THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XVIII STLR.ORG FALL 2016

ARTICLE

WORLD WIDE WEB OF EXPLOITATIONS – THE CASE OF PEACETIME CYBER ESPIONAGE OPERATIONS UNDER INTERNATIONAL LAW: TOWARDS A CONTEXTUAL APPROACH †

Ido Kilovaty*

The emergence of cyber espionage, as well as the ability to leak gathered sensitive information, has exacerbated the complexity of determining the legality of espionage under international law. Cyber espionage, just like other cyber operations, offers a highly sophisticated, relatively inexpensive, and accessible medium to achieve certain informational, political, and operational goals. The indeterminacy of cyber espionage in international law has given rise to various arguments as to which international norms and principles are applicable to cyber espionage. Divergent positions, however, focus only on certain aspects of cyber espionage. For this reason, the scope of legal treatment of cyber espionage is limited and lacks context. The purpose of this article is to reject this dichotomous approach and propose a more nuanced framework for addressing cyber espionage in international law. Cyber operations should be analyzed on a continuum that triggers different norms depending on the context and consequences. The contextual

* Cyber Fellow, Center for Global Legal Challenges, Yale Law School; Resident Fellow, Information Society Project, Yale Law School; Doctor of Juridical Sciences Candidate (S.J.D), Georgetown University Law Center; This paper was presented at the Cornell Law Scholars conference (April 2015), Yale Law Doctoral conference (December 2015), and the Georgetown Law SJD seminar. I wish to thank the organizers, colleagues, commentators, and dedicated staff of the Columbia Science and Technology Law Review who helped in the revision process of this paper.

approach focuses on the effects of a cyber operation and the context in which it occurs to determine the relevant set of norms applicable to it.

I. INTRODUCTION

In December 2014, hackers broke into U.S. Office of Personnel Management (OPM) computers and stole sensitive data, including the personal information of approximately four millions federal employees.[1] The data included social security numbers, e-mail addresses, job performance reviews,[2] and even security clearance

---

1. Ellen Nakashima, *Chinese Breach Data of 4 Million Federal Workers*, WASH. POST (June 4, 2015), http://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.

2. Brian Bennett & Richard Serrano, *Chinese Hackers Sought Information to Blackmail U.S. Government Workers, Officials Believe*, L.A. TIMES (June 5,

applications.[3] According to U.S. officials, the immediate suspect was China.[4] Certain experts went as far as to suggest that China may be collecting intelligence in preparation for a future attack against the United States[5] and that this hack "involve[d] the greatest theft of sensitive personnel data in history."[6] The Chinese government denied allegations, stating that the accusations were "not responsible and counterproductive"[7] and that the OPM hack was a criminal matter.[8]

Cyberspace allows individuals and groups, as well as states, to collect massive amounts of information, both openly and clandestinely. While espionage *per se* is far from a new phenomenon in inter-state relations, cyber espionage is a relatively new extension of that phenomenon.[9] Peacetime espionage operations are carried

---

2015, 3:52 PM), http://www.latimes.com/nation/la-na-government-cyberattack-20150605-story.html#page=1.

3. Theodore Schleifer & Evan Perez, *Hackers May Have Stolen Applications for Security Clearances*, CNN (June 13, 2015, 2:53 PM), http://www.cnn.com/2015/06/12/politics/security-clearance-chinese-hackers.

4. Matt Spetalnick & David Brunnstrom, *China in Focus as Cyber Attack Hits Millions of U.S. Federal Workers*, REUTERS (June 5, 2015, 4:03 AM), http://www.reuters.com/article/2015/06/05/us-cybersecurity-usa-idUSKBN0OK2IK20150605.

5. Kevin Liptak, Theodore Schleifer & Jim Sciutto, *China Might be Building Vast Database of Federal Worker Info, Experts Say*, CNN (June 6, 2015, 9:38 AM), http://www.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management.

6. Michael Adams, *Why the OPM Hack is Far Worse Than You Imagine,* LAWFARE (Mar. 11, 2016, 10:00 AM), https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

7. Eyder Peralta, *China Says U.S. Allegations That It Was Behind Cyberattack Are 'Irresponsible'*, NPR (June 5, 2015, 5:25 PM), http://www.npr.org/sections/thetwo-way/2015/06/05/412190405/china-says-u-s-allegations-that-it-was-behind-cyberattack-are-irresponsible.

8. Paul Carsten and Mark Hosenball, *China's Xinhua says U.S. OPM Hack was not State-Sponsored,* REUTERS (Dec. 2, 2015), http://www.reuters.com/article/us-china-usa-cybersecurity-idUSKBN0TL0F120151202.

9. Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L. L. 1071, 1072 n.2 (2006) (citing 1 ENCYCLOPEDIA OF INTELLIGENCE AND COUNTER-INTELLIGENCE xv (Rodney P. Carlisle ed., 2005) (giving the example of the Chinese military strategist Sun Tzu's *The Art of War* from about 500 B.C.E. as an early work discussing espionage). Some even trace it back to the times of Pharaoh Ramses, circa 1274 B.C. *See* Katharina Ziolkowski, *Peacetime Cyber Espionage – New Tendencies in Public International Law*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 425, 425 (Katharina Ziolkowski ed., 2013) (referring to TERRY CROWDY, THE ENEMY WITHIN: A HISTORY OF ESPIONAGE 15 (2006)).

out by a considerable number of states on a daily basis,[10] and cyber espionage comprises an increasing share of this activity.[11] While international law does not define or explicitly prohibit espionage,[12] the majority of domestic legal systems criminalize foreign espionage, whereas international law tolerates such activities.[13] In other words: "Espionage is nothing but the violation of someone else's laws."[14]

This divergence between domestic and international legal systems has sparked widespread academic debate.[15] Meanwhile, growing reliance on the Internet and information systems led to the emergence of cyber espionage, which added to the debate.

Cyber espionage represents a relatively new method of inter-state spying and data collection, which is similar, but not identical, to traditional espionage. The legal uncertainty surrounding espionage is magnified in the cyber context. Cyberspace allows for more nuanced operations, and concepts of attribution, accountability, damage assessment, and prevention become somewhat fuzzy. Cyber espionage capabilities, as well as the absence of consistent and overt state practice relating to the use of these capabilities, therefore pose an even greater challenge to legal frameworks that were ambiguous to begin with.

The purpose of this article is to unveil the uncertainties and gaps within international law with respect to cyber espionage, and to propose an approach that applies different international legal norms and principles to various types of cyber espionage operations, depending on their nature and context. First, this article will introduce the concept of cyber espionage, define its terminological boundaries, and provide real-world examples of peacetime cyber

---

10. Christian Czosseck, *State Actors and their Proxies in Cyberspace*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 1, 14 (Katharina Ziolkowski ed., 2013).

11. Pete Warren, *State-Sponsored Cyber Espionage Projects Now Prevalent, Says Experts*, THE GUARDIAN (Aug. 30, 2012 6:54 AM), http://www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent.

12. Christopher Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L. L. REV. 1091, 1093-95 (2003).

13. *See* Chesterman, *supra* note 10, at 1072.

14. *U.S. Intelligence Agencies and Activities: Risks and Control of Foreign Intelligence: Hearings Before the H. Select Comm. on Intelligence, Part 5*, 94th Cong. 1767 (1975) (statement of Mitchell Rogovin, Special Counsel to CIA Director).

15. *See generally* John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595 (2006); Geoffrey Demarest, *Espionage in International Law,* 24 DENV. J. INT'L L. & POL'Y 321 (1995).

espionage. Second, it will provide and analyze the different norms and principles of international law applicable to espionage and cyber espionage, including sovereignty, non-intervention, and the prohibition on the use of force. Third, this article will introduce the contextual approach, which distinguishes between cyber espionage operations carried out for political purposes and cyber espionage operations carried for economic or other purposes.

II. CYBER ESPIONAGE – OLD PURPOSE, NEW MEDIUM

Defining "cyber espionage" is complicated because any definition is prone to becoming outdated almost instantaneously. No universal definition exists because there is no consistent and long-standing state practice or international cyber-treaty. While it is unlikely that such a treaty will be adopted in the near future,[16] many experts (including the author of this article) have argued that a treaty following the Chemical Weapons Convention model would make sense.[17]

However, other regional treaties related to cyberspace are currently in force, such as the Council of Europe (CoE) Convention on Cybercrime, which obligates signatories to adopt legislative and other measures to prohibit certain activities in cyberspace.[18] As a relevant example, the CoE Convention requires that signatories adopt domestic laws criminalizing the intentional "interception without right, made by technical means, of non-public transmissions

---

16. *See* Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, KORET-TAUBE TASK FORCE ON NAT'L SEC. & LAW 12 (2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf ("the fundamental clash of interests concerning the regulation of electronic communications, the deep constraints the United States would have to adopt to receive reciprocal benefits in a cybersecurity treaty, and the debilitating verification problems will combine to make it unfeasible to create a cybersecurity treaty that purports to constrain governments."). *Compare with Should There be an International Treaty on Cyberwarfare?*, U.S. NEWS (June 8, 2012, 4:00 PM), http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare (noting that 6 out of 7 experts argued that there should not be a treaty on cyber warfare, for various reasons). *See also* Phillip A. Johnson, *Is It Time for a Treaty on Information Warfare?*, 76 INT'L L. STUD. 439 (2002).

17. *See* Ido Kilovaty & Itamar Mann, *Towards a Cyber-Security Treaty*, JUST SECURITY (Aug. 3, 2016, 5:07 PM), https://www.justsecurity.org/32268/cyber-security-treaty. *See also* Louise Arimatsu, *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations, in* 2012 4TH INT'L CONV. ON CYBER CONFLICT 91 (C. Czosseck, R. Otis & K. Ziolkowski eds., 2012).

