Article

Cyber–Conflict, Cyber–Crime, and Cyber–Espionage

David Weissbrodt*

I. INTRODUCTION

Computers and the Internet have changed and are continuing to change the way governments, militaries, businesses, and other organs of society manage their activities. While computers can improve efficiency, they are vulnerable to cyber–attack, cyber–crime, and cyber–espionage.[1] The international community, states, and businesses are still adapting to the unique set of challenges posed by cyber–attack, cyber–crime, and cyber–espionage. States are creating military operations that specialize in cyber–attack and defense to adapt to these relatively new threats to national security operations. [2]

* Regents Professor and Fredrikson & Byron Professor of Law, University of Minnesota Law School. The author thanks Quin Ryan for her assistance on this article. This Article was prepared for the *Minnesota Journal of International Law's* 2013 Symposium. To see a video recording of the discussion that took place, please see the *Minnesota Journal of International Law's* website, http://www.minnjil.org/?page_id=913.

1. *See generally* J. Nicholas Hoover, *Cyber Attacks Becoming Top Terror Threat, FBI Says*, INFO. WK., Feb. 1, 2012, http://www.informationweek.com/news/government/security/232600046 (emphasizing the increasing importance of cyber–attacks in modern national security concerns).

2. *E.g.*, Joanna Stern & Luis Martinez, *Pentagon Cyber Command: Higher Status Recommended*, ABC NEWS, May 2, 2012, http://abcnews.go.com/Technology/pentagon–cyber–command–unit–recommended–elevated–combatant–status/story?id=16262052 (discussing the United States' own "Cyber Command Unit" known as CYBERCOM, currently under the purview of the U.S. Strategic Command). Estonia created the Cyber Defense League in response to the DDoS attacks in 2007. Tom Gjelten, *Volunteer Cyber Army Emerges in Estonia*, NPR, Jan. 4, 2011, http://www.npr.org/2011/01/04/132634099/in–estonia–volunteer–cyber–army–defends–nation, *see infra* part II.A (outlining the DDoS attacks in 2007). Iran announced the creation of its own military cyber–unit in 2011. *Cyberattacks on Iran—Stuxnet and Flame*, N.Y. TIMES, updated Aug. 9, 2012, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html. The United Kingdom developed the Defense Cyber

In the United States there have been multiple attempts to address the flaws in the existing legal structures in order to better address the threat posed by computer network operations.[3] The first legislative attempt was in April 2012, when the United States House of Representatives passed a cyber–security bill "which called for more information sharing between national security and intelligence agencies and businesses."[4] A few months later a second cyber–security bill was introduced in the Senate, which would establish "optional standards for the computer systems that oversee the country's critical infrastructure."[5] Unable to reach a compromise in the legislature, President Barack Obama reportedly signed Policy Directive 20 which established "a broad and strict set of standards to guide the operations of federal agencies in confronting threats in cyberspace."[6] The directive provides much needed updates to cyber–security protocols in part by distinguishing between network defense and cyber operations;[7] however, it does not replace the need for legislative action to protect private networks.[8] At the international level the lack of standards is even more pronounced and the tenuous applicability of international legal paradigms to cybersecurity issues creates uncertainty and difficulty in pursuing any

Operations Group, and also has two units which are working on an offensive capability to strike back at enemies trying to launch electronic attacks. Duncan Gardham, *Britain Prepares for Cyber War*, TELEGRAPH, Nov. 25, 2011, http://www.telegraph.co.uk/news/uknews/defence/8915871/Britain–prepares–for–cyber–war.html.

3. *See generally* Michael S. Schmidt, *Cybersecurity Bill is Blocked in Senate by G.O.P. Filibuster*, N.Y. TIMES, Aug. 2, 2012, http://www.nytimes.com/2012/08/03/us/politics/cybersecurity–bill–blocked–by–gop–filibuster.html; *see also* Ed O'Keefe & Ellen Nakashima, *Cybersecurity Bill Fails in Senate*, WASH. POST, Aug. 2, 2012, http://www.washingtonpost.com/world/national–security/cybersecurity–bill–fails–in–senate/2012/08/02/gJQADNOOSX_story.html.

4. Schmidt, *supra* note 3; *see also* O'Keefe & Nakashima, *supra* note 3 (discussing other legislative efforts prior to the cyber–security bill the article focuses on).

5. Schmidt, *supra* note 3; *see generally* O'Keefe & Nakashima, *supra* note 3 (explaining the procedural issue the bill ran up against in the Senate).

6. Ellen Nakashima, *Obama Issues Guidance on Cyberwarfare*, WASH. POST, Nov. 15, 2012, at A7.

7. Network defense is what is done within one's own network, and cyber–operations are actions taken outside of one's own network space. The distinction is expected to help guide officials actions and authorize some cyber–operations that are defensive in nature. *Id.*

8. *Id.* (outlining the need for additional cyber–security policy for the private sector, either in the form of legislative action, or executive order).

standards or norms.

The legal challenge of addressing cyber operations is complicated by the broad variety of computer network operations possible and by the broad variety of potential actors. A computer network operation could be perpetrated by a lone hacker who shuts down a government website. That operation may require a much different response than when a computer network operation, executed by government agents, causes a gas pipeline to explode in another country. Identifying a computer network operation as a use of military force or armed attack may be analyzed under the United Nations Charter while other computer misuse may be assessed as espionage or other criminal offenses, depending upon issues of scale, attribution, intent, and consequences. Identifying the different types of computer network operations, as a cyber–attack, cyber–crime, or cyber–espionage is important in analyzing an appropriate legal response.

This Article explores different types of computer network operations and the scope of existing legal paradigms that can be applied to computer network operations. This Article examines three recent examples of computer network operations and analyzes the situations to determine the types of computer network operation and what, if any, legal operations apply. Finally, this Article discusses the limitations of existing legal paradigms, and analyzes the attributes and weaknesses of the three more prominent proposals for addresses regulation of international computer network operations.

II. ESTONIA, STUXNET, AND FLAME: EXAMPLES OF INTERNATIONAL COMPUTER NETWORK OPERATIONS

A. ESTONIA

On April 27, 2007, Estonian officials moved a Soviet–era memorial celebrating an unknown Russian who died fighting the Nazis during World War II.[9] The memorial had long been a gathering place for both Russian and Estonian nationalist groups, so officials moved the memorial from Central Tallinn to

9. *Estonia Removes Soviet Memorial*, BBC NEWS, Apr. 27, 2007, http://news.bbc.co.uk/2/hi/europe/6598269.stm (specifying the date the statue was moved, and the significance of the statue); Daniel J. Ryan et al., *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161, 1164 (2011).

the Tallinn Military Cemetery outside of town.[10] In anticipation of the move, thousands of ethnically Russian Estonians protested.[11] The protests eventually turned violent, and led to rioting, hundreds of arrests, and one death.[12] This event began a series of Distributed Denial–of–Service (DDoS)[13] attacks launched against several Estonian national websites.[14] Estonian government websites that would generally receive 1,000 visits a day were receiving 2,000 visits every second, causing the websites to be shut down for several hours at a time.[15] The attacks became more sophisticated and persisted for several weeks until NATO and the United States sent security experts to Estonia to investigate and protect the computers from further attack.[16] Estonia initially blamed the Russian government for the attacks;[17] others claimed that Russia worked with cyber–criminals making their large botnets[18] available for misuse.[19] At this time investigations indicate the attacks were not affiliated with the Russian government, but rather the product of "spontaneous anger from a loose federation of separate attackers."[20]

10. Ryan et al., *supra* note 9, at 1164; *Estonia Removes Soviet Memorial*, *supra* note 9.

11. *See* Ryan et al., *supra* note 9, at 1164; *Estonia Removes Soviet Memorial*, *supra* note 9.

12. *See* Ryan et al., *supra* note 9, at 1164; *Estonia Removes Soviet Memorial*, *supra* note 9.

13. Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 444–45 (Spring 2012) define Distributed Denial–of–service (DDoS), as a DoS that launches requests simultaneously from multiple computers, creating a much larger scale attack on the targeted computers or websites than a simple DoS attack. DoS is a type of cyber–attack that cripples the computer or websites' processing speeds or completely preventing a user from using the system by overwhelming the target with data and requests, *id.* DDoS attacks can also be combined with other types of attacks such as malicious software, *see id.* at 442–43; *see infra* note 52.

14. CLAY WILSON, CONG. RESEARCH SERV., RL 32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 7 (2009).

15. *Id.*

16. *Id.*

17. *Id.* at 8.

18. "Botnets, or 'Bot Networks,' are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely–controlled through commands sent via the Internet." *Id.* at 5; *see also*, Kesan & Hayes, *supra* note 1313, at 443 (describing potential overlap between Botnets, DDoS attacks, and other types of malicious code).

