TULANE JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW

VOLUME 28 WINTER 2019 NO. 1

Cyberwarfare: A Tortuous Problem for the Law of Armed Conflict?

Dr. Waseem Ahmad Qureshi*

I. INTRODUCTION

Globally, more than 2.7 billion people use the Internet,[1] and most developed countries rely on computer systems to serve their critical national infrastructure, putting at risk their national security. In this setting even the most capable countries are vulnerable to cyberattacks.[2] Therefore, the international community is worried about security, defense, and the capacity to prevent cyberattacks.[3] The United Nations (U.N.) General Assembly has acknowledged that cyberattacks put the peace and security of the world at risk and have the capacity to undermine the security and integrity of critical national infrastructure, which provide services in the civil and military domains.[4] For instance, the Stuxnet virus used by the United States and Israel to target Iranian nuclear facilities caused the destruction of numerous centrifuges; malware—used by Israel and the United States—disrupted Syrian radar system data and enabled Israeli fighter jets to enter sovereign Syrian airspace to carry out armed attacks;[5] and the Estonia attack compromised and halted government services, banking systems, and media in that country.[6] These examples of cyberattacks are a threat to national security. At present, cyberwarfare is taking place and aggressive states have set up dedicated cyberintelligence units to wage wars against other states to serve their geopolitical interests.[7] So the most relevant question here is what the applicable legal framework is to regulate and prevent cyberattacks.[8] It is pertinent to note here that cyberattacks by nonstate actors (especially those that cannot be attributed to any state) are not within the scope of this Article, which is to analyze the *jus ad bellum* of cyberattacks.

In this context, this Article will try to explore three main dimensions of cyberattacks: (1) What is the nature of the threat posed by cyberattacks?

---

1. INT'L TELECOMM. UNION, MEASURING THE INFORMATION SOCIETY (2013).
2. Michael N. Schmitt, *Cyber Operations and the Jud Ad Bellum Revisited*, 56 VILL. L. REV. 569, 588-89 (2011).
3. FREDERICK WAMALA, INT'L TELECOMM. UNION, INTERNATIONAL TELECOMMUNICATION UNION NATIONAL CYBERSECURITY STRATEGY GUIDE 13-14 (2011).
4. *See* G.A. Res. 56/19, at 1-2 (Jan. 7 2002); G.A. Res. 58/32, at 2 (Dec. 8, 2003); G.A. Res. 59/61, at 2 (Dec. 3, 2004); G.A. Res. 60/45, at 2 (Dec. 8, 2005); G.A. Res. 61/54, at 2 (Dec. 6, 2006); G.A. Res. 62/17, at 2 (Dec. 5, 2007); G.A. Res. 63/37, at 2 (Dec. 2, 2008); G.A. Res. 64/25, at 2 (Dec. 2, 2009); G.A. Res. 65/41, at 2 (Dec. 8, 2010); G.A. Res. 66/24, at 2 (Dec. 2, 2011); G.A. Res. 67/27, at 2 (Dec. 3, 2012).
5. FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR 161 (2016).
6. HEATHER H. DINNISS, CYBER WARFARE AND THE LAWS OF WAR 38 (2012).
7. *See* KAPLAN, *supra* note 5, at 156, 159-60.
8. MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INT'L LAW APPLICABLE TO CYBER WARFARE 3 (2013).

(2) What are the key international legal principles applicable to cyberattacks? (3) What are the applicable international laws that can regulate or prevent cyberattacks? For these purposes, this Article is divided into three main Parts. Part II will explain the severity and nature of the threats posed by cyberattacks, by discussing various kinds of cyberattacks. Part III will discuss general principles and integral concepts under international laws applicable to cyberattacks. Part IV will mainly discuss the *jus ad bellum* of cyberattacks.

II. THREATS

This Part will explain the severity and nature of threats posed by cyberattacks by discussing various kinds of cyberattacks. It is divided into three sections: Section A will discuss espionage using cyberattacks as a threat to nations; Section B will discuss terrorism through cyberattacks as a threat; and Section C will discuss other cyberoperations employed by aggressive states against victim states.

A. Espionage

The prevalence[9] of cyberespionage is emerging as a threat to the peace and security of the world. Currently, the Internet or cyberspace is considered a "gift from God" for surveillance and espionage purposes,[10] and this age has been called a "golden age for espionage."[11] In cyberespionage, unauthorized states and nonstate actors infiltrate computer information systems to collect confidential information.[12] Cyberespionage can be defined as "[o]perations and related programs or activities conducted . . . in or through cyberspace, for the primary purpose of collecting intelligence . . . from, computers, information or communication systems, or networks, with the intent to remain

9. Pete Warren, *State-Sponsored Cyber Espionage Projects Now Prevalent*, GUARDIAN (Aug. 30, 2012), https://www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent; *see also* Russell Buchan, *Cyber Espionage and International Law*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 168 (Nicholas Tsagourias & Russell Buchan eds., 2015).

10. David P. Fidler, *Tinker, Tailor, Soldier, Duqu: Why Cyberespionage Is More Dangerous Than You Think*, 5 INT'L J. CRITICAL INFRASTRUCTURE PROT. 28, 29 (2011).

11. Katharina Ziolkowski, *Peacetime Cyber Espionage—New Tendencies in Public International Law*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBER-SPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 425 (Katharina Ziolkowski ed., 2013).

12. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2 (2013); Buchan, *supra* note 9, at 168.

undetected."[13] Cyberespionage is distinguished from the normal hacking of computers by its element of accessing and copying[14] confidential data by exploiting cyberspace.[15] It can violate international obligations and national laws.[16] More specifically, it violates the basic principle of equal sovereignty among states[17] and breaches the prohibition of using force and intervening in other states.[18] Thus, it threatens the peace and security of the world.[19]

For instance, in 2010, Google alleged that Chinese hackers gained access to the Gmail accounts of Chinese human rights activists.[20] Similarly, in 2012, the Russian Kaspersky Lab (a security firm) detected the Flame virus emanating from the United States and Israel, which accessed, monitored, and collected the confidential data of Iranian oil companies.[21] In another example of cyberespionage, China also hacked and copied terabytes of data regarding F-35 fighter jets from the server of the company Lockheed Martin.[22] The United States protested that this activity was a threat to U.S. national and international peace and security.[23] Reports such as the *Mandiant Report of 2013* show that there is a unit in the Chinese Liberation Army known as "Unit 61398," which acts as an instrument of state and is tasked with undertaking massive espionage

13. U.S. Presidential Policy Directive No. 20, U.S. Cyber Operations Policy (Oct. 2012), https://fas.org/irp/offdocs/ppd/ppd-20.pdf.

14. *See* Ziolkowski, *supra* note 11, at 429.

15. DENNIS C. BLAIR, S. COMM. ON INTELLIGENCE, 111TH CONG., ANNUAL THREAT ASSESSMENT OF THE INTELLIGENCE COMMUNITY FOR THE SENATE ARMED SERVICES COMMITTEE 39 (2009).

16. Buchan, *supra* note 9, at 169, 171-72.

17. U.N. Charter art. 2, ¶ 1.

18. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 202 (June 27).

19. OFFICE OF THE NAT'L COUNTER-INTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 2009-2011 (2011).

20. David Drummond, *A New Approach to China*, GOOGLE'S OFFICIAL BLOG (Jan. 12, 2010), https://googlebl og.blogspot.com/2010/01/new-approach-to-china.html.

21. Ellen Nakashima et al., *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASH. POST (June 19, 2012), https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html; *see also* Dave Lee, *Flame: Massive Cyber-Attack Discovered, Researchers Say*, BBC NEWS (May 28, 2012), https://www.bbc.com/news/technology-18238326.

22. Alexander Melnitzky, *Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses*, 20 CARDOZO J. INT'L & COMP. L. 537, 545 (2012).

23. *Id.*; *see also* Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, WALL ST. J. (Apr. 21, 2009), https://www.wsj.com/articles/SB1240274 91029837401.

operations to bolster the Chinese political position in the world.[24] Likewise, a whistleblower (a former contractor of the U.S. National Security Agency (NSA)), Edward Snowden, leaked thousands of confidential NSA documents to the public through *The Washington Post* and *The Guardian* that proved that the United States had been monitoring and collecting confidential data from several states, heads of state and government (for example, German Chancellor Angela Merkel and Israeli Prime Minister Ehud Olmert), nonstate actors, religious leaders (such as the Pope), officials of organizations (for example, individuals from the European Union), companies (such as Petrobras, a Brazilian oil company) and non-governmental organizations (such as UNICEF).[25] As a protest against NSA surveillance and espionage against Brazil, the Brazilian President formally denounced NSA activities in the U.N. General Assembly, and he cancelled his scheduled meetings with the United States.[26] He said that the NSA had violated international law,[27] the sovereignty of the Brazilian nation, and the fundamental human rights of its citizens.[28] In regard to NSA leaked documents, *The Guardian* established that Angela Merkel's activities had been monitored for more than a decade.[29] Such activity can be seen as a breach of the German state's sovereignty.[30] In response, Merkel telephoned President Obama to protest the breach of her trust and demanded explanations.[31] She said that "spying among friends is not at all acceptable against anyone, and that goes for every citizen in Germany."[32] The Brazilian and Chinese governments took similar stances with regard to NSA activities and demanded apologies; they viewed the surveillance as violations of "their sovereignties" and the "human rights of their

24. *See* Buchan, *supra* note 9, at 169.

25. *Id.*

26. Julian Borger, *Brazilian President: US Surveillance a 'Breach of International Law*,' GUARDIAN (Sept. 24, 2013), https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance; *see also* Buchan, *supra* note 9, at 178.

27. Borger, *supra* note 26; Buchan, *supra* note 9, at 178.

28. Borger, *supra* note 26; Buchan, *supra* note 9, at 178.

29. Paul Owen, *NSA Files—Edward Snowden's Letter to Angela Merkel*, GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/2013/nov/01/nsa-files-edward-snowdens-letter-to-angela-merkel-live-coverage.

30. *See* Buchan, *supra* note 9, at 179.

31. Ian Traynor et al., *Angela Merkel's Call to Obama: Are You Bugging My Mobile Phone?*, GUARDIAN (Oct. 24, 2013), https://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german.

32. Alex Spillius, *Angela Merkel: Spying Between Friends Is Unacceptable*, TELEGRAPH (Oct. 24, 2013), https://www.telegraph.co.uk/news/worldnews/europe/germany/10402570/Angela-Merkel-spying-between-friends-is-unacceptable.html.

citizens."[33] China remonstrated that NSA activities were so severe that they should be rejected and condemned by the collective international community.[34]

Since, according to the *Nicaragua* case, the principle of non-intervention is a part of customary international law,[35] the use of espionage violates sovereignty, political integrity, [36] and the principle of non-intervention in other states.[37] United Nations General Assembly (UNGA) Resolution 66/24 (2011) establishes that "[s]overeignty and international norms and principles that flow from sovereignty apply to state conduct of ICT-related activities."[38] The U.N. secretary-general substantiated this UNGA proposition by anchoring "ICT security in the existing framework of international law and understandings that govern state relations and provide the foundation for international peace and security."[39] Russell Buchan argues that cyberespionage can cause massive damage to other states by disrupting governmental activities and banking systems; therefore, Article 2(4) of the U.N. Charter (prohibition on the use of force in other states) should be interpreted as including cyberespionage. [40] Similarly, Alexander Melnitzky also believes that the prohibition on the use of force under Article 2(4) of the U.N. Charter does include cyberespionage, because data thefts in cyberespionage entails detrimental effects on the peace and security of nations.[41]

B. Terrorism

Cyberterrorism refers to attacks using electronic means such as computing devices to harm computer systems or physical infrastructure dependent on such computer systems.[42] It is defined by the United Nations Office of Drugs and Crime as the "deliberate exploitation of computer

---

33. Borger, *supra* note 26; *see also* Associated Press Beijing, *China Demands Halt to 'Unscrupulous' US Cyber-Spying*, GUARDIAN (May 27, 2014), https://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying.

