_source=hs_email&utm_medium=email&utm_content=85308521&_hsenc=p2ANqtz-8-XJ_x1tNb-Vspuc2CoVbalosrTb-w3h7ifr-

e1wNzMCocsKxsJtggq6uHCfXnhk3hM-EPHnRxHDbh1TPGigkT7MqUVQ&_hsmi=85308521.

19) J. Crawford. State Responsibility: The General Part. Cambridge Studies in international and comparative law. Cambridge University Press. 2013.
20) J.-T. Kim, T. Hyun. Status and Requirements of Counter-Cyberterrorism. World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering. Vol:1, No:6. 2007. Available at: https://publications.waset.org/11708/status-and-requirements-of-counter-cyberterrorism
21) J. Jarvis, S. Macdonald. What is cyberterrorism? Findings from a survey of researchers. Terrorism and Political Violence 27, no. 4. 2017.
22) K. Mačák, T. Jančárková, T. Minárik. The right tool for the job: how does international law apply to cyber operations? Humanitarian Law & Policy. ICRC blogs. 2020. Available at: https://blogs.icrc.org/law-and-policy/2020/10/06/international-law-cyber-operations/.
23) L. MacKinnon, D. Gan, L. Bacon, G. Loukas. D. Chadwick, D. Frangiskatos. Strategic Intelligence Management. Book Chapter 20: Cyber Security Countermeasures to Combat Cyber Terrorism. 2013. Available at: https://www.researchgate.net/publication/285181525_Cyber_Security_Countermeasures_to_Combat_Cyber_Terrorism
24) M. Bergwick. Due Diligence in Cyberspace. An assessment of rule 6 in the Tallinn Manual 2.0. Uppsala Universitet. 2020, p. 23. Available at: https://www.diva-portal.org/smash/get/diva2:1417207/FULLTEXT01.pdf
25) M. Burgess. History of Terrorism. POGO. 2012. Available at: https://www.pogo.org/investigation/2015/02/brief-history-of-terrorism/
26) M. Conway. Cyberterrorism: Hype and Reality. Dublin City University. 2007. Available at: https://core.ac.uk/download/pdf/11308376.pdf
27) M. G. Devost, B. K. Houghton, N. A. Pollard. Information Terrorism: Political Violence in the Information Age. 1997.
28) M. Sassoli. Transnational armed groups and international humanitarian law. Program on Humanitarian Policy and Conflict Research. Occasional Paper Series. No. 6, February 2006, 22.
29) M. Vlasic, H. Turku. 2016. Our cultural heritage is under attack. We must all join the fight to protect it. World Economic Forum (WEF). Available at:

https://www.weforum.org/agenda/2016/10/our-cultural-heritage-is-under-attack-we-must-all-join-the-fight-to-protect-it/.

30) M.P. Scharf. How the war against ISIS changed international law. Case Western Reserve Journal of International Law 48. 2016. Available at: scholarlycommons.law.case.edu/faculty_publications/1638.
31) Mark M. Pollitt. Cyberterrorism: Fact or Fancy?,' published in Computer Fraud and Security in 1998.
32) National Research Council, Computers at Risk: Safe Computing in the Information Age. Washington DC: National Academy Press. 1991. Available at: http://www.nap.edu/books/0309043883/html/index.html
33) N. A. Makhutov, V. P. Petrov, and D. O. Reznikov. Countering Terrorism: Biological Agents, Transportation Networks, and Energy Systems: Summary of a U.S.-Russian Workshop. Chapter: 7 Characteristics of Technological Terrorism Scenarios and Impact Factors. 2009.
34) R. Cryer, H. Friman, D. Robinson, E. Wilmshurst. An Introduction to International Criminal Law and Procedure. Other Crimes. Transnational Crimes, Terrorism and Torture. 2. ed. Cambr. 2010.
35) R. Värk. Terrorism, State Responsibility and the Use of Armed Force. ENDC Proceedings, Volume 14. 2011.
36) T. Parker, N. Sitter. The Four Horsemen of Terrorism: It's Not Waves, It's Strains. Routledge. 2016. Available at: https://www.tandfonline.com/doi/pdf/10.1080/09546553.2015.1112277
37) W. Laqueur. The New Terrorism: Fanaticism and the arms of mass destruction. New York, Oxford University Press. 1999.
38) World Academy of Science, Engineering and Technology. Status and Requirements of Counter-Cyberterrorism. Available at: https://publications.waset.org/11708/status-and-requirements-of-counter-cyberterrorism

OTHER SOURCES

1) A. Greenberg. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. The Wired. 2018. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