19. WILSON, *supra* note 14, at 8.

20. *Id.*

B. STUXNET

On June 1, 2012, officials of President Barack Obama's administration admitted that the computer worm,[21] Stuxnet, was a joint project between the United States and Israel designed to disrupt Iran's nuclear program.[22] The "Olympic Games" program[23] began in 2006 under President George W. Bush's administration and flourished under the Obama administration.[24] The Stuxnet worm, developed within Olympic Games, was first introduced into the Iranian computer system in 2008, at an underground facility at Natanz, through an employee's flash drive.[25] Stuxnet was designed to suddenly speed up or slow down the spinning of centrifuges used to enrich uranium, causing their parts to break and thereby crippling the entire uranium enrichment operation.[26] The most impressive aspect of the Stuxnet worm was that while it was changing the speeds of the centrifuges, the computers in the operation room would report normal functioning of the centrifuges indicating no problems.[27]

The Stuxnet operation was working successfully until an error in the programming[28] allowed the worm to be released after infecting an engineer's computer. The engineer took his

21. Stuxnet is more accurately described as a "rootkit." Kesan & Hayes, *supra* note 13, at 442–43l. Rootkits are malicious software programs which use system modification to hide files, processes, programs, and behaviors. *Id.* at 442.

22. David E. Sanger, *Obama Order Sped up Wave of Cyberattacks Against Iran*, N.Y. TIMES, Jun. 1, 2012, at A1.

23. "Stuxnet" is the name given to the malicious code by computer security experts studying the worm. *Id.* "Olympic Games" is the name given to the program under which Stuxnet was developed by the Bush administration. *Id.*

24. *Id.*

25. *Id.* (explaining how Stuxnet was introduced into Iran's underground nuclear facility, and how crucial the "beacon" virus, which was used to collect information about Iran's nuclear facility, was to designing Stuxnet to attack Iran's nuclear industrial control systems); *see also* Nicole Perlroth, *Researchers Find Clues in Malware*, N.Y. TIMES, May 30, 2012, http://www.nytimes.com/2012/05/31/technology/researchers–link–flame–virus–to–stuxnet–and–duqu.html?_r=2&ref=stuxnet& (noting that researchers believe the Duqu virus, was the "beacon" behind gathering the information necessary to develop stuxnet); *Duqu: Steal Everything*, KAPERSKY LAB, http://www.kaspersky.com/about/press/duqu (explicating the scope and threat of the Duqu virus).

26. Sanger, *supra* note 22.

27. *Id.*

28. The exact source of the programming error is unknown; some within President Obama's administration blame the Israeli programmers. *Id.*

computer home with him, and the worm spread when he connected to the Internet, thereby infecting over 100,000 computers worldwide and exposing Stuxnet to the public.[29] Stuxnet's intent and objective were not immediately clear to those persons who encountered it. After much consideration the Obama administration decided to continue the Stuxnet attacks since the worm was still effectively dismantling the Iranian nuclear program.[30] The overall effectiveness of Stuxnet is unclear, with the United States government arguing that it delayed Iran's nuclear development by one–and–a–half to two years,[31] while others report that Iran was able to successfully contain much of the damage caused by Stuxnet.[32] Stuxnet was programmed to self–destruct on June 24, 2012.[33]

C. FLAME

On May 28, 2012, the Kaspersky Lab[34] in Moscow announced the discovery of malicious software codenamed Flame.[35] The primary function of Flame is to collect information.[36] Flame steals valuable information from infected

29. *Id.*; *see also* NICOLAS FALLIERE ET AL., SYMANTEC SEC. RESPONSE, W32.STUXNET DOSSIER 5 (2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; *The Stuxnet Outbreak: A Worm in the Centrifuge*, ECONOMIST, Oct. 2, 2010, at 63 (claiming that 45,000 computers had been infected with Stuxnet); Wayne Madsen, *Stuxnet: A Violation of US Computer Security Law*, OPINION MAKER (Jan. 22, 2011), http://www.opinion–maker.org/2011/01/stuxnet–a–violation–of–us–computer–security–law/ (arguing that over 100,000 computers had been infected with Stuxnet).

30. *See* Sanger, *supra* note 22.

31. *Id.*

32. *See* Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifcation to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842, 858 (2012). *But see id.* at 859 (arguing that even if Iran contained much of the damage, they were harmed in other ways such as shortage of certain metals needed for the machines and the psychological impact of having a secure facility infiltrated).

33. *Id.* at 856.

34. Kaspersky Lab is a Russian producer of antivirus software. Thomas Erdbrink, *Iran Confirms Attack by Virus that Collects Information*, N.Y. TIMES, May 29, 2012, at A4.

35. *Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat*, KASPERSKY LAB (May 28, 2012), *available at* http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat [hereinafter *Kapersky Lab*] (announcing the discovery of the malicious program codenamed Flame, found during an investigation prompted by the International Telecommunications Union).

36. *Id.*

computers ranging from, but not limited to, computer display contents, documents, stored files, password information, contact data, audio conversations, and monitoring of Skype.[37] The Kapersky Lab found that "[t]he complexity and functioning of the newly discovered malicious program exceed those of all other cyber menaces known to date."[38] One reason is size. In comparison to a study done in 2010, Flame, which is believed to have been introduced in 2010,[39] is nearly sixty times the average size of other known malicious programs.[40] Kaspersky Lab researchers announced that while it is likely that Flame is part of the same campaign as Stuxnet, it appears to have been written by a different group of programmers.[41] When Flame was discovered, Kaspersky found that most of the infected computers were in the Middle East.[42] Iran had the highest number of Flame infections; Israel, the Palestinian territories, Sudan, Syria, and Lebanon also had substantial numbers of infected computers.[43] Many commenters suspect that Israel is responsible for the Flame program, and while Israel has not taken responsibility for Flame, they have also done little to deflect suspicion.[44] The Washington Post has also asserted that

37. *See* Erdbrink, *supra* note 34; *Kaspersky Lab*, *supra* note 35.

38. *Kaspersky Lab*, *supra* note 35.

39. *Id.* ("Preliminary findings indicate that this malware has been 'in the wild' for more than two years – since March 2010."). *But see* Erdbrink, *supra* note 34 (suggesting that Flame is at least five years old).

40. Amy Teibel, *Flame Virus: Suspicion Falls on Israel*, IOL.COM (May 30, 2012) http://www.iol.co.za/scitech/technology/security/flame–virus–suspicion–falls–on–israel–1.1308148.

41. *See Cyberattacks on Iran—Stuxnet and Flame*, *supra* note 2; *see also Kaspersky Lab*, *supra* note 35 ("Although the features of Flame differ compared with those of previous notable cyber weapons such as Duqu and Stuxnet, the geography of attacks, use of specific software vulnerabilities, and the fact that only selected computers are being targeted all indicate that Flame belongs to the same category of super–cyberweapons.").

42. Ellen Nakasima, *Iran Acknowledges that Flame Virus has Infected Computers Nationwide*, WASH. POST, May 29, 2012, http://www.washingtonpost.com/world/national–security/iran–acknowledges–that–flame–virus–has–infected–computers–nationwide/2012/05/29/gJQAzlEF0U_story.html.

43. *Id.* (noting that there were few instances of infected computers outside the Middle East, and that Kaspersky data is limited to infections reported by their customers).

44. Israel's vice prime minister, Moshe Yaalon, drew attention with his comment that "[w]hoever sees the Iranian threat as a significant threat is likely to take various steps, including these, to hobble it . . . . Israel is blessed with high technology, and we boast tools that open all sorts of opportunities for us." Tiebel, *supra* note 40.

Flame is part of the joint United States–Israeli operation that was launched prior to Stuxnet in order to secretly map Iran's computer networks in preparation for the Stuxnet attacks.[45]

How should these three different computer network operations be characterized? How should computer network operations be characterized more generally? Should computer network operations be considered a use of force or an armed attack under the U.N. Charter? When should computer network operations be considered a criminal offense? When should they be considered espionage? While analyzing each of these issues we will revisit the Estonian attack, the Stuxnet worm, and Flame in order to determine how these situations should be understood under international law. In order to understand how they are characterized we must first define what constitutes a computer network operation.

III. WHAT ARE COMPUTER NETWORKS OPERATIONS?

Computer network operations (CNOs) have been defined by the United States Joint Chiefs of Staff as being used to "attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure."[46] The term CNO will therefore be used in this Article to describe any type of online or computer intrusion or defense. In order to more narrowly describe each type of CNO for the purposes of this Article, cyber–attack will be used broadly to describe CNOs that include attacks which fall under the law of war and cyber–crime attacks. The term cyber–crime will refer to any "crime which is enabled by, or that targets computers."[47] Cyber–espionage will be used to describe computer operations which are used for intelligence and data collection from target or adversary computer systems.[48]

Additionally there are three main categories of the

45. Ellen Nakashima et al., *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASH. POST, June 19, 2012, http://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 supra* part II.B (discussing the history of Stuxnet and the Olympic Games program).

46. CYBERCRIMES: A MULTIDICIPLINARY ANALYSIS 192-93 (Sumit Ghosh & Elliot Turrini, eds., 2010) (citing UNITED STATES JOINT CHIEFS OF STAFF, INFORMATION OPERATIONS, 3–13 (Joint Chiefs of Staff, Feb. 13, 2006), *available at* http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf).

47. WILSON, *supra* note 14, at 4.

48. *Id.* at 12.

mechanism of CNOs: malicious software, unauthorized remote intrusions, and DoS attacks.[49] Malicious software or malware usually infects computers through infected emails or websites modifying the programs to carry out functions that were not originally intended.[50] Unauthorized remote intrusions occur when the attacker is able to access a computer through account names and/or passwords and is then able to disrupt the computer and data within.[51] Third, DoS attacks overwhelm the targeted computer system with requests and information until it ceases to function, thereby denying access to legitimate users.[52] Any of these CNOs may be specifically tailored for a particular purpose which further complicates the identification of which legal paradigm should apply to a particular CNO.