34. Associated Press Beijing, *supra* note 33.

35. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 202 (June 27).

36. Ziolkowski, *supra* note 11, at 457.

37. *See* Buchan, *supra* note 9, at 181.

38. U.N. Secretary-General, *Rep. of the Group of Governmental Experts on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Security*, 8, U.N. Doc. A/68/98 (June 24, 2013).

39. *Id.* at 4; *see also* Buchan, *supra* note 9, at 183-84.

40. *See* Buchan, *supra* note 9, at 187.

41. Melnitzky, *supra* note 22, at 566; *see also* Buchan, *supra* note 9, at 187.

42. Ben Saul & Kathleen Heath, *Cyber Terrorism*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBER SPACE, *supra* note 9, at 147.

networks as a means to launch an attack . . . intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructures."[43] The U.N. Counter-Terrorism Implementation Taskforce (CTITF) defines cyberterrorism as "terrorist attacks by remotely altering information on a computer system or disrupting the flow of data between computer systems." [44] An example of computer system controlling infrastructure is the Supervisory Control and Data system (SCADA), which monitors and controls traffic systems, railroad switches, gas and electricity distribution networks, and water purification plants. [45] The unauthorized use of SCADA by hacking can be considered cyberterrorism.[46]

General international laws[47]—prohibiting states from intervening in other states, using force, and launching terrorist activities from their states—are, by using the principle of state responsibility, flexible enough to incorporate a prohibition on cyberterrorism.[48] For instance, there have been discussions on a prohibition on using force and armed attack in other states, and on whether the use of force in self-defense encompasses cyberterrorism. [49] Specifically, more serious cyberattacks by state militaries against other states without an armed conflict come under the prohibition on the use of force.[50] Likewise, instruments of national and regional[51] laws also incorporate prohibition on the offense undertaken by cyber means, such as fraud, extortion, terrorism, stalking attacks on information systems, and misuse of computers.[52] The Association of South East Asian Nationals (ASEAN) Convention on Counter Terrorism (2007)

43. U.N. Office on Drugs & Crime, The Use of the Internet for Terrorist Purposes 11 (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

44. U.N. Counter-Terrorism Implementation Task Force, Rep. of the Working Grp. on Countering the Use of the Internet for Terrorist Purposes ¶ 20 (2009) [hereinafter CTITF].

45. *See* Saul & Heath, *supra* note 42, at 147.

46. Hamadoun I. Toure, *Cyberspace and the Threat of Cyberwarfare*, *in* THE QUEST FOR CYBER PEACE 9 (2011); *see also* CTITF, *supra* note 44, ¶ 24.

47. *See* Saul & Heath, *supra* note 42, at 148.

48. *Id.*

49. *See* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBER SPACE, *supra* note 9, at 147, 255.

50. *See* Saul & Heath, *supra* note 42, at 161.

51. Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

52. Phillip Kastner & Frederic Megret, *International Legal Dimensions of Cybercrime*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBER SPACE, *supra* note 9, at 196-98.

unequivocally incorporates cooperation among states against cyberterrorism.[53]

In general, when we are discussing cyberterrorism, this is different from other organized crimes, because the inclusion of the term "terrorism" entails that the activities have an element of "political"[54] motive attached to them. The facilitation of terrorism [55] includes the recruitment of terrorists, the coordination of their activities, financing their operations, and the incitement of terrorism.[56] Therefore, instruments of international organizations also prohibit the facilitation of terrorism through cyber means. [57] For instance, UNSC Resolution 1624 (2005) prohibits the incitement of terrorism;[58] the EU Framework Decision (2008)[59] requires EU states to criminalize the provocation, recruitment, and training of terrorism; and UNSC Resolution 1373 (2001) [60] and the Terrorist Financing Convention (1999)[61] prohibit raising or distributing funds for, and financing, terrorism. UNSC Resolution 1373 (2001) also requires the exchange of operational information regarding communication and technologies used by terrorists,[62] which was supported by the unanimous adoption of a UNGA resolution for coordinating "efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the internet."[63] As a result, UNCTITF produced a "taskforce" and "detailed research" on the use of the Internet for terrorism purposes.[64]

Saul and Heath argue that, although there is no specific convention or treaty that explicitly prohibits or covers cyberterrorism, other general

---

53. ASEAN Convention on Counter Terrorism, art. VI, ¶ 1, Jan. 13, 2007, *reprinted in* INTERNATIONAL INSTRUMENTS RELATED TO THE PREVENTION AND SUPPRESSION OF TERRORISM, U.N. Sales No. E.08.v2 (2008).

54. Ben Saul, *The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient or Criminalising Thought?*, *in* LAW AND LIBERTY IN THE WAR ON TERROR 28 (Andrew Lynch et al. eds., 2007).

55. Peter Fleming & Michael Stohl, *Myths and Realities of Cyberterrorism*, *in* COUNTERING TERRORISM THROUGH INT'L COOPERATION 35, 38 (Alex P. Schmidt et al. eds., 2001).

56. U.N. Office on Drugs & Crime, *supra* note 43, at 3; Emily Wax, *Mumbai Attackers Made Sophisticated Use of Technology*, WASH. POST (Dec. 3, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/12/02/AR2008120203519.html.

57. U.N. Office on Drugs & Crime, *supra* note 43, ¶ 57.

58. S.C. Res. 1624, ¶ 4 (Sept. 14, 2005).

59. Council Framework Decision 2008/919/JHA, ¶¶ 7, 14-15, 2008 O.J. (L 330) 21 (EU).

60. S.C. Res. 1373, at 2 (Sept. 28, 2001).

61. U.N. International Convention for the Suppression of the Financing of Terrorism art. 2, Apr. 10, 2002, 2178 U.N.T.S 197.

62. S.C. Res. 1373, *supra* note 60, at 2.

63. G.A. Res. 60/288, at 6 (Sept. 8, 2006).

64. U.N. Office on Drugs & Crime, *supra* note 43, at vi; CTITF, *supra* note 44, at v.

prohibitions on physical terrorist activities under international law can also be extended in most cases to include cyberterrorism.[65] For example, see the Arab Convention on the Suppression of Terrorism of 1998,[66] the Organization of the Islamic Conference Convention on Combatting International Terrorism of 1999,[67] and the Shanghai Cooperation Organisation Convention on Combatting Terrorism, Separatism, and Extremism of 2001.[68] As the definition of terrorism includes "damage to property, places, or systems . . . economic loss, when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act."[69] it also incorporates cyberterrorism, which is essentially compelling systems to do harmful activities or forcing them to abstain from doing an act.[70] An example of a cyberattack is "Operation Avenge Assange" by the group Anonymous, which targeted payment entities including PayPal that refused to process donations for WikiLeaks under U.S. pressure; this attack disabled websites and in the process caused damage in lost revenues.[71] However, cyberattacks that do not cause serious damage or that do not have the intent[72] to intimidate a population,[73] or to compel governments or international organizations, cannot be considered cyberterrorism under the Draft Convention.[74] Therefore, Saul and Heath believe that there is a need for specific international agreements and national legislation to respond to the threat of national security posed by cyberterrorism.[75]

65. *See* Saul & Heath, *supra* note 42, at 149-51.

66. The Arab Convention for the Suppression of Terrorism arts. 1, 3, Apr. 22, 1998.

67. Convention of the Organisation of the Islamic Conference on Combating International Terrorism, July 1, 1999.

68. Shanghai Convention on Combating Terrorism, Separatism and Extremism, June 15, 2001; *see also* Saul & Heath, *supra* note 42, at 163.

69. Measures to Eliminate International Terrorism, Rep. of the Working Group, U.N. Doc. A/C.6/56/L.9, at 16 (2001); BEN SAUL, DEFINING TERRORISM IN INTERNATIONAL LAW 137, 154 (2006).

70. *See* Saul & Heath, *supra* note 42, at 155.

71. *Id.* at 157.

72. Case No. STL-11-01/I, Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, ¶¶ 85, 95 (U.N. Special Trib. for Leb. Feb. 16, 2011).

73. S.C. Res. 1566, ¶ 3 (Oct. 8, 2004).

74. *See* Saul & Heath, *supra* note 42, at 158.

75. *Id*. at 165-66.

C. Cyberoperations

Whistleblowers like Edward Snowden and Julian Assange have revealed to the world that cyberwarfare/cyberoperations are currently the biggest threat[76] to governments, organizations, groups, and individuals. Under these activities using cyberspace, governments and corporations[77] are proactively and preventively monitoring, [78] collecting, and investigating [79] data of all the aforementioned subjects. For instance, corporations like Facebook, Microsoft, WhatsApp, LinkedIn, Google, Twitter, and AOL are collecting and monitoring the data[80] of its users for economic profit, for future business aspects, and to collaborate with intelligence services.[81] Owing to the deep analytical artificial intelligence (AI) capabilities of Google, fueled by the data of all its users regarding their political proclivities, likes and dislikes, daily routines, and query searches, it is said that Google knows an individual more than that individual knows themselves.[82]

Warlike cyberoperations and cyber activities are often referred to as cyberattacks, and their militarization under the patronage of intelligence agencies is characterized as cyberwarfare.[83] Cyberwarfare is defined by Michael Schmitt as the "employment of cyber capabilities with the primary purpose of achieving [military] objectives in or by the use of cyberspace."[84] The Netherlands has defined cyberwarfare as "the conduct of military operations to disrupt, mislead, modify or destroy an opponent's computer systems or networks by means of cyber capabilities."[85] The United Kingdom's (UK's) view is that "cyber warfare can enable actors to achieve their political and strategic goals without the need for armed conflict."[86] Schmitt's definition generally focuses on the use of cyberspace

---

76. Paul Ducheine, *The Notion of Cyber Operations*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBER SPACE, *supra* note 9, at 211.

77. Paul Ducheine & Jelle van Haaster, *Fighting Power, Targeting and Cyber Operations*, *in* PROCEEDINGS ON THE 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 303, 304 (P. Brangetto et al. eds., 2014).

78. *See* Ducheine, *supra* note 76, at 211.

79. *Id.*

80. *Id.*

81. *Id.* at 212.

82. John Lanchester, *The Snowden Files: Why the British Public Should be Worried About GCHQ*, GUARDIAN (Oct. 3, 2013), https://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester.

83. *See* Ducheine, *supra* note 76, at 213.

84. *See* SCHMITT, *supra* note 8, at 15.

85. Advisory Council on Int'l Affairs & Advisory Committee on Issues of Public Int'l Law, Cyber Warfare, Report No. 77/22, 9 (2011) [hereinafter Advisory Council].