18. Council of Europe, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, *available at* https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

of computer data to, from or within a computer system."[19] Unfortunately, the CoE Convention is focused on creating domestic criminal laws rather than setting international norms and standards for the regulation of cyber espionage. Nonetheless, the CoE Convention does provide some guidance on "trans-border access to stored data" by clarifying that parties may access stored computer data in another party's territory when that data is either publicly available or when the "lawful and voluntary consent" of the authorized person has been obtained.[20]

A. Defining Cyber Espionage

For the purposes of this article, cyber espionage will be defined as "[t]he science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence," or for other nationally sensitive, intelligence, for political ends.[21] This definition may require an update as cyber operations become more nuanced and sophisticated in the future.

There are four elements within this definition. First, the act must be covert, meaning that it should be without the awareness or consent of the entity being spied upon.[22] This is not to say that the act will remain covert, as it could be discovered by the victim or disclosed by the perpetrator.[23] The hack on the Democratic National Committee illustrates how an intelligence gathering operation was disclosed by the hackers leaking the information on WikiLeaks.[24]

---

19. *Id.* at art. 3.

20. *Id.* at art. 23.

21. This definition was first introduced by Seymour M. Hersh, *The Online Threat: Should We Be Worried About a Cyber War*?, THE NEW YORKER (Nov. 1, 2010), http://www.newyorker.com/magazine/2010/11/01/the-online-threat. Also, this definition was adopted by Oona Hathaway et al., *The Law of Cyber-Attack,* 100 CAL. L. REV. 817, 829 n. 48 (2012). For the purposes of this article, this definition was slightly modified to capture the national security aspect of cyber espionage.

22. *See* Simon Chesterman, *Secret Intelligence,* MAX PLANCK ENC. OF PUB. INT'L LAW 2011, *available at* http://opil.ouplaw.com/oxlaw/search?conr=Chesterman,%20Simon (click on "Secret Intelligence") (Jan. 2009).

23. There are instances where the perpetrator spied, then leaked the intelligence collected, *e.g.* the DNC Hack, *infra*. *See also* April Glaser, *Here's What We Know About Russia and the DNC Hack,* WIRED (Jul. 27, 2016, 9:30 AM), https://www.wired.com/2016/07/heres-know-russia-dnc-hack/.

24. Andrea Peterson, *WikiLeaks Posts Nearly 20,000 Hacked DNC Emails Online,* WASHINGTON POST (July 22, 2016),

Second, there must be a process of "capturing," meaning interception or observation of the data. Third, the data includes, but is not limited to, e-mail traffic, text messages, electronic communications, and non-public digitalized data. The data must be important to some country's national security or interests. The final element is intent – the act must be carried out for political purposes, rather than, for instance, commercial or criminal purposes.[25]

There are additional definitions provided both by official state authorities and cybersecurity scholars. For example, the U.S. Cyber Operations Policy ("PPD-20") terms cyber espionage as "cyber collection," defining it as "operations and related programs or activities conducted . . . in or through cyberspace, for the primary purpose of collecting intelligence . . . from computers, information or communications systems, or networks with the intent to remain undetected."[26]

Herbert Lin, a prominent cybersecurity policy expert, uses the term "cyberexploitation" to denote cyber espionage, defining it as:

> the use of actions and operations – perhaps over an extended period of time – to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks. Cyberexploitations are usually clandestine and conducted with the smallest possible intervention that still allows extraction of the information sought.[27]

Even the U.N. General Assembly expressed concern that "[information] technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States."[28] The General Assembly invited all Member States to inform the Secretary-General as to the "[d]efinition of basic notions related to information security, including unauthorized

---

https://www.washingtonpost.com/news/the-switch/wp/2016/07/22/wikileaks-posts-nearly-20000-hacked-dnc-emails-online/.

25. For a comprehensive analysis of economic cyber espionage, *see* Christina Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV 1165 (2014).

26. Presidential Policy Directive 20, https://fas.org/irp/offdocs/ppd/ppd-20.pdf.

27. Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. OF NAT'L SEC. & POL'Y 63, 63 (2010).

28. G.A. Res. 53/70, at 2 (Jan. 4, 1999).

interference with or misuse of information and telecommunications systems and information resources."[29]

Many additional definitions exist.[30] These definitions, however, do not touch upon the political context in which they occur. In today's geopolitical landscape, context is essential to determine whether and how a specific cyber operation violates international law.

B. The Technology of Cyber Espionage

The technicalities of cyber espionage are essential to the understanding of this new medium of intelligence collection. To carry out a cyber espionage operation (or a cyber-attack operation), a spy or attacker must gain access to the targeted computer. This means that the operation takes place through the use of the Internet (for remote access) or through the use of hardware, such as USB drivers (for close access in air gapped or otherwise isolated networks).[31] Most cyber operations are carried out by accessing and

---

29. *Id.*

30. *See* Katharina Ziolkowski, *Peacetime Cyber Espionage – New Tendencies in Public International Law*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 425, 429 (Katharina Ziolkowski ed., 2013) (proposing the definition of cyber espionage as "the copying of data that is publicly not available and which is in wireless transmission, saved or temporarily available on IT-systems or computer networks located on the territory or area under the exclusive jurisdiction of another State by a State organ, agent, or otherwise attributable to a State, conducted secretly, under disguise or false pretences, and without the (presumed) consent or approval of the owners or operators of the targeted IT systems or computer networks or of the territorial State. Copying includes also the temporary copying of data into the random access or virtual memory of an IT-system for the purpose of mere visualization or acoustic exemplification of (e.g., voice over IP) data. The copying of data saved or temporarily available on IT-systems or computer networks located on the territory or area under exclusive jurisdiction of the copying State is covered by this definition only if the data is protected under public international law"). *See also* THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 193 (Michael N. Schmitt ed., 2013) (providing a cyber espionage definition in an armed conflict context: "any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party."); Irving Lachow, *Cyber Terrorism: Menace or Myth*?, *in* CYBERPOWER AND NAT'L SEC. 437, 440 (Franklin D. Kramer et al. eds., 2009) ("the use of information technology systems and networks to gather information about an organization or a society that is considered secret or confidential without the permission of the holder of the information").

31. Owens et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Booklet, Computer Science and Telecommunications Board 1, 3 (2009),

taking advantage of a vulnerability in a system.[32] An individual carrying out a cyber operation must access such a vulnerability (also known as an "imperfection" or "loophole") within a target's system, then eventually deliver a payload.[33] Hackers can also gain access by using social engineering methods such as spear phishing, that is, targeting a specific user with access privileges within a specific organization.[34]

The payload is a particular malware that is inserted in the target's computer system, which is made possible due to a vulnerability.[35] In other words, it is a deliberate action that is carried out when a vulnerability is exploited, and it can take many forms – such as a destructive virus or a Trojan horse that grants full access to the target computer's system.[36] This process is often referred to as "cyber exploitation,"[37] although certain entities characterize it as a "cyberattack"[38] (though this is not the term used by this article).

The payload is a required component in any sort of cyber operation, be it a cyber-attack with the purpose of disrupting a certain network of computers or cyber espionage with the purpose of obtaining information from the target's computers.[39] In fact, the main difference between cyber espionage and a cyber-attack is the type of malware implanted in the target's computer system.[40] Cyber espionage's payload might be a Trojan horse[41] that collects

---

http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_050541.pdf.

32. NAT'L RES. COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 81 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).

33. *Id.*

34. FBI, *Spear Phishing – Angling to Steal Your Financial Info* (Apr 1, 2009), https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109.

35. *See* MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 18 (2014).

36. NAT'L RES. COUNCIL, *supra* note 32, at 88.

37. *See* Charles Croom, *The Cyber Kill Chain: A Foundation for a New Cyber Security Strategy*, 6(4) HIGH FRONTIER 52, 54 (2010), http://www.sldinfo.com/wp-content/uploads/2012/12/AFD-101019-079.pdf (defining exploitation as "[t]riggering of the attacker's code. Most often, the weapon exploits an application or operating system vulnerability. It might simply exploit the user by persuading him to open an executable attachment, or leverage a feature of the operating system that auto-executes code").

38. NAT'L RES. COUNCIL, *supra* note 32, at 89.

39. Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1184 (2011).

40. *Id.*

41. *See What is a Trojan Virus?*, Kaspersky Lab, http://usa.kaspersky.com/internet-security-center/threats/trojans (Trojans are

information, while cyber-attacks usually use payloads consisting of a worm or virus that disrupts a system's activity,[42] causing it to malfunction or even break down. The technical similarity between cyber espionage and cyber-attacks is one of the complicating factors in the choice of a suitable legal framework applicable to an incident.[43] As one expert aptly observed: "The difference between cybercrime, cyber-espionage, and cyberwar is a couple of keystrokes. The same technique that gets you in to steal money, patented blueprint information, or chemical formulas is the same technique that a nation-state would use to get in and destroy things."[44]

C. Cyberspace, Society, and the State

Cyber espionage, and cyberspace activities in general, occur in a specific technological trend. The information revolution, a phenomenon that incrementally disseminated the use of information and communication technologies (ICTs),[45] sparked the trend of nations becoming increasingly dependent upon cyber infrastructure in their day-to-day activities.[46] Computer systems now appear in business activities, vehicles, air traffic control, the energy sector, and more.[47] As a result, any vulnerability in the critical infrastructures that allows hostile cyber operations can be immensely harmful and detrimental to the functioning of the state.[48]

Apart from the growing national dependency on information and communication technologies, it is essential to take into account

---

malicious programs that perform actions that have not been authorized by the user. "These actions can include: [d]eleting data, [b]locking data, [m]odifying data, [c]opying data[,] [and] [d]isrupting the performance of computers or computer networks[.] Unlike computer viruses and worms, Trojans are not able to self-replicate.").