IV. LEGAL PARADIGMS FOR COMPUTER NETWORK OPERATIONS

A. THE U.N. CHARTER AND USE OF FORCE

Article 2(4) of the U.N. Charter sets forth the fundamental international law prohibition on the use of force, stating that, "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[53] There are two exceptions to the prohibition on the use of force in Article 2(4). First, Articles 39 and 41 provide that the U.N. Security Council may take action by air, sea, or land forces to maintain or restore international peace and security.[54] Second, Article 51 also authorizes use of force in self–defense, stating

49. Kesan & Hayes, *supra* note 13, at 442; Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 13–14 (2009). *Cf.* LEHTINEN ET AL., COMPUTER SECURITY BASICS 79–95, 112–33 (2d ed. 2006) (categorizing cyber–attacks in two groups: viruses and Internet vulnerabilities); ANDREW COLARIK, CYBER TERRORISM, POLITICAL AND ECONOMIC IMPLICATIONS 84 (2006) (categorizing cyber–attacks into 4 groups: viruses, denial–of–service attacks, web defacements, and unauthorized penetration).

50. *See* Sklerov, *supra* note 49, at 15–17 (explaining the range of malicious software, including viruses, worms, Trojan horses, rootkits, exploits, and zombies).

51. *Id.* at 17.

52. *Id.* at 16–17; *see also id.* at 16 (describing DDoS attacks, which launch coordinated attacks from multiple computers).

53. U.N. Charter art. 2, ¶ 4.

54. U.N. Charter art. 39, 41.

that, "nothing in the present Charter shall impair the inherent right of individual or collective self–defense if an armed attack occurs against a Member of the United Nations."[55] Under these fundamental provisions no nation may use force against another nation unless it is authorized by the U.N. Security Council or is in self–defense against an armed attack.

These U.N. Charter provisions can be applied to cyber–attacks. There has been an international consensus among scholars and the U.N. that cyber–attacks may be understood under the U.N. Charter even though such an attack is not explicitly mentioned in the Charter.[56] Articles 2(4), 39, 42, and 51 do not list or refer to any specific weapons but the International Court of Justice in its advisory opinion on nuclear weapons found that these provisions "apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon . . . ."[57] The court went on to hold that the rules of war under the U.N. Charter apply even as new weapons are introduced that were not originally considered or even imagined by the drafters of the Charter.[58] In May 2011, the United States Department of Defense concluded in its first formal cyber–strategy that the laws of armed conflict can be expanded to include cyber–warfare thereby allowing the application of both Article 2(4) and Article 51 to cyber–attacks.[59] While there is a consensus that the U.N. Charter provisions may be applied to cyber–attacks, the more complex question is under what circumstances should the provisions be applied, and which article will be applied. Under the U.N. Charter conflicts are generally divided into Article 2(4) conflicts which involve a violation of the use of force prohibition, Articles 39 and 42 conflicts when the Security Council authorizes use of force, and Article 51 conflicts which authorize nations to act in

55. U.N. Charter art. 51.

56. Stephanie Gosnell Handler, *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, 48 STAN. J. INT'L L. 209, 216–19 (2012).

57. Legality of the Threat of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 22, ¶ 39 (July 8).

58. *Id.* at 35, ¶ 78; Handler, *supra* note 56, at 217.

59. *See* Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 30, 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html; Ed Pilkington, *Washington Moves to Classify Cyber–Attacks as Acts of War: US Sees Option of Armed Retaliation as Deterrent Concern over Practical and Legal Implications*, GUARDIAN, June 1, 2011, at 2.

self–defense to an armed attack.[60]

1. Prohibition on the Use of Force: Article 2(4)

The drafters of the U.N. Charter intended to prohibit all types of force, except when done in self–defense or as authorized by the U.N. Security Council.[61] The Security Council was intended to be the primary body for determining when force should be used. It was also to have its own military force which could use force when needed to maintain international peace and security.[62]

What constitutes a threat of force under Article 2(4) is still relatively vague, but Professor Wingfield testified to the National Research Council's report drafting committee that some threats that might constitute "threats of force" under Article 2(4) include "verbal threats, initial troop movements, initial movements of ballistic missiles, massing of troops on a border, use of fire control radars, and interference with early warning or command and control systems."[63] Cyber–attacks will be compared to the items on this non–exhaustive list to determine whether they constitute a threat of force.

Today, there is no clear definition of what constitutes use of force.[64] The U.N. Charter does not define use of force, nor has any international body.[65] Some scholars have argued that giving the term "use of force" a definite meaning is an impossible task; the term is imprecise.[66] This imprecise

60. Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 995–96 (Summer 2011).

61. Jason Barkham, 34 N.Y.U. J. INT'L & POL. 57, 69 (2001); *see* RUTH B. RUSSELL, HISTORY OF THE UNITED NATIONS CHARTER 456–57, 673–75, 1067 (1958) (covering the intentions of key drafters of the U.N. Charter).

62. Andrew Miller, Note, *Universal Soldiers: U.N. Standing Armies and the Legal Alternatives*, 81 GEO. L.J. 773, 779–83 (1993); *see* Barkham, *supra* note 61, at 69.

63. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS, TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 242 (William A. Owens et al. eds., 2009).

64. For a discussion the history and progression of the legal understanding of the "use of force" see James N. Bond, Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality Under the United Nations Charter Article 2(4) 48–80 (June 14, 1996) (unpublished M.A. final report, Naval War College) (*available at* http://www.au.af.mil/au/awc/awcgate/navy/nwc_bond.pdf).

65. *Id.* at 50–51.

66. *Id.* at 51 ("I suffer from no delusions about giving this phrase [use of force] precise meaning either. It is an impossible task.").

meaning makes it difficult to determine if or when a cyber–attack should be considered "force."

Fortunately, there are some parameters to help identify use of force despite the lack of a precise definition. Attacks which utilize conventional weapons are considered to be the use of force under the U.N. Charter.[67] Attacks which cause damage to physical or real property or injury or death to humans are also considered to involve the use of force. The International Court of Justice also established in the case of *Nicaragua v. United States of America* that arming and training a rebel group constituted a use of force, but supplying of funds to a rebel group and United States military maneuvers held near the border did not involve the threat or use of force.[68] The court also found that the laying of mines by the United States in the territorial waters of Nicaragua constituted a use of force, but that use of force did not rise to the level of an armed attack.[69] Furthermore, international law has established that economic and political coercion are expressly excluded from the definition of the use of force, despite the attempts of developing states to include them.[70] Therefore, most scholars have determined that

67. *Id.* at 58; *see* Barkham, *supra* note 61, at 72.

68. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 227–38 (June 27) (determining that although these actions did not constitute a use of force under the U.N. Charter, it was an act of intervention); *see* Barkham, *supra* note 61, at 75.

69. *Id.* In 1949, the International Court of Justice found that Albania had "used force" against Britain. The British Royal Navy had swept the North Corfu Channel for mines to ensure that it was a safe route for navigation. On May 15, 1949, an Albanian gun battery fired at two British warships passing through the channel. The International Court of Justice determined that the firing at British ships constituted a use of force in violation of Article 2(4) of the U.N. Charter. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 12–14, 19, 27, 34–37 (Apr. 9) (Merits).

70. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 908 (1999); s*ee* Janie Chuang, *The United States as A Global Sheriff: Using Unilateral Sanctions to Combat Human Trafficking*, 27 MICH. J. INT'L L. 437, 459–60 (2006) (arguing that Article 2(4) does not bar economic intervention or non–forcible intervention); ADVISORY COUNCIL ON INTERNATIONAL AFFAIRS (AIV) & ADVISORY COMMITTEE ON ISSUES OF PUBLIC INTERNATIONAL LAW (CAVV), CYBER WARFARE 20 (2011) (hereinafter Advisory Council) ("Purely economic, diplomatic and political pressure or coercion is not defined as use of force under article 2, paragraph 4."). There is a minority viewpoint that economic force or political coercion should be considered force under Article 2(4). Charter of Economic Rights and Duties of States, G.A. Res. 3281(XXIX), U.N Doc. A/RES/29/3281, art. 32 (Dec. 12, 1974) (prohibiting states from using economic sanctions to subordinate a state's sovereign rights); Comment, *The Use of Nonviolent Coercion: A Study in*

economic force and political coercion do not constitute use of force under Article 2(4) while armed force does.

Scholars have proposed two primary approaches to determine when armed force has been used in violation of Article 2(4). Michael Schmitt has proposed a seven factor test in order to determine when state action constitutes armed force, prohibited under Article 2(4), and when it constitutes economic force or political coercion, and must be approached outside of the use of force limit of Article 2(4).[71] Schmitt's seven factor test includes: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[72] #1 Severity: When actions involve harm to individuals and property that alone will amount to use of force, while those that result in minor inconvenience or irritation will not.[73] Within this framework CNOs that impact critical national interests are more likely to constitute a use of force and the scale, scope, and duration of the effects will be considered when determining the severity of the attack.[74] #2 Immediacy: How quickly the effects occur after the CNO. #3 Directness: The greater connection between the attack and the effect the more likely it can be considered a use of force.[75] #4 Invasiveness: The more securely defended the system that is attacked the more likely it will be considered a use of force.[76] #5 Measurability: The more the impact of the CNO can be identified and quantified the more likely the state's interest is to be viewed as affected.[77] #6 Presumptive Legitimacy: If the activity has not been banned, then it is permitted.[78] #7 Responsibility: A state must be held responsible in order for the actions to be deemed a use of force.[79] Through this approach a CNO operation can be analyzed to determine if the CNO reaches the level of use of force or whether they are better

Legality Under Article 2(4) of the Charter of the United Nations, 122 U. PA. L. REV. 983, 988 (1974) ("This Comment will argue for a broad interpretation of the word 'force' in Article 2(4)—in particular, its extension to include political and economic coercion.").

71. Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569, 576–77 (2011).

72. *Id.*

73. *Id.* at 576.

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.* at 576–77.

78. *Id.* at 577.

79. *Id.*

placed outside the use of force boundary.[80] However, this test is not universally followed. Schmitt's analysis has been criticized by some scholars as being too subjective and needing too much information to be practically applied.[81]

The second proposed approach to determine when an activity qualifies as a use of force is to establish a broad, result–oriented analysis which looks at the impact of the actions, or the severity of the action, to see whether it constitutes a use of force.[82] According to Schmitt analyzing only the result of the attack, or the severity of consequences of the attack, is not sufficient to preserve the distinction between armed force and economic and political coercion; instead of being a mere interpretation of Article 2(4), it would constitute a new standard.[83] Under the result–oriented approach some economic force would be considered armed force due to its impact.[84] The results–oriented approach therefore conflicts with the current interpretation that use of force does not include economic force.[85]

2. Use of Force Authorized by the Security Council: Articles 39 and 42

The Security Council is authorized to use force when its members have determined under Article 39 that there has been a threat to the international peace, breach of the peace, or act of aggression.[86] Every threat or use of force under Article 2(4) is considered to be a breach of the peace under Article 39 of the U.N. Charter and the Security Council is therefore authorized to use force for any violation of Article 2(4).[87] The Security Council's power to authorize force extends beyond a state's violation of Article 2(4) and the Security Council may authorize force at a threshold that is considerably lower than Article 2(4).[88] Determining that there is a threat to the peace is a

80. *See* Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 448 (2009).

81. Barkham, *supra* note 61, at 85–87; Handler, *supra* note 56, at 229.

82. Schmitt *supra* note 62 at 917.

83. *Id.* at 917–19.

84. Barkham, *supra* note 61, at 86.

85. *Id.*

86. U.N. Charter arts. 39, 42.

87. THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 119 (Bruno Simma ed., 1994).

88. *Id.*

political decision, not a legal decision.[89] There are no territorial limits, requirement that a threat be a state action, or that violence needs to occur for the Security Council to determine that there is a threat to the peace.[90] Once the Security Council has made a threat to the peace determination, there is no mechanism for reviewing this decision; the Council's determination is final.[91] Scholars have concluded, based on Security Council decisions, that threats to the peace include but are not limited to extreme intrastate violence, severe human rights violations, apartheid, and cross–frontier expulsion of a large number of refugees.[92]

While the Security Council has full capacity to authorize the use of force when there is a threat to international peace, Article 39 determinations and recommendations to use force by the Security Council are difficult to achieve and are therefore rare.[93] The Security Council has the full authority to label any CNO a threat to the peace, but they are unlikely to do so.[94] Decisions to use force under Articles 39 and 42 are determined after extensive debates and deliberations, and during voting any decision to use force may be blocked through a veto made by any of the permanent members of the Security Council.[95] "In light of Russia's and China's presence on the Council (cyber operations regularly emanate from their territory), this limitation may well prove the greatest obstacle to effective U.N. action in the face of those cyber operations which would in some fashion endanger international stability."[96] Due to the extensive deliberations and permanent member veto it is

89. Schmitt, *supra* note 71, at 584.

90. *Id.*

91. *Id.*

92. WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE ix (Aegis Research Corporation 1999) at 150, http://www.cse.msstate.edu/~cse6243/readings/CyberSpace%20and%20the%20Use%20of%20Force%20–%20Sharp1999.pdf.

93. David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 88–89 (2010). The Security Council's activism has varied over time. During the Cold War (1949–1987) the Security Council established only thirteen peacekeeping operations. During the ten year period between 1988 and 1998 the Security Council sent 36 peacekeeping missions. Since this large increase following the end of the Cold War Security Council activism has leveled off and has not shown any large increases or decreases. DAVID WEISSBRODT ET AL., INTERNATIONAL HUMAN RIGHTS: LAW, POLICY, AND PROCESS 15 (4th ed. 2009).

94. Schmitt, *supra* note 71, at 584.

95. U.N. Charter, art. 27; Graham, *supra* note 93, at 89.

96. Schmitt, *supra* note 71, at 586.

unlikely that the Security Council would respond in a timely manner or even respond at all to a cyber–attack. Therefore, it is more likely for states to respond to cyber–attacks in self–defense without Security Council authorization.[97]

3. Armed Attack: Article 51

Article 51 permits the use of force in self–defense against an armed attack.[98] If the action does not rise to the level of an armed attack, states have no right to respond with force. If the action does not reach the threshold of an armed attack, then the victim state may only respond with non–forceful actions, countermeasures,[99] and seek recourse from the Security Council. The distinction between what constitutes a use of force and what amounts to an armed attack is important because an armed attack allows a victimized nation to respond with force.[100] According to the International Court of Justice in *Nicaragua v. United States of America*, an armed attack must exhibit certain "scale and effects."[101] Unfortunately, the court did not go on to determine the required criteria for when an attack reaches this threshold. Scholars have determined that with the contemporary methods of warfare an attack should be measured qualitatively and not quantitatively, so the determination is not dependent on the numbers affected by the attack but instead the overall scope of the attack.[102] Scholars have suggested several approaches to determining when an attack reaches the level of an armed attack, the

97. Kesan & Hayes, *supra* note 13, at 511 ("Because of the complicated nature of gaining Security Council approval for a use of force, some argue that it is more likely that a state would use self–defense to respond to a cyberattack in lieu of seeking Security Council approval.").

98. U.N. Charter art. 51.

99. U.N. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, *in* Rep. of the Int'l Law Comm'n, 53d sess, Apr. 23–June 1 & July 2–Aug. 10, 2001, art. 49 cmt. 1, U.N. Doc. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001), *available at* http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf ("Countermeasures may only be taken by an injured State in order to induce the responsible State to comply with its obligations under Part Two, namely, to cease the internationally wrongful conduct, if it is continuing, and to provide reparation to the injured State. Countermeasures are not intended as a form of punishment for wrongful conduct, but as an instrument for achieving compliance with the obligations of the responsible State under Part Two.").

100. U.N. Charter art. 51.

101. Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), 1986 I.C.J. 14, ¶ 195 (June 27) (Judgment).

102. *See* Schmitt, *supra* note 71, at 589.

instrumentality–based approach, the target–based approach and the consequence–based approach. The consequence–based approach has emerged as the dominant method for determining when the "scale and effects" have reached the required level to be considered an armed attack.

The first approach, which drafters of the U.N. Charter originally intended to be used, is to analyze the instrumentality that is used in the attack.[103] This approach focuses on what type of force the state is using. Since traditional instruments of force have been defined by their physical characteristics, such as a bomb, tank, or missile, this approach was originally appropriate.[104] Today, this approach is not applicable to cyber–attacks because they do not conform to the required physical characteristics. Cyber–attacks are conducted entirely through cyber–space and therefore lack the requirement of being a traditional military instrument.[105]

The second approach is known as the target–based approach and focuses on the intended target of the attack.[106] The target–based approach is simple to apply because if the attack is aimed at critical national infrastructure, it is considered to be an armed attack no matter what the actual damage is.[107] Allowing a use of force in response to a CNO which only meets the requirement of being aimed at critical national infrastructure would allow an expansion of the ability to use force in a manner not intended by the drafters of the U.N. Charter.

The third approach, which has the most support, is the consequence–based approach or equivalent–effects test. The consequence–based approach focuses not on what approach the country used but instead on the end result or the effect of the particular approach.[108] "Applying the consequence–based approach, armed attack must also be understood in terms of

103. Wolfgang McGavran, *Intended Consequences: Regulating Cyber Attacks*, 12 TUL. J. TECH. & INTELL. PROP. 259, 269–70 (2009).

104. Handler, *supra* note 56, at 227.

105. *Id.*

106. *Id.* at 228–29.

107. *Id.* Critical national infrastructure includes: government, information and communications, banking, food, water, public health, emergency services, defense industrial base, energy, transportation, chemical industry and hazardous materials, and posting and shipping. U.S. DEP'T OF HOMELAND SEC., NAT'L INFRASTRUCTURE PROTECTION PLAN 103 (2009).

108. Handler, *supra* note 56, at 228–29.

the effects typically associated with the term 'armed.'"[109] An attack is considered to be "armed" if it results in the death or injury to people or destruction of property and other tangible objects.[110] Under this approach the consequences of an attack, such as a cyber–attack, need to be analogous to the effects of a classic military operation.[111] Scholars emphasize different aspects of the attack including severity or destructive effects and immediacy to determine whether it rises to the level of a classic military operation, but under this approach the focus is on the consequences of the attack.[112] Cyber–space operations may by themselves constitute an armed attack, such as when a cyber–attack destroys its target.[113] CNOs may also support traditional military operations, aiding the fighters by disrupting enemy defenses thereby allowing forces to destroy the target without having to physically destroy their defense system.[114] Since the traditional military attack will generally constitute an armed attack, it is usually unnecessary to determine whether the cyber–attack would also be considered an armed attack thereby activating the right to self–defense. Since the consequence–based method is supported by most scholars to determine the requisite "scale and effects" to constitute an armed attack the situations discussed further in this article will be analyzed using this method.