86. *See* PAUL CORNISH ET AL., ON CYBER WARFARE, at vii (2010).

for state objectives,[87] the Dutch definition focuses on the impact of cyberspace on an opponent,[88] while the U.K. definition sees cyberwarfare as an effective and aggressive military tool that is capable of disarming enemies without using force.[89]

In nature, cyberwarfare can be proactive, aggressive, preventive, or defensive[90] and can perform the strategic functions of deterrence, prevention, aggression, intervention, stabilization, and normalization.[91] From a state-centric viewpoint, cyberoperations are undertaken to protect national security and achieve political/geopolitical interests.[92] From the perspective of corporations, cyber activities by the likes of Facebook, Google, Kaspersky, and Symantec are undertaken purely for economic benefit.[93] By contrast, activist NGOs including Anonymous,[94] the TOR Project, WikiLeaks, and Bits of Freedom have ideological and political goals.[95] The increasing use of the "Internet of Things" since the events of 9/11 and the resultant rise of terrorist threats has led to increased cyber surveillance by states.[96] The dilemma is to choose between the public's right to privacy and the security of the state's political agendas,[97] which balances necessity, effectiveness, and human rights with regard to cyberoperations.[98]

In this regard, Paul Ducheine has identified five major paradigms in the state's cybersecurity framework: (1) Internet governance and diplomacy, (2) protection, (3) law enforcement, (4) intelligence and counterintelligence, and (5) military operations.[99] Under "Internet

87. *See* SCHMITT, *supra* note 8, at 15.
88. *See* Advisory Council, *supra* note 85, at 9.
89. *See* CORNISH ET AL., *supra* note 86, at 37.
90. Hans Bouwmeester et al., *Cyber Security and Policy Responses*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES 30 (Paul Ducheine et al. eds., 2012).
91. *Id.* at 27, 32, 43.
92. *See* Ducheine, *supra* note 76, at 215-16.
93. *Id.* at 216.
94. *Id.* at 217.
95. *Id.*
96. *Id.* at 219.
97. Ewen Macaskill & Gabriel Dance, *NSA Files: Decoded,* GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.
98. Dinah PoKempner, *Cyberspace and State Obligations in the Area of Human Rights*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBER-SPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY, *supra* note 11, at 253.
99. *See* Ducheine, *supra* note 76, at 218, 220.

governance[100] and diplomacy,"[101] cyberoperations are mainly proactive and preventive, shaping governance in cyberspace,[102] keeping in mind the state's security interests and strategies.[103] In the framework of "protection," cyber activities by states are focused on protecting the integral infrastructure of state organs, such as guarding electricity, water, and military infrastructure, [104] and fighting malware viruses and other unauthorized intrusions in the systems. [105] For "law enforcement," cyber activities are an amalgam of private and public operations at national and international levels [106] to investigate conduct, penalize crimes, take repressive measures, and enhance prosecution and policing. [107] In "intelligence and counterintelligence," states undertake security operations, surveillance, [108] espionage, [109] and counterthreats. [110] Intelligence agencies are allowed by their respective states to "exploit the information for other purposes, or directly intervene in order to prevent threats from reoccurring."[111] The use of the Stuxnet virus is an example of proactive and aggressive operation by intelligence agencies for military purposes.[112] Finally, military operations under the cyberoperations of a state are undertaken to serve political interests, state strategies, and military objectives, [113] by disrupting, destroying, or misleading an opponent's networks and computer systems, [114] for deterrence,

100. Tunis Agenda for the Information Society, World Summit on the Information Society, ¶¶ 2, 29-38, Nov. 18, 2005, WSIS-05/TUNIS/DOC/6(Rev. 1)-E [hereinafter Tunis Agenda].

101. MELISSA E. HATHAWAY & ALEXANDER KLIMBURG, NATIONAL CYBER SECURITY FRAMEWORK MANUAL 127 (Alexander Klimburg ed., 2012).

102. Katharina Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBER-SPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY, *supra* note 11, at 185, 187.

103. Tunis Agenda, *supra* note 100, ¶ 68; *Global Cybersecurity Agenda*, ITU (May 17, 2007), https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx; *see also* Ducheine, *supra* note 76, at 221.

104. *See* Ducheine, *supra* note 76, at 221; *see also* Bouwmeester et al., *supra* note 90, at 34.

105. *See* Ducheine, *supra* note 76, at 222.

106. HATHAWAY & KLIMBURG, *supra* note 101, at 29-30.

107. Bert-Jaap Koops, *Cybercrime Legislation in the Netherlands*, 14.3 ELECTRONIC J. COMP. L. 1, 16 (2010); *see* Ducheine, *supra* note 76, at 223.

108. *See* Ducheine, *supra* note 76, at 224.

109. *See* Buchan, *supra* note 9, at 169.

110. AIDAN WILLS, UNDERSTANDING INTELLIGENCE OVERSIGHT 11; *see* Ducheine, *supra* note 76, at 224-25.

111. HATHAWAY & KLIMBURG, *supra* note 101, at 124.

112. *See* Ducheine, *supra* note 76, at 225.

113. *See* SCHMITT, *supra* note 8, at 32-33.

114. *See* Advisory Council, *supra* note 85, at 9.

intervention, prevention, protection, and stabilization,[115] short of using armed force.[116]

Examples of cyberwarfare include intelligence, counterintelligence, and military cyberoperations. For instance in domestic cyberoperations, Dutch intelligence agencies are legally entitled through a 2002 Act[117] to intercept, search, and store data of telecommunications and hack computer systems.[118] Aggressive international cyberoperations, such as the Stuxnet virus of 2010 and the Estonia attacks of 2007, made the world realize that the security of critical infrastructure is important,[119] because international cyberoperations can disrupt societies.[120] In a joint collaborative cyberwarfare operation in 2010, the United States and Israel partnered to target Iranian nuclear facilities with the Stuxnet virus.[121] Even though the Iranian system was not connected to the Internet, making cyber intrusion very difficult, Stuxnet was successful in sabotaging the Iranian "Industrial Control System."[122] Another example of aggressive intelligence and military operation is the cyberwarfare against Syria.[123] In 2007, cyberattacks by Israel used coding and tooling to trick the Syrian air defense system into not noticing invading Israeli fighter jets targeting Syrian nuclear facilities at al Kibar.[124] The governing principles of international law, including the notion of sovereignty and the principle of nonintervention (prohibition on the use of force), are violated by proactive/aggressive cyber military operations/cyberwarfare targeting other states.[125] Cyberoperations may also violate trade law, private

115. Bouwmeester et al., *supra* note 90, at 27, 32. 43.

116. *See* CORNISH ET AL., *supra* note 86, at 37.

117. Wet op de inlichtingen-en veiligheids [Intelligence and Security Services Act] 7 Feb. 2002, Stb. 2002, 148 (Neth.).

118. *Interception of Telecomm. by the AIVD: Rules and Regulations*, GEN. INTELLIGENCE & SEC. SERV. (Nov. 29, 2013), https://english.aivd.nl/latest/news/2013/11/29/interception-of-telecommunications-by-the-aivd-rules-and-regulations.

119. *See* Ducheine, *supra* note 76, at 221.

120. Sean Lawson, *Cyber Attack Scenarios and the Evidence of History*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 90, at 277; *see also* Ducheine, *supra* note 76, at 221.

121. DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 188-89 (2012).

122. Michael Hanspach & Michael Goetz, *On Covert Acoustical Mesh Networks in Air*, 8 J. COMM. 758, 759 (2013); *see also* Ducheine, *supra* note 76, at 212.

123. PETER W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 126 (2014).

124. *Id.* at 127.

125. *See* Marco Roscini, *Cyber Operations as a Use of Force*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBER SPACE, *supra* note 9, at 245.

international law, and public international law,[126] in addition to the laws of using force.

III. KEY CONCEPTS

This Part will discuss general principles and integral concepts under international law that are applicable to cyberattacks. It is divided into two sections: Section A will discuss the notions of "cyberspace" and "national jurisdiction" in relation to cyberattacks, and Section B will discuss the concept of "state responsibility" with regard to cyberattacks.

A. Cyberspace & National Jurisdiction

Cyberspace is defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[127] This definition does not cover the software side of the cyberspace; more aptly, cyberspace can be defined as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via independent and interconnected networks using information-communication technologies."[128] Cyberspace has three layers; its first layer includes physical infrastructure such as computers, circuits, and cables; its second layer consists of "software"; and its third layer involves "data packets and electronics."[129]

From an international law perspective, the key questions are whether cyberspace is subject to sovereignty and whether cyberspace is sovereign itself. Sovereignty is a body of rights attributed to state territory in relation

---

126. David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies*, 17 A.S.I.L. INSIGHTS 1, 3 (2013); *see also* Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1073, 1077 (2006).

127. U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 58 (Nov. 8, 2010, amended in 2019); Nicholas Tsagourias, *The Legal Status of Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE, *supra* note 9, at 15.

128. Daniel T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, *in* CYBERPOWER AND NATIONAL SECURITY 28 (Franklin D. Kramer et al. eds., 2009); *see also* Tsagourias, *supra* note 127, at 15.

129. Lior Tabansky, *Basic Concepts in Cyber Warfare*, 3 MIL. & STRATEGIC AFF. 75, 77 (2011).

to other states,[130] serving to "divide between nations the space upon which human activities are employed" [131] and depicting political and legal limits.[132] Sovereignty as a power, and not as territory, is substantiated and operated through jurisdiction[133] (legal authority).[134] Goldsmith establishes that cyberspace is subject to sovereignty, and states can regulate upon the domestic effects of extraterritorial activities in cyberspace.[135] Therein, states can exercise their jurisdiction upon their "nationals," [136] "nonnationals in their territory,"[137] infrastructure in their territory,[138] and the flow of information in their territory, [139] cyberspace technology, software activities and web addresses.[140] States can also exercise their jurisdiction in cases where their nationals are victim to cybercrime committed by a foreigner in another country under the "passive nationality principle," [141] where the foreign cyber activity has detrimental and foreseeable[142] effects in their territory[143] under the "effect doctrine,"[144] where their national interest is endangered by some extraterritorial activity[145] under the "protective head of jurisdiction,"[146] or over activities

130. Corfu Chanel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. 15, 28, 35 (Apr. 9).

131. Island of Palmas Case (U.S. v. Neth.), Award, 1928 R.I.A.A. 839 (Apr. 4).

132. Tuomas Forsberg, *Beyond Sovereignty, Within Territoriality: Mapping the Space of Late-Modern Geo-Politics*, *in* COOPERATION & CONFLICT 355, 362 (1996); *see also* John G. Ruggie, "*Territoriality and Beyond" Problematizing Modernity in International Relations*, 47 INT'L ORG. 139, 159 (1993).

133. *See* Tsagourias, *supra* note 127, at 19.

134. Michael Akehurst, *Jurisdiction in International Law*, 46 BRIT. Y.B. INT'L L. 145, 145-46, 159 (1972-1973); Wedding v. Meyler, 192 U.S. 573, 583 (1904).

135. Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. OCCASIONAL PAPER 32-33 (1998).

136. Nottebohm Case (Liech. v. Guat), Judgment, 1995 I.C.J. 4, 23 (Apr. 6).

137. The Case of the S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 19, 23 (Sept. 7).

138. Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEX. L. REV. 1571, 1575 (2010).

139. R. v. Sheppard [2010] EWCA (Crim) 65, [15], [20] (Eng.); *see also* Kanuck, *supra* note 138, at 1573-74.

140. *See* Tsagourias, *supra* note 127, at 19-21.