42. Williams, *supra note 40*, p. 1184.

43. *Id.*

44. Tom Gjelten, *Cyber Insecurity: U.S. Struggles to Confront Threat*, NPR (Apr. 6, 2010, 12:00 AM), http://www.npr.org/templates/story/story.php?storyId=125578576.

45. *See* Mariarosaria Taddeo, *An Analysis for A Just Cyber Warfare*, *in* 4th INT'L CONF. ON CYBER CONFLICT 209, 210 (Katharina Ziolkowski et al. eds., 2012).

46. *See* HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 12 (2012).

47. *See* PHILIP HARRIS, DEVELOPING HIGH PERFORMANCE LEADERS: A BEHAVIORAL SCIENCE GUIDE FOR THE KNOWLEDGE OF WORK CULTURE 85 (2012).

48. *See* DAVE CLEMENTE, CYBER SECURITY AND GLOBAL INTERDEPENDENCE: WHAT IS CRITICAL? 7 (2013).

the fact that computer systems are massively interconnected, rather than isolated.[49] A particular computer system exchanges traffic regularly with other computers globally, thereby relying on the proper functioning of other computer systems. If a computer on a network fails to operate, it could create a ripple effect with tremendous negative consequences.[50] Such interconnectedness is a universal phenomenon, suggesting that one disrupted critical computer system may affect other, dependent computer systems.[51]

Warfare itself is also changing. If traditional warfare implied military forces clashing directly or indirectly via kinetic weapons, modern warfare implies subtler, less "forceful" methods. Cyber warfare represents this new variety. A study on cyber warfare suggested that it includes "(1) web vandalism, (2) disinformation campaigns, (3) gathering secret data, (4) disruption in the field and (5) attacks on critical national infrastructure."[52] With the possible exception of (5), this list indicates that warfare has shifted from "hard" warfare to "soft" warfare. In today's warfare, the spread of disinformation over the Internet can be used as a strategic tool between conflicting states, not just the physical destruction of military targets. This is sometimes referred to as the "weaponization of information."[53]

That is not to say that "soft" warfare is less serious or threatening than the "hard" warfare of the past. Many would agree that the value of data surpasses the value of physical devices. For example, the contact information, text messages, and photos on an

---

49. *See* Jorge L. Contreras et al., *Mapping Today's Cybersecurity Landscape*, 62 AM. U. L. REV. 1113, 1117 (2013).

50. Jack Goldsmith, *The Persuasive General Alexander, and Why Critical Infrastructure Protection Regulation is... Critical*, LAWFARE (May 10, 2012, 9:30 AM), http://www.lawfareblog.com/2012/05/the-persuasive-general-alexander-and-why-critical-infrastructure-protection-regulation-is-critical/ (citing Michael Chertoff: "[I]n an interconnected and interdependent world, the failure of one part of the network can have devastating collateral and cascading effects across a wide range of physical, economic and social systems.").

51. Ray Rothrock, *The Cybersecurity Domino Effect*, INFO SECURITY (Dec. 30, 2015), http://www.Infosecurity-Magazine.Com/Opinions/The-Cybersecurity-Domino-Effect/.

52. Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors,* 89 INT'L L. STUD. 406, 435-6 (2013) (citing *Special Focus: Cyberwarfare*, CTR. FOR THE STUDY OF TECH. & SOC'Y (2016), http://www.libertyparkusafd.org/Hale/Special%20Reports%5CNational%20Security%20Agency%5CSpecial%20Focus%20on%20Cyberwarfare.htm).

53. Peter Pomerantsev & Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money,* THE INTERPRETER (2014), http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf.

average smartphone are likely more valuable than the hardware to the phone's owner. Because data is more valuable than its physical counterparts, international law should adapt to protect data for the sake of its intrinsic societal value. International law has not yet adapted to this reality, however, and cyber espionage keeps occurring due to the misconception that it is an extension of traditional espionage.

These tendencies and recent cyber incidents have motivated states to increase cyberspace militarization efforts.[54] The U.S., Russia, China, Israel, and France are at the top of the competition as the main cyber espionage perpetrators.[55] Surprisingly, countries such as Iran,[56] North Korea[57] and Belarus[58] have also emerged as significant cyber powers considered to have cyber offensive capabilities.

Unlike traditional espionage, which primarily occurs in the territory of the state being spied upon,[59] cyber espionage is not geographically limited. It frequently takes place remotely and instantaneously.[60] It also enables massive infiltrations of information that would be impossible using traditional methods of espionage.[61] These characteristics complicate effective deterrence against

---

54. *See generally*, Myriam Dunn Cavelty, *The Militarization of Cyberspace: Why Less May be Better*, 4th INT'L CONF. ON CYBER CONFLICT 141, 141 (Katharina Ziolkowski et al. eds., 2012).

55. Nick Kosturos, *The Emerging Threat of Cyber Espionage Against U.S. Economic Interests*, SCIR (June 26, 2013), http://scir.org/2013/06/the-emerging-threat-of-cyber-espionage-against-us-economic-interests/.

56. Eric Shafa, *Iran's Emergence as a Cyber Power*, STRATEGIC STUDIES INST. (Aug. 20, 2014), http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20.

57. Associated Press in South Korea, *North Korea has 6,000-strong cyber-army, says South*, THE GUARDIAN (Jan. 6, 2015, 9:00 AM), http://www.theguardian.com/world/2015/jan/06/north-korea-6000-strong-cyber-army-south-korea.

58. Intel Security, *Hacking Summit Names Nations with Cyberwarfare Capabilities*, MCAFEE (Oct. 3, 2013), https://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities.

59. *See* Roger D. Scott, Note & Comment, *Territorially Intrusive Intelligence Collection and International Law*, 46 A. F. L. REV. 217, 219 (1999).

60. *See* Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors,* 89 INT'L L. STUD. 406, 419 (2013); GEORG KERSCHISCHNIG, CYBERTHREATS AND INTERNATIONAL LAW 9 (2012).

61. Ido Kilovaty, *The Democratic National Committee Hack: Information as Interference,* JUST SECURITY (Aug. 1, 2016, 10:53 AM), https://www.justsecurity.org/32206/democratic-national-committee-hack-information-interference.

espionage because spies are no longer present in the territory of the spied state, making cyber espionage more appealing than traditional espionage to some.[62]

To better understand how cyber espionage occurs in the real world, this article will next analyze cases of peacetime cyber espionage activities, namely, the *DNC Hack, GhostNet, Shady Rat* and *Flame.*

1. The DNC Hack

In July 2016, WikiLeaks released nearly 20,000 e-mails belonging to Democratic National Committee's top officials, in which the officials humiliated and criticized Senator Bernie Sanders. These e-mails strengthened Sanders supporters' charge that the Democratic Party favored Secretary Hillary Clinton.[63] Robby Mook, the campaign chief for Clinton, suggested that Russia was behind the hack "for the purpose of helping Donald Trump."[64] Many other cybersecurity experts pointed the finger at Russia, and even the US government itself acknowledged that it believed Russia to be behind the DNC hack.[65] This is not the first time that sensitive e-mails have been leaked to the public with the intent to intervene in international politics. Almost two weeks before the DNC hack, WikiLeaks published nearly 300,000 e-mails belonging to Turkish President

---

62. Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage, in* INT'L CYBER NORMS: LEGAL, POL'Y & INDUS. PERSPECTIVES 65, 66 (Anna-Maria Osula & Henry Roigas eds., 2016) ("[T]he exploitation of cyberspace for the purpose of espionage has emerged as a particularly attractive method to acquire confidential information because of the large amount of information that is now stored in cyberspace and because cyberspace affords a considerable degree of anonymity to perpetrators of espionage and is thus a relatively risk free enterprise.").

63. Theodore Schleifer & Eugene Scott, *What Was in the DNC Email Leak?*, CNN (July 25, 2016, 12:38 PM), http://www.cnn.com/2016/07/24/politics/dnc-email-leak-wikileaks/.

64. Tom Hamburger & Ellen Nakashima, *Clinton Campaign – And Some Cyber Experts – Say Russia Is Behind Email Release*, WASH. POST (July 24, 2016), https://www.washingtonpost.com/politics/clinton-campaign–and-some-cyber-experts–say-russia-is-behind-email-release/2016/07/24/5b5428e6-51a8-11e6-bbf5-957ad17b4385_story.html.

65. Spencer Ackerman & Sam Thielman, *US Officially Accuses Russia of Hacking DNC and Interfering with Election*, THE GUARDIAN (Oct. 8, 2016, 9:09 PM), https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election.

Recep Tayyip Erdogan's political party following the failed coup against him.[66]

There are three important and novel details about the DNC hack. First, it was comprised of an immense volume of data exfiltration. As many as 20,000 e-mails were collected, allegedly by Russia, a volume unimaginable using traditional espionage methods. Second, the hackers apparently intended to influence the U.S. presidential election for their own ends. Third, the information collected in the DNC hack was leaked, meaning that Russia deliberately distributed it and made it public.

2. GhostNet

GhostNet was a Trojan horse that primarily targeted governments in South and Southeast Asia, but was found in 103 countries.[67] One-third of the 1,295 computers it infected were characterized as sensitive computers at ministries, embassies and international organizations.[68] The Munk Center for International Studies at the University of Toronto investigated GhostNet at the request of the office of the Dalai Lama, the Tibetan leader.[69]

The perpetrators obtained contact and other information from the infected computers, which helped spread the Trojan horse through e-mails that appeared to be from reliable senders.[70] GhostNet was a covert, hard-to-detect espionage system, which gained full control of infected computer systems.[71]

The Information Warfare Report claims that the identities and motives of the perpetrators are still unknown; however, China has been improving its cyberspace capabilities tremendously during the last two decades[72] with the main purpose of bolstering its position in

---

66. Andy Greenberg, *Wikileaks Dumps 'Erdogan Emails' After Turkey's Failed Coup*, WIRED (July 19, 2016, 5:59 PM), https://www.wired.com/2016/07/wikileaks-dumps-erdogan-emails-turkeys-failed-coup/.