Under Article 51, a classic military armed attack activates the target nation's right to respond in self–defense.[115] A nation responding to an armed attack must fulfill the requirements of necessity, proportionality, and immediacy. The principle of necessity requires that "non–forcible remedies must either prove futile *in limine* or have in fact been exhausted in an unsatisfactory manner."[116] The attack must be traced back to a

109. Michael N. Schmitt, *supra* note 71, at 588.

110. *Id.*

111. *Id.*

112. *See* Stephanie Gosnell Handler, *supra* note 56, at 228–29.

113. *Id.* at 216.

114. *See Id.*

115. U.N. Charter art. 51.

116. Yoram Dinstein, *Computer Network Attacks and Self–Defense, in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 109 (Michael N. Schmitt & Brian T. O'Donnell eds., Naval War College 2002); *see* Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 98 (2009) ("Necessity involves whether effective peaceful means of resolution exist[,] the nature of the aggression, each party's objectives, and the likelihood of effective intervention by the international community.").

specific source, the targeted nation must uncover the intention behind the attack to ensure that it was not an accident, and come to the conclusion that the state needs to respond with force.[117] Proportionality requires that the response should reflect a modicum of symmetry between the response and the original attack, and should only use the amount of force needed to stop an ongoing attack or future attacks.[118] Immediacy requires that the defensive action not be too tardy.[119] This condition is read broadly and responsive action may sometimes be taken days, weeks, or even months after the original attack.[120]

An additional consideration is whether anticipatory self–defense is permitted under the U.N. Charter. Anticipatory self–defense occurs when a nation acts in self–defense before it is the victim of an actual armed attack.[121] Scholars disagree as to whether Article 51 permits anticipatory self–defense.[122] Some scholars believe that Article 51 limits self–defense until after an armed attack occurs.[123] But in analyzing claims of self–defense, governments and scholars have often invoked the *Caroline* Criteria, which were developed by the United States Secretary of Defense Daniel Webster in 1837.[124] Under this framework, anticipatory self–defense is lawful when there is a necessity of self–defense that is instant, overwhelming, leaves no choice of means, and no moment for deliberation.[125] In addition, the response cannot be unreasonable or excessive.[126] The *Caroline* Criteria have been viewed as customary international law in applying anticipatory self–defense under Article 51 of the U.N. Charter.[127] State practice, however, following the adoption of the U.N. Charter does not provide a clear conclusion as to whether acting in anticipatory self–

117. Dinstein, *supra* note 116.

118. *Id.*; David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 89 (2010).

119. Dinstein, *supra* note 116, at 110.

120. *Id.*

121. JEFFREY L. DUNOFF ET AL., INTERNATIONAL LAW NORMS, ACTORS, PROCESS: A PROBLEM ORIENTED APPROACH, 862 (3rd ed. 2010).

122. Kesan & Hayes, *supra* note 13, at 528.

123. *Id.*

124. JEFFREY DUNOFF ET AL., *supra* note 121, at 851, 863.

125. *Id.* at 851.

126. *Id.*

127. ADVISORY COUNCIL ON INTERNATIONAL AFFAIRS (AIV) & ADVISORY COMMITTEE ON ISSUES OF PUBLIC INTERNATIONAL LAW (CAVV), PRE–EMPTIVE ACTION 16 (July 2004) (Neth.).

defense is permitted.[128]

B. CYBER–CRIME

What is a cyber–crime? Law enforcement experts, commentators, and scholars disagree.[129] Some view cyber–crimes as ordinary crimes that are simply committed using a high tech computer.[130] They assert that these crimes should therefore be prosecuted under the traditional laws, such as trespass, larceny, and conspiracy.[131] Others view cyber–crimes as a new category of crime with unique challenges not present by traditional crimes, such as issues regarding jurisdiction, international cooperation, intent, and offender identification.[132] Different states have their own criminal codes which define what cyber–activities constitute crimes. The United States has codified a wide range of cyber–operations which constitute crimes, including substantive cyber–crime laws[133] and procedural cyber–crime laws.[134] In contrast to the United

128. *Id.* at 18–20. *See generally Id.* at 17–18 (detailing specific situations of state action and anticipatory self–defense after the adoption of the U.N. Charter).

129. Eric J. Sinrod & William P. Reilly, *Cyber–Crimes: A Practical Approach to the Application of Federal Computer Crime Law*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 180 (2000).

130. *Id.*

131. *Id.*

132. *Id.* At this point in time Congress has approached computer crime as both traditional and new. Congress has amended the Securities Act of 1933 to include crimes committed by a computer, but they have also enacted a new computer fraud and abuse section that can be amended as technology and computer crimes evolve. *Id.*

133. Computer Crime and Intellectual Property Section, *U.S. Dep't J., Cybercrime Laws of the United States (compiled by Al Rees, CCIPS)*, OAS, 1 (Oct. 2006), http://www.oas.org/juridico/spanish/us_cyb_laws.pdf. Substantive cyber–crime laws are laws which prohibit online identity theft, hacking, intrusion into computer systems, child pornography, intellectual property, and online gambling. *Id.* One example is the United States Computer Fraud and Abuse Act "which has been used civilly and criminally, in situations where an employer asserts that one has abused a workplace computer to violate the employer's competitively–sensitive, confidential and proprietary information, stored on or accessible through computers." The Act also prohibits hacking into computers to obtain information that has been determined to require protection from unauthorized disclosures for reasons of national defense or foreign relations, or any data restricted by Section 11 of Atomic Energy Act of 1954, and unauthorized access to computers of a federal department or agency. Leslie J. Hagin, *Workplace Cyber Crimes*, 6TH ANNUAL LABOR AND EMPLOYMENT LAW CONFERENCE 1, 5 (Nov. 2, 2012); 18 U.S.C. § 1030 (West).

134. Computer Crime and Intellectual Property Section, *U.S. Dep't J., Cybercrime Laws of the United States (compiled by Al Rees, CCIPS)*, OAS, 1

States' large number of cyber–crime laws, there are many nations which have either ineffective cyber–crime laws or have not amended their laws to include cyber–crimes at all.[135]

"As a result of rapid adoption of the Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few."[136] One identification issue is the distinction between hackers and crackers, which creates considerable problems for categorization. Hackers are people who access computer systems in order to gain knowledge about how the system itself works.[137] They like to tinker with computer systems simply for the enjoyment of doing so and do not intend to do damage to them.[138] Crackers hack the computer system and then attempt to do damage; they steal information and cause disruption for either personal, political, or strategic reasons.[139]

The cyber–crime model is currently based in domestic law, but the application of jurisdiction creates several problems when applied to cyber–crimes.[140] One of the most common

(October 2006), http://www.oas.org/juridico/spanish/us_cyb_laws.pdf. Procedural cyber–crime laws involve the authority to preserve and obtain electronic data from third parties, authority to intercept electronic communications and search and seize electronic evidence. *Id.* For additional information on cybercrime laws in the United States and internationally, see SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE (2010); JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME (2010).

135. *See* Nancy E. Marion, *The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation*, 4 INT'L J. CYBER CRIMINOLOGY 699, 700 (2010); *Cyber Crime . . . and Punishment?* Archaic Laws Threaten Global Information, MCCONNELL INTERNATIONAL, 3–4 (Dec. 2000), http://www.witsa.org/papers/McConnell–cybercrime.pdf. For additional information on international cybercrime laws and the views and practices in various jurisdictions, see CYBERCRIME AND JURISDICTION (Bert–Jaap Koops & Susan W. Brenner et al. eds., 2006). For information on each nation's current cyber–laws, see J. Stein Scholberg, *Cybercrime Law*, CYBERCRIMELAW (Feb. 22, 2013, 12:56 AM), http://www.cybercrimelaw.net/Cybercrimelaws.html.

136. Sinrod & Reilly, *supra* note 129, at 178–79.

137. *Id.*

138. Chad Perrin, *Hacker v. Cracker*, TECHREPUBLIC IT SECURITY BLOG (Apr. 17, 2009, 1:20 PM), http://www.techrepublic.com/blog/security/hacker–vs–cracker/1400. Damage does sometimes occur but it is their lack of intent to do damage that helps to distinguish them from crackers. *Id.*; *see* 18 U.S.C. § 1030 (West Supp. 1999).