141. Arrest Warrant Case (Dem. Rep. Congo v. Belg.), Judgment, 2002 I.C.J. 837, ¶ 15 (Apr. 11); *see also* Tsagourias, *supra* note 127, at 19.

142. U.S. v. Yousef, 327 F.3d 56, 86-87 (2d Cir. 2003).

143. Uta Kohl, *Jurisdiction in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE, *supra* note 9, at 35.

144. *See* The Case of the S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 23 (Sept. 7).

145. *Id.* at 32.

146. CEDRIC RYNGAERT, JURISDICTION IN INTERNATIONAL LAW 96 (2d ed. 2008).

and objects in virtual reality if they do not fall under any jurisdiction under the "permissive rule."[147]

For instance, in a French case, Yahoo (a U.S. corporation with its server in the United States) was held liable for violating French laws on the prohibition of selling Nazi artifacts because it was accessible in France "and the harm was suffered in France."[148] Later, the findings of this case were mirrored in several other cases around the globe. For example, in an English court, a U.S. publisher was convicted for publishing obscenity and violating the obscenity laws of the U.K.[149] In a German court, a Dutch seller was convicted of selling drugs online and violating German laws, even though the drug concerned was legal in the Netherlands, because the "origin rule" didn't apply here owing to the protection of public health.[150] Similarly, an English defendant was held liable in a Dutch court for violating Dutch license laws that prohibited making a gambling site accessible in the Netherlands.[151] An Australian court also found an American site guilty of defamation caused in Australia despite being in a U.S. publication,[152] and the same approach was taken by an English court against Harrods Ltd.[153] Similarly, an English court held Google responsible for collecting the data of English residents without their consent;[154] later, Spain took a similar approach against Google for violating data protection laws.[155] For data protection, states like Iran and China have completely banned certain websites including Facebook and YouTube.[156]

On the other hand, Johnson and Post propose that cyberspace should not be subject to sovereignty and must be self-regulating.[157] However, cyberspace cannot be considered sovereign itself, because it does not have any central authority to make and enforce laws, and it does not have its

147. *See* Tsagourias, *supra* note 127, at 21.

148. Kohl, *supra* note 143, at 38.

149. R. v. Perrin [2002] EWCA (Crim) 747 [1], [6] (Eng.); Perrin v. U.K., 5446 Eur. Ct. H.R. 2, 6 (2005).

150. *See* Kohl, *supra* note 143, at 39.

151. *Id.* at 41.

152. *Id.* at 43.

153. *Id.*

154. Vidal-Hall v. Google Inc., [2014] EWCH (QB) (Eng.).

155. Case C-131/12 Google Spain SI., Google Inc. v. Agencia Espanola de Protección de Datos, 2014 E.C.J.; *see* Council Directive 95/46/EC art. 4, 1995 O.J. (L281) (EP).

156. *See* Kohl, *supra* note 143, at 52.

157. LAWRENCE LESSIG, CODE: VERSION 2.0, at 3 (2d ed. 2006); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367, 1402 (1996).

own people.[158] Instead, cyberspace can be seen as one of the global commons of the whole world,[159] as, for example, outer space,[160] the high seas,[161] and Antarctica[162] are considered global commons.

B. State Responsibility

State responsibility is a principle of international law[163] that includes acts or omissions attributable to a state and breaches of obligations under international law.[164] These breaches can be undertaken by groups, organizations, or individual beings on behalf of a state.[165] First, it should be seen whether the action or omission is undertaken by the organs of a state. If not, then it should be seen whether the action or omission by individuals or organizations had been undertaken on the direction of a state.[166] Even in cases where the organs of states exceed the authority granted by their state, this can give rise to state responsibility.[167] In the *Bosnian Genocide* case, the International Court of Justice found that, even when an organization had no international recognition as a state organ, the effective control by the state and the fact that the state in question had given precise instructions to the organization were enough to prove state responsibility for the violations of international law by the organization acting on behalf of the state.[168] In this case, the ICJ did not uphold the "overall control" test formulated by the *Tardic* case, which required the state's full control and, where that is absent, stipulated that

158. *See* Tsagourias, *supra* note 127, at 24.

159. TIM BERNERS-LEE & MARK FISCHETTI, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB 123 (1999).

160. The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies arts. 2-4, Dec. 18, 1979, 1363 U.N.T.S. 3; Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies arts. 1, 2, 7, 8, Jan. 27, 1967, U.N.T.S. 90-4; G.A. Res. 1962 XVIII, ¶ 1-4 (Dec. 13, 1963).

161. Convention on the High Seas, Apr. 29, 1958, art. 2, 13 U.S.T. 2312, 450 U.N.T.S. 82; United Nations Convention on the Law of the Sea, Dec. 10, 1982, U.N. Doc. A/CONF.62/122 (1982), *reprinted in* 21 I.L.M. 1261 (1982).

162. The Antarctic Treaty art. 4, Dec. 1, 1959, 402 U.N.T.S. 71.

163. The Factory at Chorzow (Ger. v. Pol.), Judgment, 1928, P.C.I.J. 13 (Sept. 13).

164. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, [2011] 2 Y.B. Int'l L. Comm'n, U.N. Doc. A/56/10 [hereinafter *ARS*]; Case Concerning U.S. Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980, I.C.J. 3, ¶¶ 45-55 (May 24); Case Concerning Application of The Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro) Judgment, 2007 I.C.J. 43, ¶ 167 (Feb. 26).

165. *See ARS*, *supra* note 164.

166. Bosn. & Herz. v. Serb. & Montenegro, 2007 I.C.J. ¶ 396; *see ARS*, *supra* note 164, art. 5.

167. *See ARS*, *supra* note 164, art. 6-7.

168. Bosn. & Herz. v. Serb. & Montenegro, 2007 I.C.J. ¶ 397, at 400-01.

individual criminal responsibility should be applied.[169] However, the Articles on the Responsibility for States (ARS) do recognize exceptions for state responsibility for nonviolations of international law in cases involving distress,[170] self-defense,[171] necessity,[172] force majeure,[173] countermeasures[174] and consent.[175]

The notion of sovereignty under state responsibility entails that it should control all the illicit cyber activities emanating from its infrastructure and computer activities.[176] However, in cyberspace, the attribution of state responsibility in violation of international law is difficult. For instance, Germany accused the U.K. and the United States of violating international law by using their embassies in Berlin for international cybersurveillance.[177] Similarly, a number of U.S. embassies in Asia and Europe collected the data of their host states.[178] In such cases, there is a possibility that accused states could deny liability because they used proxies to undertake such attacks.[179] Therefore, in cyberspace cases, victim states are allowed a more liberal procedure to infer evidential circumstances.[180] For example, the climate of political relationships may allow some insight in sudden cyberattacks, with a reverse burden of proof allowed.[181] Since the attribution laws are a gray area in international law for the purposes of cyberattacks, there has been a rise of nonstate actors acting independently, or as a proxy for other states, rendering it very difficult for victim states to respond in self-defense.[182]

---

169. Prosecutor v. Tadic, Case No. IT-94-1-A, Judgment, ¶¶ 122, 131 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999); Bosn. & Herz. v. Serb. & Montenegro, 2007 I.C.J. ¶¶ 404, 405-06; *see ARS*, *supra* note 164, art. 8.

170. *See ARS*, *supra* note 164, art. 24.

171. *See id.* art. 21.

172. *See id.* art. 25.

173. *See id.* art. 23.

174. *See id.* art. 22.

175. *See id.* art. 20.

176. Corfu Chanel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. 18 (Apr. 9); *see* SCHMITT, *supra* note 8, at 26-28, 34.

177. Nigel Morris et al., *Germany Calls in Britain's Ambassador to Demand Explanation Over Secret Berlin Listening Post*, INDEPENDENT (Nov. 6, 2013), https://www.independent.co.uk/news/uk/politics/germany-calls-in-britains-ambassador-to-demand-explanation-over-secret-berlin-listening-post-8923082.html.

178. *Id.*

179. Harold H. Koh, Legal Advisor, U.S. Dep't of State, Remarks at the USCYBERCOM Inter-Agency Legal Conference, International Law in Cyberspace (Sept. 18, 2012).

180. U.K. v. Alb., 1949 I.C.J. at 18; *see* SCHMITT, *supra* note 8, at 34.

181. Constantine Antonopoulos, *State Responsibility in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBER SPACE, *supra* note 9, at 64.

182. Nicolo Bussolati, *The Rise of Non-State Actors in Cyberwarfare*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 102, 126 (Jens D. Ohlin et al. eds., 2015).

International obligations can be violated in cyberspace, where the sovereignty of a state is breached. Examples of such acts are surveillance and espionage by state organs or individuals from other states.[183] However, espionage is not prohibited under international law, and some further proof of damage to another state is required to establish a breach of an international obligation in cyberspace.[184] Nevertheless, where something is not mentioned in international law, that does not mean that something is entirely permissible; in fact, no state claims that espionage is a lawful act.[185] In some cases, the concept of attribution is inapplicable, where de facto organs/agents of states and concerns of failures to act are involved; here, the notion of due diligence is applicable.[186] Article 14 of ARS explicitly includes instances of failing to act, with reference to state responsibility, because the state is responsible for preventing all crimes emanating from its territories, if there is a persistent risk of it reoccurring.[187] Therefore, states cannot knowingly allow their territory to be used to violate international law, and they must take reasonable steps to prevent such activities.[188]

IV. *JUS AD BELLUM*

This Part will mainly discuss the *jus ad bellum* of cyberattacks. It will start by exploring the criteria by which cyberattacks can be considered the "use of force" and "armed force," while providing relevant definitions, *opinio juris*, and legal analyses on the subject. Then, it will analyze whether cyberattacks can be viewed as "armed attacks" and whether they can give rise to the right to self-defense. This Part is divided into three sections: Section A will provide a brief contextual analysis of the use of force and the international laws with regard to cyberwarfare; Section B will define the notion of the "use of force" in relation to cyberattacks, and

183. *See* Buchan, *supra* note 9, at 179.

184. The Case of the S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 31 (Sept. 7); *see also* SCHMITT, *supra* note 8, at 30.

185. Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, 2010 I.C.J. 403, ¶¶ 84-85 (July 22); Anne Peters, Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part 1, EJIL TALK (Nov. 1, 2013), http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/.

186. Int'l Law Comm'n Rep. on the Work of Its Fifty First Session, [1999] 2 Y.B. Int'l L. Comm'n, U.N. Doc. A/54/10; Jan Arno Hessbruegge, *The Historical Development of the Doctrines of Attribution and Due Diligence in International Law*, 36 N.Y.U. J. INT'L L. & POL. 265, 268, 275 (2004); *see also* Antonopoulos, *supra* note 181, at 66.

187. *See ARS*, *supra* note 164, art. 14.

188. *See* SCHMITT, *supra* note 8, at 26-27.

provide criteria for the circumstances in which cyberattacks can be considered the "use of force" and "armed force." Section B will also try to analyze whether cyberattacks can be considered "economic and political coercion." It will attempt to provide the *opinio juris* of some key players in the international community on the consideration of cyberattacks as the "use of force." Furthermore, it will examine different approaches to see the legality of cyberattacks under the laws of using force: the "result-based approach," the "target-based approach," the "instrument-based approach," the "contextualist approach," and the "positivist approach." Section C will discuss the notions of "armed attack" and "self-defense" in relation to cyberattacks.