67. *Id.*

68. Jon Skillings, *Malware Probes Find a China Angle*, CNET (Apr. 8, 2009, 6:48 AM), http://www.cnet.com/news/malware-probes-find-a-china-angle/.

69. Richard Koman, *Massive Chinese Spynet Targeted Dalai Lama*, ZDNET (Mar. 29, 2009, 9:33 PM), http://www.zdnet.com/article/massive-chinese-spynet-targeted-dalai-lama/.

70. *Tracking* GhostNet*: Investigating a Cyber Espionage Network,* INFO. WARFARE MONITOR at 6 (2009), http://www.nartv.org/mirror/ghostnet.pdf.

71. *Id.*

72. *Id.*, at 11. *See also* MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (Feb. 19, 2013),

the global political and economic order.[73] In fact, the involvement of the Chinese government was established in another report, which investigated the intrusions to the office of the Dalai Lama.[74] The Chinese government denied its involvement in the GhostNet incident.[75]

While GhostNet was used primarily for the purpose of obtaining intelligence, the Trojan Horse mechanism provided full control over infected computers. GhostNet could disrupt the proper functionality of the infected computers and manipulate resident information within these systems. GhostNet is an example of how cyber espionage and cyber-attacks are similar in many ways, and it demonstrates how difficult it is to distinguish between the two in real time.

3. Shady Rat

The methods of operation in *Shady Rat* were quite astounding. *Shady Rat*'s malicious code was hidden inside digital images, e-mailed to various targets, and eventually triggered the installation of a Trojan horse.[76] The specific commands were invisible to the computer user,[77] and many firewalls did not stop its installation, particularly because firewalls are often configured to allow image files to pass as part of HTTP traffic.[78] After its installation, the Trojan horse allowed the attackers to remotely command the infected computers.[79]

---

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

73. Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage, in* INT'L CYBER NORMS: LEGAL, POL'Y & INDUS. PERSPECTIVES 65, 66 (Anna-Maria Osula & Henry Roigas eds., 2016).

74. SHISHIR NAGARAJA & ROSS ANDERSON, THE SNOOPING DRAGON: SOCIAL-MALWARE SURVEILLANCE OF THE TIBETAN MOVEMENT (2009), http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf.

75. Seth Jacobson, *China Denies Involvement in GhostNet Cyber-Attacks,* THE WEEK (Mar. 31, 2009), http://www.theweek.co.uk/politics/24131/china-denies-involvement-ghostnet-cyber-attacks.

76. The method of concealing a code within another file is called "steganography." *See* Kelly Jackson Higgins, *'Operation Shady RAT" Attackers Employed Steganography*, INFO. WEEK (Aug. 11, 2011, 2:42 PM), www.darkreading.com/attacks-breaches/operation-shady-rat-attackers-employed-steganography/d/d-id/1136162.

77. *Id.*

78. Brian Prince, *Digging Deeper into Operation Shady RAT,* SEC. WEEK (Aug. 8 2011), http://www.securityweek.com/digging-deeper-operation-shady-rat/.

79. Hon Lau, *The Truth Behind the Shady RAT*, SYMANTEC (Aug. 4 2011), http://www.symantec.com/connect/blogs/truth-behind-shady-rat.

At least one leading cybersecurity expert has publicly claimed that China is behind *Shady Rat*,[80] however, some other experts were not as specific, and only claimed that there is a state actor behind *Shady Rat* without naming any state.[81] China is viewed as the actor behind this espionage operation mainly because targets had information valuable to Beijing.[82] China itself did not comment on the allegations.[83]

4. Flame

It is unclear when *Flame* started operating, but it was first reported in 2010, and "circumstantial evidence" suggests that it began as early as 2007.[84] The main targets of *Flame* were Middle Eastern countries, including Iran, which had the highest number of infected computer systems, followed by Israel, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt.[85]

Flame was so complex and advanced that experts believe a state must be behind the worm, either directly or otherwise.[86] Some allege that the United States and Israel are behind *Flame*,[87] because they

---

80. *See* Michael Gross, *Exclusive: Operation Shady Rat—Unprecedented Cyber Espionage Campaign and Intellectual Property Bonanza*, VANITY FAIR (Aug. 2 2011), http://www.vanityfair.com/news/2011/09/operation-shady-rat-201109 (citing the claim of James Lewis, Director of Technology and Public Policy at the Center for Strategic and International Studies that "All signs point to China. . . who else spies on Taiwan?").

81. Jim Finkle, "*State Actor" Behind Slew of Cyber-attacks*, REUTERS (Aug. 3 2011), http://www.reuters.com/article/2011/08/03/us-cyberattacks-idUSTRE7720HU20110803.

82. *Id.*

83. *Id.*

84. Elinor Mills, *Behind the 'Flame' Malware Spying on Mideast Computers (FAQ)*, CNET (June 4, 2012), http://www.cnet.com/news/behind-the-flame-malware-spying-on-mideast-computers-faq (quoting Roel Schouwenberg, Senior Researcher at Kaspersky).

85. *Id.*

86. *Id.*

87. *See Flame virus: who is behind the world's most complicated espionage software*, THE TELEGRAPH (May 29, 2012), http://www.telegraph.co.uk/technology/news/9296827/Flame-virus-who-is-behind-the-worlds-most-complicated-espionage-software.html ("Given the pattern of the Flame infection known so far - Iran, the West Bank, Syria, Egypt - and its technological prowess, Israel has quickly emerged as many commentators' prime suspect. Richard Silverstein, a US-based commentator and critic of the Israeli government, has made widely-shared claims that "my senior Israeli source confirms that it is a product of Israeli cyberwarfare experts." The *Jerusalem Post* thinks Vice President Ya'alon may even have already hinted Israel is behind Flame.). *See also* Will Oremus, *Obama's Flame Wars*, SLATE (June 19, 2012),

previously used another, similar worm called *Stuxnet* to target Iran's cyber infrastructure.[88] However, the United States and Israel never assumed responsibility for *Flame,* and, unlike *Stuxnet*, *Flame* did not distribute itself automatically to other computers – its distribution was limited.[89] Additionally, if the allegations regarding the identity of the perpetrators are true, then there is much more space and incentives for cooperation between states than initially imagined.

D. The DNC Hack, GhostNet, Shady Rat and Flame – Different Operations, Same Story

All four espionage operations collected information from sensitive computer systems and were able to operate for a prolonged period of time before they were discovered and treated. As viruses, worms, and Trojan horses become more sophisticated and evasive every day, it is increasingly challenging to respond to them efficiently and promptly in real time, particularly when these operations exploit a "zero day vulnerability."[90]

Moreover, all four espionage operations were allegedly carried out by state actors, which demonstrates that states are deeply involved in intelligence gathering for national security purposes. Cyber espionage for the purposes of national security is far more hostile than the collection of trade secrets because while trade secrets are usually relevant only to commercial competition, snooping for military secrets suggests intent beyond mere spying. For instance, cyber spies may collect information in preparation for future conflicts, including armed conflict. The U.S. government itself recognizes that distinction, but reached a different conclusion than the one presented in this article, namely that national security-related espionage is legitimate, while commercial cyber espionage is not.[91]

---

http://www.slate.com/blogs/future_tense/2012/06/19/flame_virus_us_israel_created_worm_used_in_iran_cyberattack.html.

88. Ellen Nakashima and Joby Warrick, *Stuxnet was work of U.S. and Israeli Experts, Officials Say*, THE WASHINGTON POST (June 2, 2012), www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

89. Kim Zetter, *Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers*, WIRED (May 28, 2012), http://www.wired.com/2012/05/flame/all/.

90. "Zero day vulnerability" means that the gap between the time when the software was unknown and the time the exploit occurred is zero, meaning that the exploit is the first of its kind and cannot be treated immediately in most cases.

91. "The U.S. government makes a distinction between intelligence operations for national security purposes and government sponsored cyber-espionage for commercial gain. The United States has acknowledged that it undertakes the first, which it says is legitimate, and has accused China of doing

This distinction calls for a comprehensive analysis of current international law norms and principles, and whether such norms are effective at regulating inter-state cyber espionage.

III. PEACETIME ESPIONAGE AND INTERNATIONAL LAW – IS THERE A DEFINITIVE ANSWER?

A. The Legality Argument

While the laws of armed conflict address wartime espionage,[92] peacetime espionage has not received explicit attention from any area of international law.[93] Judging from Grotius' landmark *De Jure Belli Ac Pacis,* wartime espionage is "beyond doubt permitted by the law of nations."[94] It is unclear, however, whether such a decisive assertion would apply to peacetime espionage. Espionage is permissible during armed conflict because of the reduced respect for sovereignty and territorial integrity.[95] Interestingly, the Additional Protocol I to the Geneva Convention provides that a spy

---

also the second, which it considers illegitimate. But the information theft from the OPM seems to fit the first category more than the second." Frans Paul van der Putten & Sico van der Meer, *Deterring cyber-espionage requires a more intelligent US approach*, EAST ASIA FORUM (Oct 13, 2015), http://www.eastasiaforum.org/2015/10/13/deterring-cyber-espionage-requires-a-more-intelligent-us-approach.

92. *See* Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations Concerning the Laws and Customs of War on Land art. 24, 29-31, 18 October 1907 (Article 24: "Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible"). *See also* Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 46, 8 June 1977; ICRC Customary IHL Study, *Rule 107 on Spies*, *available at* https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule107.

93. "[P]eacetime espionage has always been seen as an issue of domestic law, even though an international event is obviously involved." Demarest, *supra* note 16, at 330.