139. Perrin, *supra* note 138. Some crackers also try to do good things after penetrating computer systems, such as providing penetration testing services, but most have a malicious intent. *Id.*

140. *Cf.* THE LAW AND ECONOMICS OF CYBERSECURITY (Mark F. Grady &

jurisdictional claims for traditional crimes is the location of the crime, but identifying the location of a cyber–crime raises numerous questions.[141] Is the source of the electronic communication the location?[142] Where it was originally received?[143] What if criminal conduct in furtherance of the offense occurred in the jurisdiction?[144] Or did the offender simply access a computer in that state?[145] It can also be very difficult to tell where the criminal act actually takes place. Material may be uploaded in one state or several states, while the hosting provided may be in another state, or publication may occur in every place where the material can be received and viewed.[146] In addition, jurisdictional claims may be based on the location of the computers, persons, effects, or the nationality of the perpetrator or the victims.[147] Each state may have its own jurisdictional framework for the prosecution of cyber–crimes.[148]

While cyber–crimes are currently being prosecuted within domestic law, there have been proposals for the establishment of an International Criminal Tribunal for Cyberspace (ICTC).[149] The jurisdiction of the ICTC would be limited to the

Francesco Parisi eds., 2007) (arguing that the issues related to cyber–security are primarily the result of computer owners purchasing less than optimal security levels and that the "problem is compounded because the insecure networks extend far beyond the regulatory jurisdiction of any one nation or even coalition of nations.").

141. Susan W. Brenner & Bert–Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH TECH. L.1, 10 (2004).

142. *See id.* at 10–16.

143. *See id.*

144. *See id.*

145. *See id.*

146. *Id.* at 15.

147. *See id.* at 10–21. For a restricted number of crimes countries may also claim universal jurisdiction. This claim of jurisdiction is for particularly heinous crimes condemned by the international community. This is a claim of jurisdiction regardless of the location of the act, the nationality of the perpetrator or victim, or any protected interest of the country. Germany and Belgium do currently claim universal jurisdiction for one particular cyber–crime: child pornography. The United States currently does not recognize universal jurisdiction for any cyber–crimes and only asserts this claim for a few crimes including piracy, hostage–taking, aircraft hijacking, aircraft sabotage, and torture. Brenner & Koops, *supra* note 141, at 28.

148. *See* Brenner & Koops, *supra* note 141, at 3–26.

149. J. Stein Schjolberg, *Recommendation for Potential New Global Legal Mechanisms Against Global Cyberattacks and Other Global Cybercrimes: An International Criminal Tribunal for Cyberspace (ICTC)* CYBERCRIMELAW (Feb. 22, 2013, 1:45 AM), http://www.cybercrimelaw.net/documents/ICTC.pdf.

cyber–crimes of most serious concern to the international community, including violations of a global treaty or set of treaties on cyber–crime, or coordinated global cyber–attacks against critical national infrastructure.[150]

It has also been suggested that the International Criminal Court (ICC) may have jurisdiction over certain cyber–crimes. At the Kampala Conference in 2010, the states that are parties to the ICC treaty agreed upon the definition of the crime of aggression: "[T]he planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a state, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations."[151] Under this definition, in order to effectively prosecute a cyber–attack under the crime of aggression, the prosecution must establish that there was a state action, which rose to the level of use of armed force, and the prosecution must establish jurisdiction over the crime.[152] While the definition of aggression did not explicitly include cyber–attacks and seems to be limited to traditional armed attacks by state actors, it could be argued that certain cyber–attacks could be considered crimes of aggression.[153] While ICC jurisdiction over cyber–crimes appears to be a possibility it is a few years off, the earliest that the ICC could have jurisdiction over crimes of aggression is January 1, 2017.[154]

Schjolberg has proposed several different locations for where the court may be located: 1. Additional provisions or articles may be included in the list under the International Criminal Court (ICC) in The Hague. 2. Establish a special International Criminal Court for Cyberspace (ICTC) as a subdivision of the ICC in The Hague. 3. Create the ICTC through a United Nations Security Council decision. 4. Base the ICTC in Singapore in conjunction with the establishment of the Interpol Global Complex (IGC). *Id.* at 15–16.

150. *Id.* at 18.

151. Int'l Criminal Court [ICC], Assembly of State Parties, Review Conference, the Crime of Aggression, ICC Doc. RC/Res. 6 (June 11, 2010).

152. Chance Cammack, *The Stuxnet Worm and Potential Prosecution By the International Criminal Court Under the Newly Defined Crime of Aggression*, 20 TUL. J. INT'L COMP. L. 303, 319 (2011).

153. *Id.* at 320. Cammack argues that under certain situations and a broad interpretation the Stuxnet worm and others could be considered a crime of aggression. *Id.*

154. Int'l Criminal Court, *supra* note 151; "2. The Court may exercise jurisdiction only with respect to crimes of aggression committed one year after the ratification or acceptance by thirty States Parties. 3. The Court may exercise jurisdiction over the crime of aggression in accordance with this article, subjection to a decision taken after 1 January 2017 by the same majority of States Parties as is required for the adoption of an amendment to

Under the current model what constitutes a cyber–crime is defined by each state individually. The current international model for prosecuting cyber–criminals is the same as prosecuting traditional criminals. If a person violates the law of a state, they may be prosecuted within that state. If the perpetrator committed the crime in one state but is located in another state, the victimized nation may ask to have the perpetrator extradited. "'Extradition' is the formal surrender of a person by a State to another State for prosecution or punishment."[155] Extradition is regulated by treaties between nations. Although the United States has treaties with over 100 countries, there remain many countries with which it does not have an extradition treaty.[156] When an individual has committed a crime in one country but is located in another country, the nation wishing to prosecute the offender may submit a request through diplomatic channels to have the offender released to the victim nation for prosecution.[157] Extradition also requires dual criminality, which requires that a person may be extradited only when their actions are criminal in both the state requesting their extradition and the requested state.[158] The varieties of cyber–crime activity, along with some countries' lack of legislation prohibiting cyber–crimes, make it difficult for many cyber–crimes to meet the dual criminality requirement.[159]

C. CYBER–ESPIONAGE

"Cyber–espionage is defined as the intentional use of

the Statute." *Id.* at art. 15, ¶¶ 2–3. *Delivering on the Promise of a Fair, Effective, and Independent Court: The Crime of Aggression*, ICCNOW, http://www.iccnow.org/?mod=aggression (last visited June 15, 2012).

155. MICHAEL JOHN GARCIA & CHARLES DOYLE, CONG. RESEARCH SERV., 7–5700, EXTRADITION TO AND FROM THE UNITED STATES: OVERVIEW OF THE LAW AND RECENT TREATIES 1 (2010).

156. *Id.* at summary.

157. *Id.*

158. Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 10 INT'L J.L. & INFO TECH. 139, 141 (2002).

159. *Id.* at 223. The Love Bug virus is a good example of how the dual criminality requirement can be a roadblock to effective prosecution of cyber–crimes. The Love Bug destroyed files and stole passwords affecting forty–five million users in more than twenty countries, causing somewhere between $2 billion and $10 billion in damage. Onel de Gusman created and disseminated the Love Bug and lived in the Philippines. Since Philippine law did not criminalize hacking and the distribution of viruses, Guzman could not be prosecuted in the Philippines or be extradited for prosecution in other countries which have cyber–crime laws. *Id.* at 139–40.

computers or digital communications activities in an effort to gain access to sensitive information about an adversary or competitor for the purpose of gaining an advantage or selling the sensitive information for monetary reward."[160] Espionage does not reach the level of use of force under the U.N. Charter.[161] Espionage is used by nations at the risk that if their spies are apprehended in a foreign jurisdiction they may be prosecuted criminally. In order for spies to be prosecuted they must be apprehended in the foreign jurisdiction, since a state is not likely to extradite their own spies to be prosecuted abroad. "The law of espionage is, therefore, unique in that it consists of a norm (territorial integrity), the violation of which may be punished by offended states, but states have persistently violated the norm . . . ."[162]

Just as traditional spies may be prosecuted if apprehended in a foreign territory, computer experts who conduct cyber–espionage may also be prosecuted if apprehended in a foreign jurisdiction. However, the opportunity for cyber–spies to be arrested is reduced compared to traditional spying because cyber–espionage can usually be conducted from within the home country. This reduced opportunity for prosecution does not alter the reality that cyber–espionage is merely another form of espionage. Therefore, the current domestic and international laws for traditional espionage can and should be applied to cyber–espionage.

Some argue that cyber–espionage needs to be treated more severely than traditional espionage, because cyber–espionage is more intrusive than traditional espionage, due to the capacity to repeatedly take huge amounts of data, and because non–state actors have the ability to effectuate an attack.[163] Scholars

160. Kevin G. Coleman, *Cyber Espionage Targets Sensitive Data*, SIP TRUNKING (Dec. 29, 2008), http://sip–trunking.tmcnet.com/topics/security/articles/47927–cyber–espionage–targets–sensitive–data.htm.

161. Anna Wortham, *Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?*, 64 FED. COMM. L.J. 643, 655 (2012).

162. Commander Roger D. Scott, Note, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 218 (1999).

163. *See* Wartham, *supra* note 161, at 658; *see also* Shackelford & Andres, *supra* note 60, at 979 ("Stephen Chabinsky, a senior FBI official responsible for cyber security. . . 'A spy might once have been able to take out a few books' worth of material, now they take the whole library. And if you restock the shelves, they will steal it again.'"). Melinzsky asserts that the severity of cyber–espionage along with the scale of the theft and lack of risk warrants

who support this proposition propose that cyber–espionage should, in some situations, be treated as a use of force or threat of use of force under the U.N. Charter.[164] In contrast, others propose that due to the new and unique nature of cyber–espionage, a new set of laws need to be developed.[165] However, it is the minority opinion that calls for treating cyber–espionage differently from traditional espionage. The majority of scholars and nations approach cyber–espionage in the same way as traditional espionage.