A. Contextual Analysis

The Estonia attack of 2007 is an example of a cyberattack in which distributed denial of service (DDoS) attacks compromised and halted government services, banking systems, and media in Estonia.[189] Though there was no physical damage to infrastructure, tens of millions of euros in damage were caused by this cyberattack.[190] Initially, Estonia accused the Russian government of conducting these attacks,[191] but it later retracted its stance to accuse the Kremlin of these damages[192]—a Kremlin-based group of youths admitted responsibility—and acknowledged that the Russian government had no hand in the attacks.[193] Likewise, in 2010, the Stuxnet virus (a cyberattack), orchestrated by state-backed professionals, targeted Iran's "industrial control system,"[194] targeting

189. *See* Dinniss, *supra* note 6, at 38.

190. Ian Traynor, *Web Attackers Used a Million Computers, Says Estonia*, GUARDIAN (May 18, 2007), https://www.theguardian.com/technology/2007/may/18/news.russia.

191. Tony Halpin, *Putin Accused of Launching Cyber War*, N.Y. TIMES (May 18, 2007), http://web.b.ebscohost.com/ehost/detail/detail?vid=0&sid=3020bfbe-e98c-41e4-831e-93627c050874%40pdc-v-sessmgr06&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=7EH1035512869&db=n5h.

192. Traynor, *supra* note 190.

193. Charles Clover, *Financial Times: Kremlin-Backed Group Behind Estonia Cyber Blitz*, CYRUS FAVIAR BLOG (Mar. 11, 2009), https://cyrusfarivar.com/blog/20 09/03/12/financial-times-kremlin-backed-group-behind-estonia-cyber-blitz/.

194. NICHOLAS FALLIERE ET AL., SYMANTEC SECURITY RESPONSE, W32.STUXNET DOSSIER 2 (version 1.4, 2011); *Iran Says Cyber Foes Caused Centrifuge Problems*, REUTERS (Nov. 29, 2010), https://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129 [hereinafter *Iran*].

centrifuges[195] at the Natanz and Bashair nuclear facilities.[196] Iran formally accused Israel and the West of this malware cyberattack,[197] but no author was identified conclusively.[198] As a result of this attack, more than a thousand damaged IR-1 centrifuges were replaced in the nuclear facilities attacked.[199] The Stuxnet virus was introduced in the Iranian system through a USB stick that contained the Stuxnet virus, which changed the rotation settings of the centrifuges and sabotaged the regular settings of the operating system.[200] In the "Farewell Dossier," a similar approach was undertaken to introduce the malware to change system settings that caused a pipeline explosion.[201] Such examples prove that cyberattacks on host states can cause physical damage in the real world, in addition to the destruction of information and software in cyberspace.[202]

Generally, states[203] and international organizations[204] are reluctant to view cyberattacks as armed attacks. So the question remains whether cyberattacks can be considered to be the use of force against other states, in the sense of Article 2(4) of the U.N. Charter, which explicitly prohibits all states from using force against other states.[205] The prohibition on the use of force is a part of customary international law[206] and is considered

---

195. *Iran*, *supra* note 194; *see also Iran Says Nuclear Programme Was Hit by Sabotage*, BBC NEWS (Nov. 29, 2010), https://www.bbc.com/news/world-middle-east-11868596 [hereinafter *Nuclear*].

196. *Nuclear*, *supra* note 195.

197. *Iran*, *supra* note 194; *see also Nuclear*, *supra* note 195.

198. Christopher Williams, *Israeli Chief Celebrates Stuxnet Cyber Attack*, TELEGRAPH (Feb. 16, 2011), https://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html; *see also* Kim Zetter, *Did the U.S. Government Lab Help Israel Develop Stuxnet?,* WIRED (Jan. 15, 2011), https://www.wired.com/2011/01/inl-and-stuxnet/; DAVID ALBRIGHT ET AL., INST. FOR SCI. & INT'L SEC., STUXNET MALWARE AND NATANZ: UPDATE OF ISIS DECEMBER 22, 2010 REPORT 10 (2011).

199. ALBRIGHT ET AL., *supra* note 198, at 1-4; Kim Zetter, *Report Strengthens Suspicions That Stuxnet Sabotaged Iran's Nuclear Plant*, WIRED (Dec. 27, 2010), https://www.wired.com/2010/12/isis-report-on-stuxnet/.

200. FALLIERE ET AL., *supra* note 194, at 7; William J. Broad & David Sanger, *Worm Was Perfect for Sabotaging Centrifuges*, N.Y. TIMES (Nov. 18, 2010), https://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html.

201. *See* Dinniss, *supra* note 6, at 38, 281.

202. *Id.* at 38-39, 281.

203. *Id.* at 39.

204. Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (May 17, 2004), https://www.theguardian.com/world/2007/may/17/topstories3.russia.

205. U.N. Charter art. 2, ¶ 4.

206. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 190 (June 27); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 87 (July 9); Case Concerning Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶ 148 (Dec. 19).

jus cogens.[207] There are only two exceptions to this principle: the use of force in self-defense[208] and the use of force with the authorization of the U.N. Security Council,[209] inscribed under Articles 51 and 39-41 of the U.N. Charter, respectively. This next Section will explore what conditions need to be met for cyberattacks to be deemed the "use of force" for the purposes of Article 2(4) and as an "armed attack" for the purposes of self-defense under Article 51 of the U.N. Charter. In addition, the Section will also discuss the elements that shape the conditions of applying the rules of *jus ad bellum* to cyberattacks.

B. Use of Force

Cyberattacks amounting to an "armed attack" or the "use of force" can violate the Article 2(4) prohibition on the use of force and therein can give rise to the right to self-defense under Article 51 of the U.N. Charter.[210] The *Tallinn Manual on the International Law Applicable to Cyber Warfare* clearly states that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[211] The United States' legal advisor, Harold Koh, also affirmed that "if the physical consequences of a cyberattack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber-attack should equally be considered a use of force." [212] Koh considered cyberattacks resulting in nuclear plant meltdown, dam destruction in populated areas, airplane crashes due to disabled air-traffic to be the use of force.[213] These types of destruction caused by cyberattacks are indirect in nature,[214] but the ICJ in the *Nicaragua* case had established that the use of force can be indirect in nature.[215] The 1982 installation of malware software, causing the destruction of a gas pipeline in Soviet Serbia by the United States' CIA, and the Stuxnet virus by the United States and Israel, damaging nuclear centrifuges in Iranian nuclear facilities, are examples of cyberattacks that can cause destruction equivalent to the

---

207. Nicar. v. U.S., 1986 I.C.J. ¶ 190.
208. U.N. Charter art. 51.
209. *Id.* arts. 39-41.
210. *See* Roscini, *supra* note 125, at 241-42; Carlo Focarelli, *Self-Defense in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBER SPACE, *supra* note 9, at 265.
211. *See* SCHMITT, *supra* note 8, at 45.
212. Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. INT'L L.J. 1, 4 (2012).
213. *See id.*
214. *See* Roscini, *supra* note 125, at 242.
215. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27); *see* Dinniss, *supra* note 6, at 66.

use of force and armed attacks.[216] Therefore, the threshold of cyberattack destruction should be equivalent to the use of force to violate Article 2(4) and equivalent to an "armed attack" to give rise to the right to self-defense under Article 51.[217] However, it is pertinent to note here that Article 2(4) does not provide any scale of threshold for the use of force, and any kind of use of force against the sovereignty of a state is therefore forbidden.[218] For instance, in 2012 the largest oil company in Saudi Arabia, Saudi Aramco, was attacked by a virus that deleted all its data from 30,000 computers and replaced it with a U.S. flag.[219] In this regard, since the notions of use of force and armed attack also apply to the destruction of property in addition to the destruction of life, any large-scale attack on data can be considered an armed attack[220] and will also violate the principle of nonintervention.[221] Similarly, any cyberattack that targets defense systems such as missile systems, radar systems, and satellites, putting the defense and national security of a country at risk, should also be considered the use of force against a sovereign state.[222] Therefore, states including the United

216. *See* THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 4 (2013); *see also* DAVID ALBRIGHT ET AL., INST. FOR SCI. & INT'L SEC., DID STUXNET TAKE OUT 1,000 CENTRIFUGES AT THE NATANZ ENRICHMENT PLANT? 1 (2010); *see* Roscini, *supra* note 125, at 238.

217. OLIVIER CORTEN, THE LAW AGAINST WAR: THE PROHIBITION ON THE USE OF FORCE IN CONTEMPORARY INTERNATIONAL LAW 66-67 (Christopher Sucliffe trans., 2010); *see* Koh, *supra* note 212, at 4.

218. NILS MELZER UNIDIR, CYBERWARFARE AND INTERNATIONAL LAW 6, at 8-9 (2011); *see* Roberto Ago, *Addendum to the Eighth Report on State Responsibility*, [1980] 2 Y.B. Int'l L. Comm'n 41, U.N. Doc. A/CN.4/SER.A/1980/Add.1.

219. *Saudi Aramco Says Cyber Attack Targeted Kingdoms Economy*, AL ARABIYA (Dec. 9, 2012), http://english.alarabiya.net/en/News/2012/12/09/Saudi-Aramco-says-cyber-attack-targeted-kingdoms-economy.html.

220. John F. Murphy, *Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?*, 89 INT'L L. STUD. 309, 325 (2013).

221. Terry D. Gill, *Non-Intervention in the Cyber Context*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBER-SPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY, *supra* note 11, at 32.

222. *US Drones Infected by Key Logging Virus*, ALJAZEERA (Oct. 8, 2011), https://www.aljazeera.com/news/americas/2011/10/201110816388104988.html; Robert Johnson, *New Evidence Suggests China's Hacking into US Drones Using Adobe Reader and Internet Explorer*, BUS. INSIDER (Dec. 22, 2011), https://www.businessinsider.com/chinas-hacking-into-us-drones-using-adobe-reader-and-internet-explorer-2011-12; Charles Arthur, *Chinese Hackers Suspected of Interfering with US Satellites*, GUARDIAN (Oct. 27, 2011), https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected.

States,[223] Mali,[224] and Russia[225] view cyberattacks disrupting the critical infrastructure of a country as the use of force against the sovereign victim state. The main critique of this interpretation is that the use of force in these attacks is not armed force[226] (this approach is known as the instrumental approach, which is discussed in Section IV.B.5 below).[227] This perspective argues that, instead of armed force, such use of force should be considered to be within the realms of "economic and political coercion."[228]

1. Economic and Political Coercions

The wording of the U.N. Charter prohibits the "use of force."[229] This use of force includes intention to coerce and use of weapons.[230] The Eastern countries have repeatedly asked for economic and political coercions to be included within the meaning of the use of force.[231] For instance, the Brazilian government proposed including coercion by economic means in the realms of Article 2(4), though this was rejected.[232] The view of David Harris[233] and the Belgian delegates[234] is that the rejection of the Brazilian proposal does not prove that Article 2(4) does not include other forms of coercion. However, the prevailing and the Western[235] view is that the wording of the "use of force" is limited to include "armed force,"[236] given the fact that the wording of the U.N.