94. HUGO GROTIUS, THE LAW OF WAR AND PEACE, BOOK III, ch. IV xviii 655 (1625) ("[S]pies, whose sending is beyond doubt permitted by the law of nations - such as the spies whom Moses sent out, or Joshua himself - if caught are usually treated most severely. "It is customary," says Appian, "to kill spies." Sometimes they are treated with justice by those who clearly have a just case for carrying on war; by others, however, they are dealt with in accordance with that impunity which the law of war accords. If any are to be found who refuse to make use of the help of spies, when it is offered to them, their refusal must be attributed to their loftiness of mind and confidence in their power to act openly, not to their view of what is just or unjust.").

95. Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW (DATE) 12.

in an armed conflict shall be treated as a prisoner of war if he or she was in a uniform of the armed forces while engaging in espionage.[96] In addition, a member of the armed forces who engaged in espionage is untouchable once he rejoins his armed forces upon completion of his mission.[97] However, the analogy of rejoining the armed forces in a cyber espionage setting is unclear because cyber spies need not leave the safety of their own territory in the first place.

In contrast, most of the scholarship on peacetime espionage focuses on general applications of international legal norms that constrain inter-state activities.[98] Indeed, most jurisdictions prohibit and prosecute acts of espionage, mainly to discourage such acts and to create a price for undertaking them.[99] However, domestic prohibitions of espionage, even as widespread as they are, do not create a violation under public international law.[100]

The main legality argument contends that international law simply does not ban the use of espionage in inter-state relations.[101] In fact, the argument goes even further – peacetime espionage is inherent to the function of a state, and it has been used massively throughout history, up to the point that peacetime espionage has become part of a consistent state practice.[102] In Kurt Singer's clever words: "[T]here has never been a war without spies, and there never has been a peace in which spies have not engaged in preparations for a future war."[103]

Another argument is more responsive to the illegality argument discussed below. The legality of peacetime espionage, according to this argument, is based on the right of anticipatory or preemptive

---

96. 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 art. 46 ¶ 2.

97. *Id.* at art. 46 ¶ 4.

98. *See* Williams, *supra* note 40.

99. Chesterman, *supra* note 10, at 1077.

100. *Id.*

101. "Espionage is not prohibited by international law as a fundamentally wrongful activity; it does not violate a principle of *jus cogens*." *See* Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 218 (1999).

102. Jeffrey H. Smith, *Keynote Address* 28 MICH. J. INT'L. L. 543, 544.

103. Richard A. Falk, *Foreword* to ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at v (Roland J. Stranger ed., 1962) (quoting Kurt D. Singer, THREE THOUSAND YEARS OF ESPIONAGE: AN ANTHROPOLOGY OF THE WORLD'S GREATEST SPY STORIES vii (1948)).

self-defense frameworks.[104] These frameworks represent a broad interpretation of the right to self-defense.[105] States conduct peacetime espionage operations to collect intelligence, potentially about an imminent armed attack against the spying state, therefore enhancing the spying state's ability to prepare for self-defense actions and safeguard its national security.[106]

This justification was used in the 1960 "U-2 incident", when an American U-2 spy plane was shot down while conducting espionage over the Soviet Union.[107] The then-Secretary of State defended the operation by saying that "the Government of the United States would be derelict to its responsibility not only to the American people but to free peoples everywhere if it did not, in the absence of Soviet cooperation, take such measures as are possible unilaterally to lessen and to overcome this danger of surprise attack."[108] From 1950 to 1969, at least 22 aircraft suspected of spying were shot down, mostly by the U.S.S.R.[109] It is important to note that arguments for preemptive self-defense are often dismissed as inconsistent with Article 51 of the UN Charter, which limits the inherent right of self-defense to only apply "if an armed attack occurs."[110] The right to preemptive self-defense was, for example, debated in relation to the 2003 U.S. invasion of Iraq.[111] Anticipatory self-defense is generally more accepted when an armed attack is imminent, meaning that it is almost certain that the armed attack will occur. In other words, the difference between "preemptive" and "anticipatory" is mainly a question of imminence, which is required to justify self-defense measures.[112]

---

104. Alexander Melnitzky, *Defending America against Chinese Cyber Espionage Though the Use of Active Defenses* 20 CARDOZO J. OF INT'L & COMP. L. 538, 564 (2012).

105. Baker, *supra* note 13, at 1095.

106. *Id.*

107. Wright, *supra* note 96, at 17-18.

108. HALFORD RYAN, ORATORICAL ENCOUNTERS: SELECTED STUDIES AND SOURCES OF TWENTIETH-CENTURY POLITICAL ACCUSATIONS AND APOLOGIES (CONTRIBUTIONS TO THE STUDY OF MASS MEDIA AND COMMUNICATIONS) (1988), p. 144.

109. THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE, 352 (2000).

110. *See* U.N. Charter art. 51.

111. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 604 (2007).

112. Byard Q. Clemmons & Gary D. Brown, *Rethinking International Self-Defense: the United Nations' Emerging Role*, 45 NAVAL L. REV., 217, 228 (1998). An imminent attack is "fairly inferable" under the circumstances.

States have often used new technologies for espionage purposes. Two relevant domains in which technology allowed for espionage are the sea and outer space.[113] Resorting to a different body of international law, maritime law, might assist in determining whether international law prohibits cyber espionage. As an analogy, Article 19(2)(c) of United Nations Convention on the Law of the Sea (UNCLOS)[114] provides that "any act aimed at collecting information" would be "prejudicial to the peace, good order or security of the coastal State."[115] This prohibition extends only to the twelve nautical miles of territorial sea of the coastal state, meaning that spying is only legitimate when it takes place more than 12 miles away from the target state, which suggests that cyber espionage is similarly permissible due to its remoteness.[116] Similarly, the Outer Space Treaty, which provides that the Outer Space is not subject to "national appropriation by claim of sovereignty", does not prohibit the use of satellites for intelligence collection purposes.[117]

Oftentimes the legality argument is also based on the 1961 Vienna Convention on Diplomatic Relations (VCDR), which, according to a prominent information warfare expert, "explicitly recognizes the well-established right of nations to engage in

---

113. *See* Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage, in* INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES, 65, 66 (2016), https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch4.pdf. ("States have, however, exploited technological developments in order to devise more effective methods through which to conduct espionage. Since the emergence of vessels, aeroplanes and celestial bodies, the sea, the skies and outer space have all been used as platforms to engage in (often electronic) surveillance of adversaries; that is, to commit espionage from afar.")

114. Williams, *supra note 40*, at 1176.

115. Article 19(2)(c) of the United Nations Convention on the Law of the Sea, opened for signature Dec. 10, 1982, 1833 U.N.T.S. 397, http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf. The Article provides that "Passage of a foreign ship shall be considered to be prejudicial to the peace, good order or security of the coastal State if in the territorial sea it engages in any of the following activities: . . . (c) any act aimed at collecting information to the prejudice of the defense or security of the coastal State".

116. *Id.* at 23. Article 3 of UNCLOS provides that "Every State has the right to establish the breadth of its territorial sea up to a limit not exceeding 12 nautical miles, measured from baselines determined in accordance with this Convention".

117. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205, http://www.unoosa.org/pdf/publications/ST_SPACE_061Rev01E.pdf. *See also* Williams, *supra note 40*, at 1176.

espionage during peacetime."[118] Since both the VCDR and the customary international law pertaining to diplomatic relations grant immunity to diplomats, the risks of espionage are lowered since states are incentivized to collect information through their diplomatic missions.[119] This risk decrease is associated with spying diplomats who will be declared *persona non grata* and expelled while regular spies will be prosecuted and punished with accordance to the criminal law in the spied state legal system.[120]

As it relates to cyber espionage, there are no cyber-treaty or universal cyber norms that permit or prohibit the use of cyber espionage for inter-state intelligence collection. Because international law is a legal system that requires a breach of definitive norms to assume state responsibility, it appears that cyber espionage is legal, unless expressly prohibited in the future.[121]

B. The Illegality Argument

Some experts believe that peacetime espionage operations interfere with the principle of sovereignty.[122] Specifically, this refers to territorial sovereignty, which guarantees nations protection from physical intrusions.[123] Those who view peacetime espionage as the most severe of inter-state activities argue that these are proscribed "uses of force" within the meaning of Article 2(4) of the U.N. Charter.[124] This argument focuses on peacetime espionage being "against the *territorial integrity* or *political independence*"[125] of a

---

118. WINGFIELD, *supra* note 110, at 350 ("The practice of states has specifically recognized a right to engage in such clandestine intelligence collection activities as an inherent part of foreign relations and policy."). *See also* WALTER SHARP, CYBERSPACE AND THE USE OF FORCE 123 (1999).

119. Radsan, *supra* note 112, at 595, 598-599.

120. SHARP, *supra* note 119, at 126.

121. *See e.g.*, G.A. Res. 56, Supplement No. 10 (A/56/10) Report of the International Law Commission Chapter II on Countermeasures of the Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001). Art. 2 of G.A. Res. 56 notes that "There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State."

122. Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L. SEC. L. & POL'Y. 180, 198 (2011).

123. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. Rep 4, ¶35 (Apr. 9).

124. U.N. Charter art. 2 ¶4. Article 2(4) of the UN Charter reads: "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 Nations."

125. Wright, *supra* note 96, at 12 (emphasis added).

state, given its intrusive nature.[126] Additionally, espionage preceding an armed attack could be regarded as a threat to use force.[127] In contrast, it is argued that the prohibition on the use of force was not intended to limit non-forceful inter-state operations.[128] A softer version of this argument simply holds that peacetime espionage would be a violation of the norm of peaceful cooperation between states.[129]

One caveat to the use of force argument is that its invocation has traditionally required kinetic effects comparable to military force.[130] Therefore, cyber espionage alone does not qualify.[131] However, in certain circumstances, cyber espionage could constitute a *threat* to use force.[132]

Although not all peacetime espionage operations cause kinetic consequences that qualify as "forceful," peacetime espionage could arguably violate the customary principle of non-intervention.[133] The

---

126. Ziolkowski, *supra* note 30, at 432.

127. Forcese, *supra* note 123, at 198.

128. Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 628 (2007).

129. Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. IN'L. L. 53, 67 (1984). Delupis writes, "espionage appears to be illegal under international law in time of peace if it involves the presence of agents sent clandestinely by a foreign power into the territory of another state. Such operations offend the principle of peaceful cooperation of states."

130. Michael Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, *in* 4th INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283, 288 (Katharina Ziolkowski et al. eds., 2012). *See also* Ziolkowski, *supra* note 30, at 451.

131. BRUNO SIMMA, THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 210 (2nd ed. 2002).

132. *See* Anna Wortham, *Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force*?, 64 FED. COMM. L. J. 643, 656 (2012).

133. *See Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua v. United States*), Judgment, 1986 I.C.J Rep 14, ¶ 205 (June 27, 1986). The Court provided that "a prohibited intervention must be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely (for example the choice of a political, economic, social and cultural system, and formulation of foreign policy). Intervention is wrongful when it uses, in regard to such choices, methods of coercion, particularly force, either in the direct form of military action or in the indirect form of support for subversive activities in another State". *See also* Michael Wood, *The Principle of Non-Intervention in Contemporary International Law: Non-Interference in a State's Internal Affair Used to be a Rule of International Law: Is It Still?*, CHATHAM HOUSE (Feb. 28, 2007), https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/il280207.pdf.

principle of non-intervention is based on the idea of sovereign equality, as suggested by Article 2(7) of the U.N. Charter: "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state."[134] The U.N. General Assembly also provided its own strict view of the principle of non-intervention in its landmark Declaration on Friendly Relations and Co-operation Among States.[135] It was later reaffirmed in the General Assembly's Declaration on the Inadmissibility of Intervention.[136]

Espionage might indeed constitute a prohibited form of intervention; however, in most cases peacetime espionage would lack the "coercive" factor.[137] Covert espionage operation might be so well concealed that it will not have any tangible effects on the spied-upon state.[138]

Finally, some consider espionage to be a violation of territorial sovereignty.[139] The landmark *Lotus* decision by the Permanent Court of International Justice laid down the fundamental principle that, in the absence of an explicit international law prohibition of a specific conduct, "every State remains free to adopt the principles which it regards best and most suitable."[140] Espionage was usually carried out by the physical presence of the spies or spying tools

---

134. *See* U.N. Charter art. 2 ¶ 7.

135. G.A. Res. 2625 (XXV), Declaration on the Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970). G.A. Res. 2625 provided that "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law."

136. G.A. Res. 36/103, art. 1 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States (Dec. 9, 1981).

137. Anne Peters, *Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon*, Part I, Blog of the European Journal of International Law (Nov. 1, 2013), http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i.

138. Gerald O'Hara, *Cyber Espionage: A Growing Threat to the American Economy,* 19 COMMLAW CONSPECTUS 241, 243 (2010), citing Scott Charney at Corporate and Industrial Espionage and Their Effects on American Competitiveness: Hearing Before the Subcomm. on Int'l Econ. Pol'y & Trade of the H. Comm. on Int'l Relations, 106th Cong. 180 (2000) ("If I [physically] steal your car, you know because it is gone, but if I steal your customer list or a design plan . . . you will not know that I have it, and you will remain comfortable.").

139. Ziolkowski, *supra* note 30, at 457.

140. *See* S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, ¶ 46 (Sept. 7).

within the land, airspace or territorial sea of the spied state.[141] It is unclear, however, whether electronic intrusion could be equated with physical intrusion and invasion.[142]

According to the illegality argument, peacetime cyber espionage would be a violation of international law. But as will be discussed in this article, cyber espionage's novelty calls for a new approach.

C. Reconciling the Legal and Illegal Arguments – Is There an Explicit Answer?

It is difficult to conclude whether espionage is *clearly* legal or illegal under international law. Both arguments have merit, and due to the lack of explicit black letter law on the matter, it would be neither possible nor wise for this article to adopt either stance. Therefore, this article will address the legality of *cyber espionage* in relation to the context in which it occurs.

IV. PEACETIME CYBER ESPIONAGE – A CALL FOR A NEW APPROACH?

Five characteristics distinguish cyber espionage from traditional espionage. First, cyber espionage is highly efficient, since it allows access to massive amounts of data, which was not achievable under traditional espionage means.[143] While espionage in the traditional sense was limited in scope, cyber espionage offers access to databases that contain tremendous amount of data and metadata. This makes cyber espionage more efficient than traditional espionage. Additionally, growing national dependency on cyber infrastructure and the information stored within makes cyber espionage a tempting course of action for states.[144] One expert goes so far as to claim that the type of massive intelligence collection

---

141. Ziolkowski, *supra* note 30, at, 457.

142. *Ibid*. *See also* DEPARTMENT OF DEFENSE GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (1999), http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf ("It seems beyond doubt that any unauthorized intrusion into a nation's computer systems would justify that nation at least in taking self-help actions to expel the intruder and to secure the system against reentry. An unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory, but such issues have yet to be addressed in the international.").

143. Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUR. J. INT'L L. 129, 135 (2013).

144. Ziolkowski, *supra* note 30, at 463.

cyber espionage enables was previously only possible with military occupation.[145] Today, it seems, the cyberspace contains unprecedented amounts of information.[146] Although not a clear example of cyber espionage, the case of CIA's whistleblower Edward Snowden demonstrates how massive amounts of data are easily accessible through the use of computers and how easy it is to publicly circulate this data through the Internet.[147] Snowden's leak could not have been achieved without the use of computer systems and the Internet, which allowed the exfiltration of an immense volume of data. Incidents like the Snowden leaks never happened before the emergence of, and massive reliance on, information and communication technologies.

Second, due to its similarity to cyber-attacks in the method of operation, it is difficult to distinguish in real time between cyber espionage, which does not end up with kinetic consequences, and cyber-attacks, which tend to have disruptive, kinetic effects.[148] Cyber espionage operations require the same active hacking tools that cyber-attacks do, and from the victim's perspective, distinguishing between the two may be perplexing.[149] Both cyber espionage operations and cyber-attacks are computer exploitations that take advantage of vulnerabilities in computer systems, or gain unauthorized access to the system. The only technical difference between the two is in the character of the payload.[150]

---

145. Melnitzky, *supra* note 105, at 566.

146. SHARP, *supra* note 119, at 127. ("Here is perhaps no richer source of information than what can potentially be accessed via the Internet.").

147. Mark Mazzetti & Michael Schmitt, *Ex-Worker at C.I.A. Says he Leaked Data on Surveillance*, N.Y. TIMES, June 9, 2013, http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html.

148. *Goldsmith*, *supra* note 144, at 135.

149. Bruce Schneier, *There's No Real Difference Between Online Espionage and Online Attack*, The Atlantic (Mar. 6, 2014), http://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/.

150. For an apt analogy demonstrating this point, *see* Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, STRATEGIC STUDIES QUARTERLY Fall 2012, at 126, 134-5: "[T]here are important differences between cyber espionage and more traditional means of spying. Surreptitiously entering a foreign country and leaving behind a sensor to collect and transmit intelligence data is one thing. But what if that sensor also contained a powerful explosive that could be detonated from a distance, causing grave destruction? If a government discovered such a device, it would be classified as a weapon of war; that would subsume any thought that it might have been placed during an espionage activity. This second scenario is perhaps more akin to some current cyber espionage techniques. Network accesses and cyber spying capabilities may be just as capable

Third, while traditional espionage was criminalized in most legal systems, prosecuted in the territory of the spied state, and punished heavily, cyber espionage is carried out remotely, so it is difficult to prosecute and punish perpetrators (the "deterrence problem").[151] However, deterrence is not only difficult due to the remoteness, but also due to the anonymity that characterizes many cyber incidents.[152]

Fourth, cyber espionage provides easy access not only to superpowers' computer systems, but also to those of small states and non-state actors, such as hacktivist groups and armed militias.[153] The recent pro-Islamic State cyber-attacks against 19,000 French websites showcase the ease of access to cyber espionage and cyber-attack tools by armed groups.[154] It is believed that over 120 countries in 1996 possessed the capabilities of carrying out computer attacks at this level.[155] All of those distinguishing factors pose a great threat to national security and set cyber espionage apart from traditional espionage.[156] Cyber espionage does not make weaker states or non-state actors superior to traditionally powerful states, but it is definitely narrowing the gap in military power between states.

Fifth, cyber espionage enables the leaking of collected intelligence, as the world recently witnessed in the DNC hack and other similar operations.[157] This type of transformation makes cyber

---

of being used for disruption of systems or deletion of data. The cyber victim may be left to wonder whether the rogue code it discovers on its network is a tool meant for espionage or attack."

151. Ziolkowski, *supra* note 30, at 447.

152. SHARP, *supra* note 119, at 128.

153. John J. Kruzel, *Cybersecurity Poses Unprecedented Challenge to National Security, Lynn Says*, AMERICAN FORCES PRESS SERVICE (June 15, 2009), http://www.defense.gov/news/newsarticle.aspx?id=54787 ("Once the province of nations, the ability to destroy via cyber means now also rests in the hands of small groups and individuals: from terrorist groups to organized crime, hackers to industrial spies to foreign intelligence services.").

154. Jay Akbar, *'Death to France. Death to Charlie': Pro-ISIS hackers launched 'unprecedented' wave of cyber-attacks on 19,000 French websites*, THE DAILY MAIL (Jan 15, 2015), http://www.dailymail.co.uk/news/article-2912280/Death-France-Death-Charlie-Pro-ISIS-hackers-launched-unprecedented-wave-cyber-attacks-19-000-French-websites.html.