The test to determine what constitutes cyber–espionage is simple. If the CNO is only collecting information, then it is cyber–espionage. If the CNO is doing more than merely collecting information, then it is considered to be more than espionage and may rise to the level of use of force or an armed attack. While the test is simple, it is often difficult to determine from the computer code alone whether a CNO's objective is merely the collection of information, or something more malicious, since both can use similar technology.[166]

V. APPLICATION OF LEGAL PARADIGMS TO SITUATIONS

A. ESTONIA

The CNOs against Estonia in 2007 present a unique opportunity to analyze whether the disabling of their government websites could be considered a use of force under the U.N. Charter, an armed attack, or a crime.

Michael Schmitt determined that although the attacks against Estonia caused no deaths or physical injury, the CNOs

military action. "The severity of the problem of data theft is too great and its effects too harmful." "The scale of thefts is unprecedented: 'Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies.'" In order to steal that much information a spy would have needed a forklift and a van and would have a high level of risk including the risk of getting caught or killed. Alexander Melnitzky, Note, *Defending America Against Cyber Espionage Through the Use of Active Defenses*, 20 CARDOZO J. INT'L AND COMP. L. 537, 566 (2012).

164. Alexander Melnitzky, *supra* note 163, at 564–65 (arguing that cyber–espionage may amount to an armed attack under an effects–based approach because it is the potential for an armed attack that makes the activity an armed attack and cyber–espionage has that potential).

165. Wartham, *supra* note 161, at 657. ("The capabilities of cyber technology simply differ too much from those of traditional espionage, and the ease with which the technologies for cyber–exploitation and cyber–attack can be used together demands a new set of laws.").

166. Kesan & Hayes, *supra* note 13, at 426.

affected the overall operation of Estonian society and was, therefore, a use of force.[167] Under the seven–factor test Schmitt determined that the effects of the attack were immediate and also long–lasting.[168] The effects were direct since the DoS attacks promptly resulted in an inability to access funds, government websites, and news sources.[169] The attacks were also invasive since they targeted websites and computer systems that were protected and secured.[170] Schmitt determined that if Russia had been responsible for the CNO, then it would be considered a cyber–attack and in violation of Article 2(4) of the UN Charter.[171] Under the result–oriented approach it is most likely that the CNO would be considered a violation of Article 2(4) because the CNO spread panic and confusion, disrupted the economy, and disrupted key government functions.[172] The results of this attack were therefore severe and arguably in violation of Article 2(4).

Under the consequence–based or equivalent–effects test, the CNOs against Estonia would not rise to the level of an armed attack. The CNOs affected government and other key websites which were vital to the everyday functioning of Estonia. However, there were no deaths or physical destruction as a result of the CNOs. The CNOs could not be considered similar to an attack by traditional military forces.

Even when assuming the attacks against Estonia rose to the level of a use of force, the CNOs against Estonia can only be considered under the laws of war if a state is responsible for the CNOs.[173] Following the CNOs against Estonia, Estonian officials immediately blamed Russia and charged them with violating the U.N. Charter.[174] Other commentators claimed that Russia had made large botnets available for use by groups of individuals so that they could more effectively launch CNOs

167. Michael N. Schmitt, *supra* note 71, at 577.
168. *Id.*
169. *Id.*
170. *Id.*
171. *Id.*
172. *Id.*
173. *See* U.N. Charter art. 2, ¶ 4; U.N. Charter art. 51.
174. WILSON, *supra* note 14, at 8; *see* Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (May 16, 2007), http://www.guardian.co.uk/world/2007/may/17/topstories3.russia; John Leyden, *Cyberwarriors on the Eastern Front: In the Line of ~~Fire~~ Packet Floods*, THE REGISTER (Apr. 25, 2011), http://www.theregister.co.uk/2011/04/25/estonia_cyberwar_interview/.

against the Estonian computer network.[175] Computer network analysts have found that the CNOs were conducted by individual attackers from around the world who communicated mostly through Russian chat rooms.[176]

Article VIII of the International Law Commission's *Draft Articles on the Responsibility of States for International Wrongful Acts* implicates that there is state control for actions when state actors or official organs are "acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[177] The definition of the word "control" has been left for the courts to decide. The International Court of Justice established the effective control test in *Nicaragua v. United States of America*.[178] The court determined that a state has control over non–state actors only when the actors act in "complete dependence" on the state.[179] In contrast, the International Criminal Tribunal for the Former Yugoslavia (ICTY) established the overall control test in *Prosecutor v. Tadic*.[180] The court determined that a state has control, or that actions by non–state actors are attributable to the state, when the state has a role in organizing, coordinating, and providing support for the group.[181]

Under the effective control test, the actions of the non–state actors responsible for the CNOs could not be considered under the effective control of Russia because, from the information that has been uncovered, Russia was not directing the CNOs.[182] The CNOs were being sent from one to two million compromised computers in 100 jurisdictions around the

175. Leyden, *supra* note 174.

176. *Id.*

177. Int'l Law Comm'n, 2 *Draft Articles on Responsibility of States for Internationally Wrongful Acts,* Part 2, art. 8, U.N. Doc. A/56/10, Chapter IV.E.1 (Nov. 2001).

178. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 110 (June 27); Advisory Council on International Affairs & Advisory Committee on Issues of Public International Law, *supra* note 70.

179. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 110 (June 27); Advisory Council on International Affairs & Advisory Committee on Issues of Public International Law, *supra* note 70.

180. Prosecutor v. Tadic, Case No. IT–94–1–I, Decision on Defense Motion for Interlocutory Appeal on Jurisdiction (Int'l Crim. Tib. for the Former Yugoslavia Oct. 2, 1995).

181. *Id.*

182. *See* WILSON, *supra* note 14, at 8.

world. [183] There is no indication that Russian officials were directing their operations or that the actors were "completely dependent" upon Russia.[184] It is unknown whether Russia made their botnets available to assist the perpetrators,[185] but if this could be proven Russia may be responsible for the perpetrators' actions because it knowingly provided support to the attackers. Under the overall–control test Russia would be supporting the efforts of non–state actors and their actions are attributable to the state. This would be considered use of force, and thus could be considered an armed attack under the target–based approach. The uncertainty regarding the role that Russia had in the CNO against Estonia makes it difficult to attribute responsibility to Russia for the cyber–attacks.

The most common challenges under international law are the issues of responsibility and attribution. Who is responsible for the CNOs? Were the CNOs conducted by a state? Were the CNOs conducted by individuals acting alone? Can individual or group actions be attributed to the state? Identifying who is responsible for a CNO creates serious difficulties for distinguishing a CNO as use of force, armed attack, cybercrime, or cyber espionage. The Internet creates nearly endless opportunities to hide the identity of an attacker. To identify the source of a CNO requires associating the Internet Protocol (IP) address with an individual, group, or state.[186] Attackers can create stepping stones between the attacking computer and the system used to perpetuate the attack.[187] Attackers can also create faulty IP addresses which make it look like another party is responsible for the attacks.[188] If the attackers know how to effectively utilize the Internet, it is nearly impossible to uncover who is responsible for the attack.

Since Estonia was unable to attribute responsibility to Russia for the cyber–attacks only individuals and groups who perpetrated the attacks could be held responsible under criminal law. It has been difficult to determine who was responsible for the attacks. At this point, only one individual

183. Leyden, *supra* note 174.

184. *See A Cyber–Riot: Estonia Has Faced Down Russian Rioters. But Its Websites are Still Under Attack*, ECONOMIST (May 10, 2007), http://www.economist.com/node/9163598?story_id=9163598.

185. *See* WILSON, *supra* note 14, at 8.

186. Duncan D. Hollis, *An e–SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 398 (2011).

187. *Id.* at 398–99.

188. *Id.*

has been prosecuted for the attacks.[189] Dmitri Galushkevich, a twenty year old ethnic–Russian Estonian, admitted his guilt, and was fined the equivalent of $1,200 for attacks against the Estonian Prime Minister and leader of the Reform Party, Andrus Ansip.[190] Galushkevich identified possible targets in online chat rooms.[191] At this time, no additional individuals, groups, or states have been charged with executing the attacks.[192]

The cyber–attacks against Estonia reflect challenges regarding categorization of the CNOs as either a use of force, armed attack, or cyber–crime. Cyber–attacks do not always fit neatly into one of these categories. How a cyber–attack is classified often depends on the test applied. Another issue that cyber–attacks raise is determining who is responsible for the attack. The answer to this question may decide which law is controlling. For instance, Article 2(4) and Article 51 of the U.N. Charter are only applicable to cyber–attacks if the attacks can be attributed to the state.[193] Assigning responsibility, although difficult, is necessary to determine whether the U.N. Charter provisions on use of force and armed attack apply or whether criminal law applies.