223. U.S. Dep't of Def., *Assessment of International Legal Issues in Information Operations*, 76 INT'L L. STUD. SER. US NAVAL WAR C. 459, 483 (2002) [hereinafter *Assessment*]; *see* U.S. DEP'T OF DEF., CYBER SPACE POLICY REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, ¶ 934 (2011); U.S. Presidential Policy Directive, *supra* note 13; U.N. Secretary-General, *Developments in the Field of Information and Telecommunication in the Context of International Security* 18, U.N. Doc. A/66/152 (July 15, 2011).

224. U.N. Secretary-General, *Developments in the Field of Information and Telecommunication in the Context of International Security* ¶¶ 16, 22, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009) [hereinafter *Developments*].

225. Vida Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 166 (2005).

226. ELIZABETH WILMSHURST, PRINCIPLES OF INTERNATIONAL LAW ON THE USE OF FORCE BY STATES IN SELF-DEFENCE 6 (2006).

227. Stephanie Gosnell Handler, *New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, 48 STAN. J. INT'L L. 209, 226-27 (2012).

228. *Id.*

229. U.N. Charter art. 2, ¶ 4.

230. *See* Roscini, *supra* note 125, at 237.

231. *See* Dinniss, *supra* note 6, at 41.

232. *Id.* at 43.

233. D.J. HARRIS, CASES AND MATERIALS ON INTERNATIONAL LAW 890 (6th ed. 2004).

234. *See* Dinniss, *supra* note 6, at 43.

235. *Id.*

236. *Id.*

Charter in Articles 41, 42, and 44 use the phrase "armed force"[237] and that Article 51 includes "armed attack."[238] Developing states have proposed including economic and political coercion in the prohibition of the use of force, but every time such proposals from the developing countries have received negative votes and rejection from the Western states.[239] Similar arguments have been used to reject, including the term "aggression" instead of "the use of force" in proposals, because the term "aggression" is not properly defined in a universally accepted manner.[240] So the Western bloc insisted in UNGA resolutions that the use of force is limited to armed forces, and the Soviet, European, and developing states bloc insisted that the prohibition on the use of force should also include political and economic coercions that threaten the political independence and sovereignty of a state.[241]

Bond believes that the term "use of force" is only relatable to the traditional/conventional use of weapons.[242] Roscini also concludes that the prohibition on the use of force does not include economic and political coercions, because they do not include weapons, which is implied under Article 41.[243] Therefore, the United States argues that other forms of aggression, such as political and economic coercions, can be covered as a threat to international peace and security under Article 39[244] of the U.N. Charter.[245] The inclusion of cyberattacks under economic and political coercions is flawed because the latter employs the economy as a weapon to pressure states by political and diplomatic means, and the former uses malware direct attacks as instruments to destroy targeted structures.[246] Roscini questions why, when a kinetic bomb employed to destroy a financial institution is surely an armed attack, the same result by cyberattacks and the use of another weapon of choice should be considered any less.[247]

---

237. U.N. Charter arts. 41, 42.

238. *Id.* art. 51; *see* Dinniss, *supra* note 6, at 41-42.

239. *See* Dinniss, *supra* note 6, at 44.

240. *Id.*

241. *Id.* at 47.

242. James Bond, Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality Under the United Nations Charter Article 2(4) (June 14, 1996) (unpublished M.A. thesis, Naval War College) (on file with the Naval War College in the Center for Naval Warfare Studies); *see* Dinniss, *supra* note 6, at 44.

243. *See* Roscini, *supra* note 125, at 237-38.

244. U.N. Charter art. 39.

245. *See* Dinniss, *supra* note 6, at 44.

246. *See* Roscini, *supra* note 125, at 249.

247. *Id.*

The UNGA has defined aggression as "the most serious and dangerous form of the illegal use of force," including nondestructive actions such as breaching a treaty, providing land to an aggressor, and allotting a naval blockade.[248] The ICJ also established that arming and training armed groups is a use of force.[249] And if we look at the intention of the drafters and history of developing the Article 2(4) prohibition on the use of force, it is clear that it has the ability to adapt to changing circumstances;[250] it was drafted to stop aggression against other states.[251] Ian Brownlie concluded that the Kellogg-Briand Pact was intended to prohibit any use of substantial armed force.[252] In attempts to clarify the meaning of the use of force in the U.N. Charter, states have struggled to define it through UNGA resolutions but have failed to attain consensus.[253] The Organization of American States Charter includes economic and political coercions separately from the use of armed force,[254] to clarify that there is no relation between the use of force and other coercive measures. Richard Aldrich and Tom Farer conclude that the general prohibition on economic and political coercion under the OAS Charter are unenforceable,[255] because it even outlaws all diplomatic measures by deeming them political coercion.[256] Similar to the OAS Charter, the U.K. also believes that political and economic coercion should not be treated under the principle of prohibition on the use of force, but instead threats to political independence and sovereignty within such coercion should be seen as a violation of the principle of non-intervention in other states.[257] For these reasons, all types of coercions should be seen as different from the use of force.[258]

---

248. G.A. Res. 3314 (XXIX), at 143 (Dec. 14, 1974).

249. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.*),* Judgment, 1986 I.C.J. 14, ¶ 228 (June 27).

250. Edward Gordon, *Article 2(4) in Historical Context*, 10 YALE J. INT'L L. 271, 273 (1985).

251. *See* Dinniss, *supra* note 6, at 45.

252. IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 87 (1963); *see also* D.W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW 136 (1958).

253. CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 9 (Malcolm Evans & Phoebe Okowa eds., 2000).

254. Charter of the Org. of American States, arts. 19-20 (1948).

255. Richard Aldrich, *How Do You Know You Are at War in the Information Age?*, 22 HOUS. J. INT'L L. 223, 251 (2000).

256. Tom J. Farer, *Political and Economic Aggression in Contemporary International Law*, *in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE 121 (A. Cassese ed., 1986).

257. *See* Dinniss, *supra* note 6, at 47-48.

258. *See* Roscini, *supra* note 125, at 235-36.

2. *Opinio Juris*

Since the prohibition on the use of force was adopted before the electronic age of information, it can be applied to cyberattacks.[259] Countries including China,[260] Hungary,[261] Australia,[262] Cuba,[263] Italy,[264] Iran, [265] the Russian Federation, Mali, [266] U.K., [267] Qatar, [268] the Netherlands,[269] and the United States,[270] as well as the European Union,[271] believe that the prohibition on the use of force does include cyberattacks. Russia is of the view that cyberattacks are a use of force, similar to the use of weapons of mass destruction.[272] It noted that,

> from a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not . . . . Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.[273]

Belarus also considers cyberattacks to be equivalent to weapons of mass destruction.[274] Kazakhstan noted that ICT weapons can be used during

---

259. U.S. DEP'T OF DEF., DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 56 (2019).

260. Li Zhang, *A Chinese Perspective on Cyber War*, 94 INT'L REV. RED CROSS 801, 804 (2012).

261. Janos Martonyi, Minister of Foreign Affairs of Hungary, Speech at the Budapest Conference on Cyberspace, Opening Session (Oct. 4, 2012).

262. *See* U.N. Secretary-General, *supra* note 223, at 12.

263. U.N. Secretary-General, *Developments in the Field of Information and Telecommunication in the Context of International Security* 3-4, U.N. Doc. A/57/166/Add.1 (Aug. 29, 2002).

264. Governo Italiano, La Posizione Italiana Sui Principi Fondamentali Di Internet (Sept. 17, 2012), http://download.repubblica.it/pdf/2012/tecnologia/internet.pdf.

265. *See* Rep. of the S.C., at 1-3, U.N. Doc. A/60/730 (2006).

266. Developments, *supra* note 224, ¶¶ 19, 22.

267. PRIME MINISTER, A STRONG BRITAIN IN AN AGE OF UNCERTAINTY: THE NATIONAL SECURITY STRATEGY 29 (2010).

268. U.N. Secretary-General, *Developments in the Field of Information and Telecommunication in the Context of International Security* 9, U.N. Doc. A/65/154 (July 20, 2010).

269. GOV'T NETHERLANDS, DUTCH GOVERNMENT RESPONSE TO THE AIV/CAVV REPORT ON CYBER WARFARE 5-6 (Apr. 26, 2012); *see also* U.N. Secretary-General, *supra* note 223, at 13.

270. *See* Roscini, *supra* note 125, at 233-34.

271. CYBERSECURITY STRATEGY OF EUROPEAN UNION, AN OPEN SAFE AND SECURE CYBERSPACE, JOINT COMMUNICATION TO THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS JOIN 1 final (Feb. 7, 2013).

272. *See* Dinniss, *supra* note 6, at 54.

273. *Id.*

274. James Andrew Lewis, *Cyber Security and Cyberwarfare: Assessment of National Doctrine and Organization*, *in* THE CYBER INDEX, UNDIR 2013/3, INTERNATIONAL SECURITY TRENDS AND REALITIES 12 (2013).

armed conflicts.[275] Cuba stated that ICT weapons can cause destruction to critical national infrastructure (CNI) and can threaten the peace and security of the world.[276] Spain made an analogy similar to the Cuban stance.[277]

Canada, the U.K., Australia, India, France, New Zealand, and Germany have been the victims of large- and small-scale cyberattacks, but none has treated cyberattacks as the use of force against their land.[278] Instead, they have treated cyberwarfare to be the equivalent of cyberespionage.[279] China has also been a victim of massive cyberattacks, which have compromised its military secrets and caused damage to the state;[280] thus far, China has also not formally published any statement that treats cyberattacks as the use of force.[281] The U.S. policy against cyberattacks is to pursue defensive and preemptive counter-cyberattacks targeting the computer systems of perpetrators with military means,[282] but it is not clear whether the United States considers cyberattacks to be the use of force. The international community is reluctant to treat cyberattacks as the use of force because, with the exception of one attack—the Farewell Dossier[283]—none of the attacks have caused human injury.[284] It is pertinent to note here that the United States includes the employment of non-kinetic weapons and information operations within its vision,[285] and the U.K.

---

275. U.N. Secretary-General, *Developments in the Field of Information and Telecommunication in the Context of International Security* 4, U.N. Doc. A/64/129 (July 8, 2009).

276. U.N. Secretary-General, *Developments in the Field of Information and Telecommunication in the Context of International Security*, at 2, U.N. Doc. A/66/152/Add.1 (Sept. 16, 2011).

277. Developments, *supra* note 224, at ¶ 10.

278. *See* Dinniss, *supra* note 6, at 55.

279. *Id.*

280. John Leyden, *France Blames China for Hack Attacks*, REGISTER (Sept. 12, 2007), https://www.theregister.co.uk/2007/09/12/french_cyberattacks/; *see also* Edward Cody, *Chinese Official Accuses Nations of Hacking*, WASH. POST (Sept. 13, 2007), http://www.washingtonpost.com/wpdyn/content/article/2007/09/12/AR2007091200791.html.

281. BRYAN KREKEL, CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION 6 (2009).

282. Bradley Graham, *Bush Orders Guidelines for Cyber-Warfare*, WASH. POST (Feb. 7, 2003), https://www.washingtonpost.com/archive/politics/2003/02/07/bush-orders-guidelines-for-cyber-warfare/dd8b4a18-140c-4690-88a5-0041d4ce1b1c/; Hillary R. Clinton, Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010); Ellen Nakashima, *U.S. Eyes Preemptive Cyber-Defense Strategy*, WASH. POST (Aug. 29, 2010), http://www.washingtonpost.com/wpdyn/content/article/2010/08/28/AR2010082803312.html.

283. *See* Dinniss, *supra* note 6, at 57.

284. *Id*.