155. U.S. GENERAL ACCOUNTING OFFICE, REPORT TO CONGRESSIONAL REQUESTERS: INFORMATION SECURITY, COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS (1996) at 27, www.gao.gov/assets/160/155448.pdf.

156. Ziolkowski, *supra* note 10, at 447.

157. *See* Sam Biddle, *The NSA Leak is Real, Snowden Documents Confirm*, THE INTERCEPT (Aug. 19, 2016), https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm.

espionage distinct, since it does not remain solely in the hands of the spy, but is being spread and disseminated throughout the world. The implication is that sensitive information capable of harming individuals, organizations, and democratic values is under constant threat of being stolen and leaked.

International law, particularly the principles and norms discussed in the second section of this article, is often general and broad, allowing existing international laws to address and apply to new threats.[158] However, cyber espionage is truly *sui generis*, requiring a new approach that tackles its distinctiveness directly. In this regard, it is critical to note that cyber espionage being *sui generis* does not mean that there is a *lacuna* within international law with regard to cyber espionage, but that cyber espionage is distinct from traditional espionage and requires a special treatment within the confines of international law.

A. Cyber Espionage as Hostile Intent

Some experts grapple with cyber espionage by proposing a new category of cyber espionage operations, namely those that demonstrate "hostile intent."[159] This approach seeks to isolate cyber espionage incidents that target sensitive computer systems, such as "early warning or military command and control systems, missile defense computer systems, and computers that maintain the safety and reliability of a nuclear stockpile."[160]

Naturally, this "hostility" in cyber espionage could lead to the conclusion that a particular act of cyber espionage is a threat to use force.[161] Such a threat would be a violation of Article 2(4) of the U.N. Charter, which prohibits not only the actual use of force, but also the threat to use force.[162] This assertion is based on two premises. First, cyber espionage targets sensitive information, particularly the information resident in national security targets, which indicates that the motivation of the perpetrators is to collect intelligence for a prospective cyber-attack or military operation against the spied-upon state. Second, the exploitation that made the cyber espionage possible, given that the target of espionage is indeed sensitive, could be construed as a threat to abuse that exploitation for more severe attacks. In other words, if an exploitation in the

158. Ziolkowski, *supra* note 10, at 450.

159. SHARP, *supra* note 119, at 130.

160. *Id.*

161. Wortham, *supra* note 133, at 655.

162. U.N. Charter art. 2, ¶ 4 ("All Members shall refrain . . . from the threat or use of force.").

computer systems of a nuclear plant is abused by another state for espionage, that could indicate that the spying state might exploit that flaw to conduct more severe cyber-attacks in the future.[163]

At this point, the volume of possible scenarios that fall within the scope of the threat to use of force prohibition is very limited. It is also important to note that labeling a cyber espionage operation as a "threat to use force" does not invoke the right to self-defense enshrined in Article 51 of the U.N. Charter. Self-defense is applicable only "when an armed attack occurs," and a simple threat to use force, or actual use of force which does not meet the armed attack threshold, would not trigger self-defense. Applying the label of "threat to use force" to cyber espionage could deter the spying state, since it suggests that if the spying does take place, the spying state will be held responsible for an internationally wrongful act.[164] The implication is that victim states will not be eligible for acting in self-defense. At most, they will be entitled to engage in countermeasures due to a violation of international law on the attacking state's behalf.[165]

B. Cyber Espionage as Coercion

Intelligence collection could be used not only for purposes of future conflict, but also as a method to coerce a state into a policy decision that it would not otherwise pursue.[166] Cyber espionage could constitute a method of coercion if the information obtained from the operation is used to intervene in the internal or external affairs of the spied state.[167] The DNC hack is a good demonstration

---

163. Wortham, *supra* note 133, at 656.

164. U.N. Charter art. 2, ¶ 4 could constitute a breach of international obligation, giving rise to state responsibility under the Draft Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission at its fifty-third session, G.A. Res. 56, Supplement No. 10 (A/56/10) Report of the International Law Commission (2001).

165. Draft Articles on Responsibility of States for Internationally Wrongful Acts, adopted by the International Law Commission at its fifty-third session, G.A. Res. 56, Supplement No. 10 (A/56/10) Report of the International Law Commission (2001), Art. 49.

166. Also referred to as "interference", OPPENHEIM'S INTERNATIONAL LAW 418 (Robert Jennings & Arthur Watts eds., Oxford University Press 9th ed. 2008) (1905). ("[T]he interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question. Interference pure and simple is not intervention.")

167. *See Nicaragua v. United States*, *supra* note 134, at ¶ 205 ("[T]he principle forbids all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States.")

of that, with Russia leaking sensitive information to influence a fundamental democratic process – presidential election.

Non-intervention (or non-interference) is a well-established customary international law having great relevance to cyber espionage operations.[168] Non-intervention partially overlaps with Article 2(1) of the UN Charter, which provides "the principle of the sovereign equality of all its Members."[169] The International Court of Justice attempted to clarify the boundaries of "intervention" by arguing that intervention is wrongful when it amounts to coercion.[170] Cyber espionage operations that end up being coercive by the spying state will violate the principle of non-intervention. The main difference between the non-intervention framework and the threat to use force framework as they relate to cyber espionage is that the first deals with politically or economically coercive acts by the spying state, while the latter deals with intelligence collection for an upcoming attack.

Responsibility for a prohibited intervention will not justify military response. It could, under certain conditions, justify countermeasures.[171] Yet again, discouraging cyber espionage under the non-intervention principle could, to some degree, prevent the use of cyber espionage for coercive purposes.

C. Cyber Duck or Cyber Rabbit?[172] *– Diminishing the Peacetime-Wartime Dichotomy through the Contextual Approach*

As suggested above, the weakness of the espionage and international law discourse until today is that it focused on a very dichotomous understanding of the applicable legal frameworks. Although this very article is guilty of expressly using the misleading and contradictory term "peacetime cyber espionage," this distinction does not serve any purpose in today's world, given the complexity

---

168. *See Id.* at ¶ 202 ("The principle of nonintervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law.")

169. U.N. Charter art. 2, ¶ 1.

170. *See Nicaragua v. United States*, *supra* note 134, at ¶ 205.

171. *See generally* G.A. Res. 56, Supplement No. 10 (A/56/10) Report of the International Law Commission Chapter II on Countermeasures of the Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001).

172. This title was inspired by Rosa Brooks' piece on "Duck-Rabbit and Drones." Rosa Brooks, *Duck-Rabbit and Drones: Legal Indeterminacy in the War on Terror,* 25 STAN. L. POL'Y REV. 301 (2014).

of recent conflicts and cyber operations.[173] The term "peaceful" is misleading because it denotes a benign phenomenon, while in reality "peacetime" is a term of art that indicates applicability of international law, excluding laws of war.

The purpose of this section is to propose a new approach to cyber espionage, which previous writings on espionage failed to provide. For example, a recent paper on the status of peacetime cyber espionage provided that surveillance without direct injury to people or property would not reach the threshold of the use of force paradigm and that "intrusion into another state's systems by breaching firewalls and cracking passwords fails to violate nonintervention."[174] This permissive approach, though advanced by various scholars, does not provide guidelines for future cyber espionage operations, which might yield slightly different consequences or occur in a new context, for example during a presidential election. This article also seeks to refute the notion that cyber espionage or exploitation is "not governed by international law at all."[175] The contextual approach, as its name suggests, seeks to address cyber espionage in the context in which it occurs. The previous sub-sections' discussions of hostile-intent cyber espionage and coercive cyber espionage lay the foundations for the contextual approach.

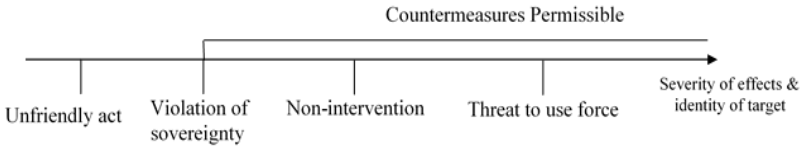
This approach uses a continuum of possible context of cyber incidents, which differ in their severities and applicable legal frameworks. The following spectrum provides a graphical illustration of the concept behind the approach:

---

173. *See* Rosa Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 675 (2004) ("Both international and domestic law take as a basic premise the notion that it is possible, important, and usually fairly straightforward to distinguish between war and peace, emergencies and normality, the foreign and the domestic, the external and the internal . . . [T]hese binary distinctions are no longer tenable.").

174. Christopher Yoo, *Cyber Espionage or Cyber War? International Law, Domestic Law, and Self-Protective Measures,* 15-3 U. PA. PUB. L. & LEGAL THEORY RES. PAPER SERIES 8 (2015).

175. *Id.* at 26.



One side of the spectrum, "unfriendly act," potentially denotes a low intensity, non-politically motivated cyber operation, which could constitute a cyber-crime,[176] which is subject at most times to the domestic criminal law and extradition procedures, and under certain conditions would be treated under the auspices of the Budapest Convention on Cybercrime, which among other things, obligates state parties to domestically criminalize unauthorized access to computer systems.[177] The second extreme, "threats to use force," are politically motivated acts that collect militarily or politically sensitive intelligence, and could also escalate to a "cyber-attack," by yielding kinetic destructive consequences, such as death or injury to persons or damage to objects, leading to an actual use of force.[178]

A particular cyber espionage operation could be located at any point on the spectrum – The novelty of this approach to cyber espionage is in that it takes into the account the context – the motivations of the perpetrators, the actual and expected effects, as well as the identity of the target and its importance to the overall network, when assessing the proper legal framework. For example, cyber espionage against a non-sensitive target with no coercive subsequent use would be at most a violation of territorial

---

176. *See* Hathaway, *supra* note 22, at 832-835.