2) BBC News. Ariana Grande reflects on Manchester bombing ahead of anniversary. 2020 Available at:
https://www.bbc.com/news/entertainment-arts-52752383
3) BBC News. Aum Shinrikyo: The Japanese cult behind the Tokyo Sarin attack. 2018. Available at:
https://www.bbc.com/news/world-asia-35975069
4) BBC News. Running for your life from terror in north-east Mozambique. 12 March 2021. Available at: https://www.bbc.com/news/av/world-africa-56373615
5) BBC News. Sri Lanka attacks: Easter Sunday bombings marked one year on. 2020. Available at:
https://www.bbc.com/news/world-asia-52357200
6) BBC News. Sri Lanka to ban burka and other face coverings. 2021. Available at:
https://www.bbc.com/news/world-asia-56386426
7) BBC News. Switzerland referendum: Voters support ban on face coverings in public. 2021. Available at: https://www.bbc.com/news/world-europe-56314173
8) BBC News. 7 July London bombings: What happened that day? 2015. Available at:
https://www.bbc.com/news/uk-33253598
9) BBC News. Westgate attack: Two jailed over Kenyan shopping mall attack. 2020. Available at:
https://www.bbc.com/news/world-africa-54748341
10) Cambridge Dictionary. Cyberterrorism. Available at: https://dictionary.cambridge.org/dictionary/english/cyberterrorism.
11) Cambridge Dictionary. Terrorism. Available at: https://dictionary.cambridge.org/dictionary/english/terrorism.
12) Collins Dictionary. Cybererrorism. Available at: https://www.collinsdictionary.com/dictionary/english/cyberterrorism
13) Collins Dictionary. Terrorism. Available at: https://www.collinsdictionary.com/dictionary/english/terrorism.
14) Digwatch. UN GGE and OEWG. Available at: https://dig.watch/processes/un-gge
15) D.Mair. #Westgate: A Case Study: How al-Shabaab used Twitter during an Ongoing Attack, Studies in Conflict & Terrorism. Available at: https://www.tandfonline.com/doi/pdf/10.1080/1057610X.2016.1157404?casa_token=0NzngSf4tisAAAAA:hajQRdhfivqtRzSdPEZgdjdZxhv4VZEMRmqb9ZPx5QyOblTaUNOXq_z54mGlKqfM5ww5WYm8mN6BxA

16) E. Nakashima, J. Warrick. Stuxnet was work of U.S. and Israeli experts, officials say. The Washington Post. 2012. Available at: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

17) Encyclopedia Britannica. Cybercrime. Types of Cybercrime. Available at: https://www.britannica.com/topic/cybercrime#ref1285671.

18) Encyclopedia Britannica. Peshawar school massacre. Available at: https://www.britannica.com/event/Peshawar-school-massacre

19) Encyclopedia Britannica. Types of Terrorism. Available at: https://www.britannica.com/topic/terrorism/Types-of-terrorism.

20) Foreign Broadcast Information Service (FBIS). Russia Cracks Down on 'Cyberterrorism'. ITAR-TASS. FBIS-SOV-2002-0208. 8 February, 2002.

21) N. Forrester. 2020. "New report reveals countries most targeted by 'significant' cyberattacks". EU Security Brief. 13 July 2020. Available at: https://securitybrief.eu/story/new-report-reveals-countries-mosttargeted-by-significant-cyber-attacks

22)

23) I. Jibilian, K. Canales. The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. Business Insider. 2021. Available at: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

24) I. van den Herik, C. Rose, Y. Radi. Towards an international terrorism tribunal? Universiteit Leiden. video tuition course. n.d. para 2. Available at: https://www.coursera.org/lecture/international-law-in-action/towards-an-international-terrorism-tribunal-wNQY1

25) J. Davis. Hackers Take Down the Most Wired Country in Europe. The Wired. 2007. Available at: https://www.wired.com/2007/08/ff-estonia/.

26) J. Griffiths. 'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on. CNN Business. 2020. Available at: https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html

27) J. P. Jenkins. Terrorism. Encyclopedia Britannica. Available at: https://www.britannica.com/topic/terrorism.
28) Macmillan Dictionary. Terrorism. Available at: https://www.macmillandictionary.com/dictionary/british/terrorism.
29) South China Morning Post. Istanbul airport bombers planned to take hostages during attack. Available at: https://www.scmp.com/news/world/middle-east/article/1984157/istanbul-airport-bombers-planned-take-hostages-during-attack
30) The Economist. “On the edge of a precipice”: Macron's stark warning to Europe. 9. November 2019. Available at: https://www.economist.com/weeklyedition/2019-11-09
31) The Guardian. Charlie Hebdo trial: French court convicts 14 over 2015 terror attacks. 2020. Available at: https://www.theguardian.com/world/2020/dec/16/charlie-hebdo-trial-french-court-convicts-14-over-2015-terror-attacks
32) The New York Times. Anders Behring Breivik, Killer in 2011 Norway Massacre, Says Prison Conditions Violate His Rights. 2016. Available at: https://www.nytimes.com/2016/03/16/world/europe/anders-breivik-nazi-prison-lawsuit.html
33) The New York Times. Realizing It’s a Small, Terrifying World After All. Orlando Shooting. 2016. Available at: https://www.nytimes.com/2016/06/21/us/orlando-shooting-america.html
34) The New York Times. Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage. Available at: https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html.
35) Z. Whittaker. Two Years after WannaCry, a million computers remain at risk. TechCrunch. 2019. Available at: https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1