285. JOINT CHIEFS OF STAFF, JOINT VISION 2020—AMERICA'S MILITARY: PREPARING FOR TOMORROW 23 (2000).

considers the use of cyberspace against other states to be a "military weapon."[286]

Based on the *opinio juris* of U.N. members, the UNGA report of 2013 on the inclusion of cyberattacks within the realm of the prohibition on the use of force concluded that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [Information and Communications Technologies] environment."[287] For such application, however, cyberattacks need to meet three main criteria: (1) The cyberattack must be attributable to a state; (2) the cyberattack must be equivalent to the use or threat of force, which is armed force capable of causing the destruction of property or life; and (3) the cyberattack must be international in nature (taking place across borders), where one state is targeting another.[288] In addition, any cyberattack that produces the same results that a conventional kinetic energy weapon does can be considered the use of armed force.[289]

3. Result-Based Approach

Scholarly opinion is divided on what perspective or approach should be used to analyze the emerging threat of cyberattacks in the form of cyberwarfare. Brownlie believes that the use of force must employ a weapon that can cause the destruction of property or human injury.[290] Weapons can be defined as instruments that are capable of destruction[291] and are used for destruction[292] or violence.[293] Weapons are, therefore, "instruments that produce violent consequences."[294] Weapons are determined by their result and not by their mechanism.[295] Ian Bowett also

286. PRIME MINISTER, *supra* note 267, at 29.

287. U.N. Secretary-General, *Developments in the Field of Information and Telecommunication in the Context of International Security* 2, U.N. Doc. A/68/98 (June 24, 2013).

288. *See* Roscini, *supra* note 125, at 234.

289. Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 103 (2001); *see also* Daniel Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, 76 INT'L L. STUD. 89, 92 (2002).

290. BROWNLIE, *supra* note 252, at 362.

291. THE PROGRAM ON HUMANITARIAN POLICY & CONFLICT RESEARCH AT HARV. UNIV., MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE, at xxiv (2013) [hereinafter THE PROGRAM].

292. JEAN M. HENCKAERTS & LOUISE DOSWALD-BECK, 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 239 (2005).

293. *Weapon*, BLACK'S LAW DICTIONARY (9th ed. 2009).

294. *See* Roscini, *supra* note 125, at 238.

295. Katharina Ziolkowski, *Computer Network Operations and the Law of Armed Conflict*, 49 MIL. L. & L. WAR REV. 47, 69 (2010).

considers that the use of force must cause some sort of human injury.[296] Under this presumption, the vast majority of cyberattacks, which do not cause any sort of destruction, can never be considered the use of force.[297] Brownlie argues that, for instance, though biological and chemical weapons do not employ kinetic force, because they can cause the destruction of property and life, they can still easily be considered a weapon.[298] This kind of analysis of consequences is known as the result-based perspective.[299] Under this perspective, Cassandra LaRae-Perez argues that long-term economic sanctions can cause a lot of damage to both property and human life, in a similar way to other weapons using kinetic energy, and thus sanctions should also be considered the use of force under the aegis of Article 2(4).[300] However, the economic embargos that caused massive destruction such as the embargos on Cuba and Arab states, by the United States and Israel, respectively, were never treated by the international community as the use of force.[301] Therefore, Schmitt maintains that quantifying direct destruction caused by economic coercion is a difficult task.[302] Nonetheless, Heather Dinniss counterargues that cyberattacks using non-kinetic force, causing destruction of property, should not, from a legal perspective, be differentiated from other forms of use of force, using a result-based approach.[303] This result-based approach is the prevailing and the most acceptable approach, judging the characteristics of armed forces by analyzing the destruction it causes to property and human beings.[304]

Therefore, the cyberattacks should not be viewed as any less than other weapons used in armed conflicts.[305] The *HPCR Manual* endorses cyberattacks, computer codes, malware, and their associated components as being considered means of warfare and accepts that destruction can be

296. BOWETT, *supra* note 252, at 191-92.

297. Todd A. Morth, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter*, 30 CASE W. RES. J. INT'L L. 567, 591 (1998).

298. BROWNLIE, *supra* note 252, at 362.

299. Cassandra LaRae-Perez, *Economic Sanctions as a Use of Force: Re-Evaluating the Legality of Sanctions from an Effects-Based Perspective,* 20 B.U. INT'L L.J. 161, 162-63 (2002).

300. *Id.* at 180-81.

301. Bond, *supra* note 242, at 59.

302. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 906 (1999).

303. *See* Dinniss, *supra* note 6, at 60.

304. Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT & SECURITY L. 211, 217 (2012); *see also* Dinniss, *supra* note 6, at 74.

305. Yoram Dinstein, *Cyber and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference*, 89 INT'L L. STUD. 276, 280 (2013); *see also* Schmitt, *supra* note 302, at 913.

caused without using kinetic means.[306] Similar to other kinetic weapons, cyberattacks also employ payloads in the form of codes and malware; they have delivery systems including emails and USB sticks; and they can cause harm to vulnerable targets, reaching them via entry points.[307] However, it is pertinent to note here that cyberattacks designed only for extracting data or information cannot be considered the use of force, without causing destruction of property or life.[308] Nevertheless, such cyber exploitation and information destruction may still violate state sovereignty.[309]

4. Target-Based Approach

The target-based approach argues that all cyberattacks that intercept information or structures that are critical to national security, such as CNI, are a use of force and armed attack,[310] even in circumstances where there is no physical damage caused.[311] As Walter G. Sharp argues, the non-armed use of force such as cyberattacks on critically important information even have the capacity to cause more damage than actual/physical armed attacks.[312] Conversely, the international community does not share Sharp's expansive interpretation of cyberattacks; instead, international law sees such intrusions as acts of espionage and not as the use of force or armed attack.[313]

5. Instrument-Based Approach

This approach argues that only the use of traditional or conventional weapons can amount to the use of force, and cyberattacks can never be considered the use of force even in cases where it causes physical damage, because it merely uses computer coding in cyberspace instead of kinetic weapons.[314] Scholars believe that such an approach is "ill-suited" for

306. THE PROGRAM, *supra* note 291, at xxiv.

307. Fred Schreier, *On Cyberwarfare* 66-67 (DCAF Horizon 2015, Working Paper No. 7, 2015), https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf.

308. Thomas Rid & Peter McBurney, *Cyber Weapons*, 157 RUSI J. 1, 10 (2012).

309. *See* Roscini, *supra* note 125, at 241.

310. WALTER G. SHARP, CYBERSPACE AND THE USE OF FORCE 130 (1999).

311. *Id.* at 128-29; *see also* Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 E.J.I.L. 825, 855 (2001).

312. SHARP, *supra* note 310, at 133.

313. *See* Dinniss, *supra* note 6, at 81.

314. Handler, *supra* note 227, at 227; *see also* Matthew C. Waxman, *Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions*, 89 INT'L L. STUD. 109, 111 (2013).

analyzing cyberattacks,[315] and the weapon of choice can be anything ranging from ordinary household tools[316] to nonkinetic energy weapons.[317] For instance, the ICJ accepted that assistance to armed bands could amount to the use of force, because enabling people to use force is itself a use of force.[318] One should not focus on the weapon of choice or the mechanism employed, but rather see the consequences.[319] For example, an analogy of a murder case will suffice to prove that the instrument-based approach is ill-suited for analyzing the use of force under the U.N. Charter. If a murder is committed by using a pen to stab a victim in his chest or neck, the instrument-based approach will conclude that, since a pen is not a traditional weapon, this death cannot be considered murder. However, a reasonable legal analysis will consider the intentions behind using a pen and will conclude that the pen in this case is a weapon of choice, through which a murder was carried out.[320] Ultimately, the ICJ has established that uses of force "do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed."[321]

6. Contextualist Approach

The contextualist approach, used by Michael Schmitt and Michael Reisman, proposes that all sorts of coercion are based on a variety of factors and therefore should be analyzed in relation to the world order.[322] Schmitt argues that the choice of instrument in a coercion does not matter; instead, its consequences do.[323] In a way, when Schmitt's argument relies on the consequences of coercion, disregarding the weapon of choice, his argument is strikingly similar to the result-based approach, which also ignores the means and method and concludes by analyzing the results of the damage caused.[324] From a contextualized perspective, Reisman and Myres McDougal argue that coercions should be categorized in legal and illegal coercions, [325] based on the characteristics amplifying or

315. *See* Roscini, *supra* note 125, at 236.
316. Bond, *supra* note 242, at 83-84.
317. BROWNLIE, *supra* note 252, at 362.
318. *See* Roscini, *supra* note 125, at 238.
319. Ziolkowski, *supra* note 295, at 69-70.
320. *Id.*
321. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion 1996 I.C.J. 226, ¶ 39 (July 8).
322. *See* Dinniss, *supra* note 6, at 62.
323. Schmitt, *supra* note 302, at 912.
324. *Id.* at 914.
325. MYRES S. MCDOUGAL & FLORENTINO P. FELICIANO, LAW AND MINIMUM WORLD PUBLIC ORDER: THE LEGAL REGULATION OF INTERNATIONAL COERCION 153 (1961).

undermining the world order.[326] By bridging the contextualist and result-based approaches, Schmitt concludes that a number of factors—severity of damage, measure of damage immediacy of consequences, directness, invasiveness, presumptive legitimacy, and responsibility—determine whether the subject's actions can be considered the use of force.[327] Jason Barkham has criticized Schmitt's inclusion of presumptive legitimacy, where permissive actions can be presumed illegitimate; he simply states that legitimacy should be determined by the rules of international law and not be presumed.[328] However, according to Oliver Corten and Dinniss, this subjective approach in law creates uncertainty in international law, which is an even greater threat to the peace and stability in the world.[329]

7. Positivist Approach

In the positivist approach, writers such as Yoram Dinstein, Ian Brownlie, and Christine Gray argue that anything that is not covered in the prohibition on the use of force is legally allowed and permitted.[330] However, such conclusions create a gray area to be exploited by aggressive states, where developed nations can use their international influence to subjugate developing nations to serve their own political interests, compromising the political independence and sovereignty of victim states. However, it is pertinent to note that the positivist approach is limited to the context of the Article 2(4) prohibition of the use of force in other states.[331] Therefore, threats to political independence and sovereignty other than the use of force can still be treated as a threat to the international peace and security of the world;[332] from a positivist approach it should just not be included within the parameters of using force.

326. W.M. Reisman, *Criteria for the Lawful Use of Force in International Law*, 10 YALE J. INT'L L. 279, 282 (1985); *see also* Michael N. Schmitt, *The Resort to Force in International Law: Reflections on Positivist and Contextual Approaches*, 37 A.F. L. REV. 105, 120 (1994).

327. Schmitt, *supra* note 302, at 914.

328. Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. 57, 85 (2001).

329. Oliver Corten, *The Controversies over Customary Prohibition on the Use of Force: A Methodological Debate*, 16 E.J.I.L. 812, 814 (2005); *see* Dinniss, *supra* note 6, at 62.

330. *See* Dinniss, *supra* note 6, at 62.

331. *See* GRAY, *supra* note 253, at 9.