177. As of May 9, 2015, 45 state parties have ratified the Budapest Convention on Cybercrime, mostly Council of Europe Member States and non-members such as the U.S., Australia and Japan. Article 2 of the Budapest Convention reads: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system." Convention on Cybercrime art. 2, *opened for signature* Nov. 23, 2001, T.I.A.S. No. 13,174.

178. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, *supra* note 30, at 45-52. *See also* Schmitt, *supra* note 131, at 288.

sovereignty, or even an unfriendly act,[179] depending on the gravity of consequences and identity of the targeted computer system. However, politically motivated cyber espionage that targets sensitive computer systems will be treated as a threat to use force. Naturally, the share of cyber espionage operations that reach the threat to use force level of gravity is extremely low, but under certain circumstances is possible. In the aftermath of the DNC hack, the author of this article (among others) has argued that a new approach for non-intervention in the context of cyber espionage is required. In that approach, the intent and intrusiveness of a cyber operation are analyzed to determine its degree of coerciveness, which is a key factor in the norm of non-intervention.

What matters, therefore, is the context in which such espionage operations take place. For example, we want to encourage information regarding torture practices in an armed conflict to become public for the sake of protection of human rights. That would be an espionage operation legitimate under international law, as the context and intent suggest that the information is highly important for the protection of human rights. At the same time, we should not tolerate foreign actors who use intrusive cyber operations to disrupt an ongoing political process or intimidate political communities. Distinguishing between the two cases may be difficult at times, but the identity of the actors involved, the timing, context, and even the type of operation employed can all tip the scales in one direction or the other. States should clarify the acceptable bounds of cyber espionage before more incidents take place because it may be very difficult to apply the norm of non-intervention to difficult future cases.

Another important factor in the contextual approach is that it does not use outdated peacetime-wartime distinctions. The only characteristics the contextual approach uses to value different cyber espionage incidents are severity, identity of the target, and the actual and intended use of the intelligence. The question of peacetime or wartime does not bear any relevance to the overall evaluation using the contextual approach.

The first factor of the contextual approach is the target of the cyber incident. In other words, the applicability of international law norms depends on the strategic value of the target. This, in fact, is

---

179. DAGMAR RICHTER, MAX PLANCK ENC. OF PUB. INT'L LAW (Rudolf Bernhard & Peter Macalister-Smith eds., 2003) defines "unfriendly act" as follows: "An 'unfriendly act' is a conduct (act or omission) of a subject of international law which inflicts a disadvantage, disregard or discourtesy on another subject of international law without violating any legal norm."

not a novel factor in relation to cyber warfare. A 1998 study on *Information Warfare and International Law* attempted to map cyber threats within three criteria: physical destructiveness, physical intrusiveness, and character of target.[180] The identity of the target gains particular emphasis from scholars who argue that the mere intrusion into a "critical infrastructure" target constitutes a hostile intent and even a use of force.[181] A prominent proponent of this approach (colloquially referred to as the "target-based approach"[182]) argued that espionage into "early warning or command and control systems, missile defense computer systems, and other computers that maintain the safety and reliability of a nuclear stockpile" demonstrates hostile intent, and that in these cases "the necessity of self-defense may be instant, overwhelming and leaving no choice of means, and no moment for deliberation."[183] This, however, is not the conclusion advanced by this article. The identity of the target is only one factor, and does not, in itself, give rise to the right to self-defense.

The identity of the target can range from the computers of individuals, private corporations, or military contractors, to critical civil infrastructure and military systems. The characterization of a cyber espionage operation will depend upon the target's identity – whether such target is essential to the national security and the proper functioning of that state.

The second factor is the actual and intended use of the intelligence gathered. As the continuum suggested by this article indicates, the use can be anything from curiosity (no use) to coercion (mild degree of use) to hostility (severe degree of use). This step in the evaluation seeks to determine (1) how the information obtained was used, if at all; (2) whether the actual and intended use of the intelligence is to coerce the targeted state (*i.e.*, to force that state to make certain choices or intervene in that state's core policy choices, whether social, economic or political); and (3) whether the actual and intended use of the information obtained is to carry out an attack (cyber or non-cyber) against the target state (*i.e.*, utilizing the location of military targets, weapon stockpiles, munitions factories and more). Since this evaluation is most likely to be done *ex post*,

---

180. Lawrence Greenberg et al., INFORMATION WARFARE AND INTERNATIONAL LAW 5-6 (1998), http://www.dodccrp.org/files/Greenberg_Law.pdf.

181. SHARP, *supra* note 119, at 129 – 131.

182. Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CAL. L. REV 1079, 1119 (2013).

183. SHARP, *supra* note 119, at 130.

the "intended use" could be determined upon examination of the *quality* of intelligence obtained, which could be either useless for hostile acts, such as private information of soldiers or which could be effective and useful for an attack, such as the exact locations of weapon stockpiles and military camps.

The DNC Hack, for example, took place in a very close and dramatic presidential election process. It was allegedly carried out by Russia, a country that has not been traditionally "peaceful" in cyberspace towards the U.S.

GhostNet, which experts believe China carried out against Tibet, did not occur in a vacuum. It happened in the context of ongoing tensions between them. Already in 2009, the Dalai Lama declared that the Chinese government had made life "hell on Earth"[184] for Tibetans, and since 2006 China has displaced more than two million Tibetans to weaken the Tibet Autonomous Region; this is only the tip of the iceberg.[185]

Flame also did not occur in a political vacuum. There have been tensions between Israel and Iran over the past several years, particularly due to Iran's nuclear program, which creates major dissatisfaction with Israeli leaders.[186] *Flame* also occurred after the infamous *Stuxnet* cyber-attack, carried out by Israel and the United States against Iran's nuclear plant in Natanz.[187]

These last two examples demonstrate that it is important to take the context into account when assessing a cyber espionage operation. In both cases, cyber espionage was carried out in a tense environment, but it would be a deep understatement to classify these events as "peacetime" espionage operations. That implies that political tensions may tilt the scales in the process of determining whether a cyber espionage operation violated international law.

---

184. *Dalai Lama: China makes life 'hell on Earth' for Tibetans*, CNN (Mar. 10, 2009, 7:24 AM), http://www.cnn.com/2009/WORLD/asiapcf/03/10/india.dalai/index.html?iref=24hours.

185. *Seven years in Tibet: 2 million 'displaced' by Chinese relocation policy*, THE TELEGRAPH (Jun. 27, 2013, 6:25 PM) www.telegraph.co.uk/news/worldnews/asia/tibet/10146867/Seven-years-in-Tibet-2-million-displaced-by-Chinese-relocation-policy.html.

186. *See* Jeffery Heller, *Netanyahu draws "red line" on Iran's nuclear program*, REUTERS (Sep. 27, 2012, 7:39 PM), www.reuters.com/article/2012/09/27/us-un-assembly-israel-iran-idUSBRE88Q0GI20120927.

187. Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet.

Just like cyber espionage, the contextual approach would also analyze cyber-crimes and cyber-attacks on a continuum. These occur in varied contexts as well, requiring different treatment. The specific nature of cyber-attacks and crimes is, however, beyond the scope of this article.[188]

Cyber espionage operations could also violate human rights, especially the right to privacy as codified by the U.N. as a prohibition against unlawful and arbitrary interference with privacy,[189] which prohibits unlawful attacks against individuals' honor and reputation.[190] However, such a solution is not necessarily optimal for two main reasons. First, non-state actors are not bound by international human rights instruments, and states who are bound by them will argue that privacy was not violated, since there was no arbitrariness or unlawfulness attached to the act; or that there is no extraterritorial application of international human rights law.[191] In other words, such interference is justified on the grounds of national security or public order. Secondly, Article 4(2) of the International Covenant on Civil and Political Rights allows derogation from Article 17 (the right to privacy), which puts this right at a disadvantage compared to other human rights. Fundamentally, the human rights grounds to address inter-state cyber espionage are unstable.

V. CONCLUSION

This article argues for a new approach towards cyber espionage. What researchers and policymakers have failed to appreciate is the tremendous difference between traditional methods of espionage and cyber espionage, which opens up the path to a more nuanced approach to address the latter. Cyber espionage has the potential to obtain enormous amounts of information. It is a tool available to every state and non-state actor, deterrence is extremely complicated, and it shares technical real-time similarities with destructive cyber-attacks. Leaks of information gathered using cyber espionage are

---

188. *See* TALLINN MANUAL, *supra* note 30 at 45-52 for an approach that is heavily based on context. *See also* Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM J. TRANSNAT'L L. 885, 914-915 (1998-1999).

189. International Covenant on Civil and Political Rights art. 17, ¶ 1, *opened for signature* 16 Dec. 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976).

190. *Id.*

191. Beth Van Schaack, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change*, 90 INT'L L. STUD. 20, 23 (2014).

increasingly prevalent. This further differentiates cyber espionage from traditional espionage. These differences call for a new approach, distinct from the approach used with traditional espionage, to restrict and regulate cyber espionage in a way that conveys its uniqueness, and responds to the overall gravity of the situation.

Using outdated approaches to new threats and challenges is inefficient and detrimental to international peace and order. Every threat and challenge to the international community should be addressed within existing norms and principles, unless it is proven that current norms and principles are unable to adapt efficiently to that threat. In the case of cyber espionage, the current norms and principles are deeply inadaptable and modern times require a more nuanced approach, such as the one advanced by this article, which takes into account the identity of the targets, as well as the actual and expect effects.

The approach to cyber threats and challenges that is offered by this article would be a multilateral international norm-creation process, which will take into the account the inherent uniqueness of these threats and challenges and provide a state-centered seal of approval (or disapproval) to certain activities in cyberspace. Unfortunately, a norm-creation process seems unrealistic in the near future, given the political fragmentation the international community is currently suffering. In addition, bringing states together to talk about cyber espionage would be made more difficult by the fact that cyber espionage techniques are guarded fiercely by states.