332. U.N. Charter art. 2.

8. Factors Influencing Cyberattacks

Dinniss has identified four key factors that influence the legitimacy of cyberattacks: "indirectness, intangibility, locus and result."[333] Under "indirectness," cyberattacks can have indirect knock-on effects, such as changing the settings of a dam to release floodwater, or they can use proxies to indirectly present an innocent state as the culprit of such attacks.[334] Under the laws of the use of force, indirect assistance to armed activities through assistance can be considered the use of force.[335] Under "intangibility," Dinniss notes that the nature of cyberattacks is such that often "the target, the weapon used and as well the damage caused" are intangible and only exist in cyberspace or a nonphysical form, such as targeting information systems, collapsing systems, and manipulating them by computer code.[336] Here a weapon can be described as something used to gain advantage in a conflict, causing damage to property or persons.[337] Under this definition, malicious cyber code used in a cyberattack/ cyberwarfare, causing damage to property, can be considered a weapon.[338] Consider the criminal law analyses of a weapon; for instance, a wrench in the hand of a mechanic can be considered only a tool, or also a weapon for murder if used for striking the life out of a victim, based on its use and consequential results.[339] In a very similar fashion, computer code can be considered a weapon of choice if it is used with the intention and result of destroying property or life.[340] Under "locus," a cross-border use of force is necessary to violate the prohibition on the use of force.[341] Dinniss argues that, although cyberspace does not come under any jurisdiction, and the conclusive attribution is difficult and often impossible to establish, the cyberattacks do cross the borders of different states.[342] For instance, the perpetrators of cyberattacks use proxies of different countries before targeting victims, and usually the malware is sent by aggressive states into computer systems located in the sovereign territory of victim states.[343] Under "result," Dinniss maintains that, though the results of cyberattacks

333. *See* Dinniss, *supra* note 6, at 65.
334. *Id.* at 65-66.
335. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 225, 228 (June 27).
336. *See* Dinniss, *supra* note 6, at 67.
337. *Id.* at 69.
338. *Id.* at 70.
339. Bond, *supra* note 242, at 86.
340. *See* Dinniss, *supra* note 6, at 70.
341. *Id.*
342. *Id.* at 71.
343. *Id.*

are limited to targeting and destroying information systems and computer systems, they can still cause damage to property as well as to the life of human beings.[344] For instance, malfunctioning or DDoS attacks can stop life-sustaining systems in hospitals, causing death.[345] Likewise, the Israeli attack on the Syrian radar system that incapacitated Syria from detecting the aggression of Israeli fighter jets caused the deaths of Syrian civilians.[346] Cyberattacks can also cause damage to property; for example, the cyberattacks from Israel and the United States caused destruction of Iranian nuclear centrifuges.[347]

Therefore, Dinniss concludes that the tangibility of weapon of choice is irrelevant in considering whether cyberattacks can be considered the use of force.[348] Instead, she believes that the severity of damage caused in terms of destruction to property and human lives by cyberattacks determines whether the attack is a use of force or not.[349] For instance, if the physical results of a cyberattack are minimal, it cannot be considered a use of force, and if its results are grave, then it can be considered a use of force. [350] But this does not establish that lesser consequences by cyberattacks are permissible by the principle of international law; less-serious cyberattacks may still violate the principle of non-intervention and the principle of sovereignty and can still be considered a threat to international peace and security.[351]

C. Armed Attack and Self-Defense

Armed attacks are the uses of force by armed bands, with sufficient gravity of scale and effect beyond mere frontier skirmishes.[352] The UNGA has defined aggression as "the most serious and dangerous form of the illegal use of force," including nondestructive actions such as breaching a treaty, providing land to an aggressor, and allocating a naval blockade.[353] ICJ also established that "arming and training armed groups" is also a use

344. *Id.* at 72.
345. Toure, *supra* note 46, at 7.
346. John Leyden, *Israel Suspected of 'Hacking' Syrian Air Defences*, REGISTER (Oct. 4, 2007), https://www.theregister.co.uk/2007/10/04/radar_hack_raid/.
347. *See* Dinniss, *supra* note 6, at 81.
348. *Id.* at 74.
349. *Id.*
350. *Id.*
351. *Id.*
352. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27).
353. G.A. Res. 3314 (XXIX), *supra* note 248, at 143.

of force.[354] The use of force in self-defense is allowed against a more serious use of force amounting to an armed attack; a lesser form of armed attack is still an illegal use of force but does not create a right to use force in self-defense.[355] This scale of using force from lesser forms to graver forms is mainly to maintain the peace of the world.[356] However, there are two kinds of scholars: those who interpret the right to self-defense expansively and those who interpret it narrowly.[357] Scholars also argue that victim states have the right to take responsive measures even in response to lesser forms of force in a proportional manner.[358]

For instance, in an expansive view, in the *Oil Platform* case, Judge Simma argued that victim states should not be forced to not defend themselves against the use of force against them, because the principle of proportionality is able to contain escalation of incidents.[359] Russia also takes an expansive view when dealing with the right to self-defense in cyberattacks, because it doesn't differentiate between graver and lesser forms of armed attack.[360] The United States takes a narrow view for dealing with the right to self-defense in cyberattacks.[361] It said that,

> if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no-one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack.[362]

Schmitt is of the narrow view; he says that, in cases of cyberattacks where the intentions of the perpetrators is to cause the destruction of property or human life (armed attacks that threaten the stability and peace of the world), the right to self-defense is permissible.[363] On the other hand, Sharp, from an expansive view, believes that right to self-defense and the

354. Nicar. v. U.S., 1986 I.C.J. ¶ 228.

355. *Id.* ¶ 191.

356. Michael N. Schmitt, *The Sixteenth Waldemar A. Solf Lecture in International Law*, 176 MIL. L. REV. 364, 419 (2003).

357. *Id.*

358. Oil Platform Case (Iran v. U.S.), Opinion of Judge Simma, 2003 I.C.J. 167, ¶ 12 (1996).

359. Iran v. U.S. 2003 I.C.J. ¶ 12; ROSALYN HIGGINS, PROBLEMS AND PROCESS: INT'L LAW AND HOW WE USE IT 242 (1994); John L. Hargrove, *The Nicaragua Judgment and the Future of the Law of Force and Self-Defense*, 81 AM. J. INT'L L. 135, 141 (1987).

360. *See* Dinniss, *supra* note 6, at 54.

361. *Assessment*, *supra* note 223, at 483.

362. *Id.*

363. Schmitt, *supra* note 302, at 907.

responsive use of force should be allowed even in circumstances that do not cause damage to property and human life but instead interfere with information that is critical to national security;[364] he argues that the non-armed use of force, such as cyberattacks on critically important infrastructure, has the capacity to cause even more damage than actual/physical armed attacks.[365] Conversely, the international community does not share Sharp's expansive interpretation of cyberattacks, instead the international law sees such intrusions as acts of espionage and not as the use of force or as armed attacks.[366]

On theoretical grounds, Dinniss shares the narrow interpretation, which allows the use of responsive force only in situations of grave forms of armed force.[367] In this approach, most cyberattacks—even those that cause damage to property or human life as lesser forms of use of force—do not amount to armed attacks; therefore, there is no right to self-defense against them.[368] For instance, the cyberattacks in Estonia in 2007 and the Stuxnet virus in 2010 did cause damage to intrinsic government properties and can be considered uses of force.[369] But, since the gravity of the destruction they caused was moderate, they did not amount to an armed attack and did not give rise to the right to the responsive use of force in self-defense.[370] However, there remains a question of attribution in cyberattacks, since most cyberattacks cannot be attributed to a state and are conducted by nonstate actors, and there is no right to self-defense against the use of force by nonstate actors until and unless their actions are attributable to a state.[371] Similarly, for all cyberattacks, if attribution to a state is not conclusive, there is no right to self-defense against any cyberwarfare.[372]

In conclusion, the defensive use of force against cyberattacks is only permissible in cases that amount to an equivalent damage of an armed attack, which entails a graver form of the use of force, with the severe effects and scale of destruction of property and human life.[373] However, this Article concludes that, even in lesser forms of the use of force with

364. SHARP, *supra* note 310, at 129.
365. *Id.* at 133.
366. *See* Dinniss, *supra* note 6, at 81.
367. *Id.*
368. *Id.*
369. ALBRIGHT ET AL., *supra* note 198, at 10; *see also* Dinniss, *supra* note 6, at 81.
370. *See* Dinniss, *supra* note 6, at 81-82.
371. *See* Bussolati, *supra* note 182, at 121; *see* GRAY, *supra* note 253, at 99; Dinniss, *supra* note 6, at 96.
372. *See* Dinniss, *supra* note 6, at 96, 101.
373. *Id.* at 113.

cyberattacks that can destroy property or human life, a victim state has the right to self-defense, and the right to employ similar and proportionate use of force, be it in the form of responsive cyberattacks or by claiming rightful sovereignty and political independence. Lesser forms of the use of force with cyberattacks do violate the principle of nonintervention and the prohibition on the use of force, and therefore, a victim state can either take proportionate countermeasures or appeal to the Security Council to take appropriate measures against the aggressor state.[374]

V. CONCLUSION

Though the legal international framework was formed before the advent of the information age, the international law of using force under the U.N. Charter is well applicable to cyberattacks and cyberwarfare.[375] This Article concludes that the use of cyberattacks can be considered the use of force and, as armed attacks, can violate Article 2(4) of the U.N. Charter and can give rise to the right to self-defense under Article 51 of the U.N. Charter, when the gravity of their destruction of property or human life is equivalent to the destruction caused by kinetic weapons.[376] Moreover, cyberattacks entailing the nonphysical destruction of property and life, such as disabling CNI/services by cyberattacks, is also the use of armed force[377] in the form of coercions. Under the *Tallinn Manual*,[378] result-based and target-based approaches categorize most cyberattacks as armed attacks, with the qualification giving rise to the right to use responsive force in self-defense,[379] keeping in mind the principle of proportionality. Hitherto, the most rigorous challenge regarding the legitimacy of the responsive use of force entails that aggressive armed attack via cyberattack is conclusively attributable to a state. Without attribution, there can be no self-defense against states—or nonstate actors residing in other countries—without the consent of that state.[380] The principle of attribution acts as a gray area in international law for the purposes of cyberattacks; therefore there has been a rise of nonstate actors acting independently, or as a proxy of other states, rendering it very difficult for victim states to respond in self-defense.[381]

374. *Id.*
375. *See* Roscini, *supra* note 125, at 253.
376. Schmitt, *supra* note 2, at 588; *see* Dinstein, *supra* note 289, at 103.
377. *See* Roscini, *supra* note 125, at 253-54.
378. *See* SCHMITT, *supra* note 8, at 54.
379. Schmitt, *supra* note 2, at 589.
380. *See* Bussolati, *supra* note 182, at 119-20.
381. *Id.* at 126.

Further, states' intended cyberattacks[382] with lesser gravity, not destroying life or property and not disabling CNI/services, but coercing states into doing something that the victim country is free to do or not do,[383] may still violate the principle of sovereignty and the principle of nonintervention in internal affairs of a country.[384] Moreover, cyberattacks on information can be considered espionage, and they also violate the sovereignty of a state, but such attacks cannot be considered the use of force or an intervention in other countries, because such attacks have no destructive capabilities and they do not coerce states into doing something upon matters upon which they are free to decide.[385] Information-targeting cyberattacks not amounting to the use of force can instead be considered espionage, as international crimes, and as threats to the peace, security, and stability of the international community.

382. Corfu Chanel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. 18 (Apr. 9).

383. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).

384. *See* Roscini, *supra* note 125, at 253-54.

385. *Id.*