B. STUXNET

Stuxnet, at minimum, is considered to be a use of force. Under some tests, Stuxnet could also be considered an armed attack as defined by the U.N. Charter. Officials of President Barack Obama's administration admitted that the Stuxnet computer worm was a joint project between the United States and Israel.[194] This admission by the United States makes further discussion on state responsibility unnecessary.[195]

The Stuxnet attack would constitute a use of force under the U.N. Charter. Under the seven factor Schmitt analysis, the Stuxnet attack was severe because it caused physical harm to property. Stuxnet caused the centrifuges to speed up and slow down their rotation causing them to break.[196] The breaking of

189. Leyden, *supra* note 174.
190. *Id.*
191. *Id.*
192. *Id.*
193. *See* Wortham, *supra* note 161, at 648–49.
194. Sanger, *supra* note 22.
195. *See id.*
196. *Id.*

the centrifuges constitutes a physical destruction of property that rises above the level of a "minor inconvenience or irritation."[197] United States officials contend that it set back the Iranian nuclear program anywhere from eighteen months to two years.[198] The consequences were immediate; Stuxnet could change the speeds of the centrifuges at the discretion of the operators causing them to break.[199] As such, the breaking of the centrifuges was the direct result of the Stuxnet worm. The attack is considered invasive because the Natanz facility was supposed to be a secure, secret facility.[200] Furthermore, because the United States has claimed responsibility for the cyber–attack, Stuxnet certainly constitutes a use of force under Schmitt's analysis.

In contrast, under the result–oriented approach it is difficult to say for certain whether the attack reached the required level of severity to constitute use of force. While Stuxnet only caused centrifuges to break and did not cause physical harm to anyone, an argument can be made that the consequences of Stuxnet were severe because the Iranian program was set back several years. Jeremy Richmond argues that Stuxnet did more harm than just the broken centrifuges.[201] Stuxnet caused shortages of certain types of metals and had psychological effects because it infiltrated a facility believed to be secure and immune to malware.[202] Additionally, it is likely that Iran had to replace all of its computer systems at Natanz, a difficult task for a country under severe trade restrictions.[203] Whether or not these consequences are severe enough to give rise to a use of force classification is debatable. That being said, it is likely that the Stuxnet attack would be classified as a use of force.

Another approach to use of force is the consequence–based approach.[204] Under this approach, the cyber–attack must be analogous to the effects of a classic military operation.[205] In this instance Stuxnet successfully destroyed the centrifuges

197. *See* Schmitt, *supra* note 71, at 576.
198. Sanger, *supra* note 22.
199. *See id.*
200. *See* Richmond, *supra* note 32, at 859.
201. *Id.*
202. *Id.*
203. *Id.*
204. *See* Schmitt, *supra* note 71, at 587–89.
205. *See id.*

eliminating the need to use a classic military operation to slow the progress of Iran's nuclear program.[206] Stuxnet, therefore, performed a task that would have otherwise required a classic military operation. Some scholars may argue that the Stuxnet attack did not have the required severity or destructive effects typically associated with a classic armed attack and, therefore, cannot be considered the equivalent of an armed attack. At the same time, however, Stuxnet executed an objective that would traditionally have required a classic military operation, therefore, the Stuxnet attack should be considered an armed attack under the consequence–based approach.

Under the U.N. Charter the Stuxnet cyber–attack would qualify as a use of force and would likely also qualify as an armed attack under Article 51. Since Stuxnet most likely constituted an armed attack whether Iran could lawfully respond with military action in self–defense must be analyzed within the three requirements of necessity, proportionality, and immediacy.[207] It is unlikely an Iranian response would meet the requirements of necessity, proportionality, and immediacy, therefore, an armed response to Stuxnet would not be lawful.

First of all, a response by Iran would not fulfill the condition of necessity. The necessity requirement is not met because there are remedies that Iran could use in response to Stuxnet that do not require force. For example, Iran could take action to eradicate Stuxnet from the computer system. If Stuxnet is no longer present in the Natanz computer system, then it is no longer a threat to Iran. Iran could also lodge a complaint with international authorities such as the U.N. Security Council. Iran took such legal action on June 20, 2012, when Iran's Communications and Information Technology Minister, Reza Taqipour, announced that the Iranian Foreign Ministry complained to relevant international organizations.[208] Iran and the United States could also work diplomatically to try and reach an agreement prohibiting the use of CNO

206. *See* Sanger, *supra* note 22.

207. *See, e.g.*, Schmitt, *supra* note 71, at 593–94.

208. *See, e.g.*, *Iran Complains to World Bodies About Cyber Attacks:* Minister, PRESSTV, Jun. 20, 2012, http://www.presstv.ir/detail/2012/06/20/247120/iran–protests–state–cyberterrorism/. Iran has yet to disclose precisely which international organizations have been made aware of its complaint. *See id.*; *see also Iran Complains of Cyberterrorism*, UNITED PRESS INT'L, June 20, 2012, http://www.upi.com/Science_News/Technology/2012/06/20/Iran–complains–of–cyberterrorism/UPI–33471340206675/.

operations.

A response by Iran would also have to be proportionate to the Stuxnet attack to be lawful. What a proportionate response would look like is currently being debated by scholars; some argue that a victimized nation can only respond with an in–kind cyber–attack while other scholars argue that under some situations a response using traditional military force would satisfy the proportionality requirement.[209]

In addition, any response by Iran would most likely be tardy and not meet the immediacy requirement. President Barack Obama's administration did not take responsibility for Stuxnet until June of 2012, but it was discovered in June 2010, any response by Iran would have therefore been two years after the discovery of Stuxnet.[210] Iran also claims to have eradicated Stuxnet with little overall impact on the Iranian nuclear program; as such, any action by Iran at this time would be taken well after Iran eradicated any remaining Stuxnet threat. Furthermore, Stuxnet was scheduled to self–destruct on June 24, 2012, so any action taken in response to Stuxnet would be unnecessary because it is past the date that Stuxnet self–destructed. Given the above analysis, an armed response by Iran to the Stuxnet attack would not meet the three requirements of necessity, proportionality, and immediacy and would not be lawful under international law.

Stuxnet raises several important issues with regard to cyber–attacks and use of force, armed attack, and self–defense under the U.N. Charter. The United States took responsibility for the Stuxnet attack thereby making Article 2(4) and Article 51 of the U.N. Charter applicable. Stuxnet would constitute a use of force triggering Iran's right to respond with non–forceful actions and countermeasures. If Stuxnet also rose to the level of an armed attack, then Iran may respond in self–defense. Iran would not, however, be able to respond with an *armed* attack in self–defense because an *armed* attack would not meet the requirements of necessity, proportionality, and immediacy. The question remains, under what circumstances would an armed attack in self–defense to a cyber–attack be appropriate? A nation has yet to respond to a cyber–attack in self–defense,

209. *See* Kesan, *supra* note 13, at 512–14. Some scholars argue that responding to a cyber–attack in kind, instead of by traditional military forces, is more in line with the principles of international humanitarian law such as distinction, humanity, necessity, and proportionality. *Id.*

210. Sanger, *supra* note 22.

and scholars continue to debate what type of defensive action would be permissible under the principle of proportionality.[211]

C. FLAME

Computer experts who have analyzed the Flame virus have determined that its primary objective is the collection of information.[212] Computer analysts at Kaspersky Lab have asserted that Flame is so large and complex it must have been created by a government.[213] Because Flame was deployed by a government and because it collects information, it is considered cyber–espionage. If the cyber–spies responsible for the attacks were ever apprehended they could be prosecuted for espionage in any of the states where Flame collected information. The possibility that they will ever be tried for espionage is infinitesimal. In order to prosecute the victimized nation would have to identify the cyber–spies and apprehend them within their country because the state responsible is not going to extradite their own operatives. Flame is conducting cyber–espionage but could such an action also be regarded as a use of force?

Identifying the intent behind a CNO may be difficult because a CNO is merely computer code and deciphering the intent behind computer code alone can be difficult.[214] When a state is not able to decipher a CNO's intent it may lead officials to assume that they are under attack. The fear of indiscernible intent and capabilities of a CNO may lead a trigger happy nation to respond with force to a CNO that is engaged only in espionage.[215] The fear that states may respond aggressively to a cyber–espionage operation leads some scholars to assert that persistent and aggressive acts of cyber–espionage should be treated as a threat of force or use of force under the U.N.

211. *See* Kesan, *supra* note 13, at 512.

212. *Kaspersky Lab*, *supra* note 34.

213. *See "Flame" Computer Virus Strikes Middle East; Israel Speculation Continues*, CBS NEWS (May 29, 2012, 2:26 PM), http://www.cbsnews.com/8301–501465_162–57443071–501465/flame–computer–virus–strikes–middle–east–israel–speculation–continues/. "Western officials with knowledge of the effort" told reporters that the United States and Israel developed Flame to collect intelligence in preparation for cyber–attacks aimed at slowing Iran's nuclear program. Nakashima, *supra* note 45.

214. *See* Wortham, *supra* note 161, at 656.

215. *See* Herbert S. Lin, *Offensive Cyberspace Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 82–83 (2010).

Charter.[216]

On one hand, a CNO may *only* have the ability to collect information.[217] There are other CNOs however, that collect information and have the capacity to launch a cyber–attack at the operator's instructions.[218] Furthermore, even if the CNO is only able to collect information it could potentially be upgraded with the required capabilities to launch a cyber–attack if needed.[219] Scholars note that because CNOs may contain, or be updated with, the ability to launch a cyber–attack, and because the cyber–espionage and attack operations do not have to be mutually exclusive, a targeted country will sometimes not know, and have no way of finding out, whether they have been exploited or attacked.[220]

While the primary objective of Flame appears to be the collection of information, a CNO like Flame may have the capability to be upgraded to contain a destructive component.[221] As is, Flame conducts cyber–espionage because it collects information on computer displays, and stores data, documents and other information.[222] However, through an upgrade in the software, Flame may have the capability to take destructive action such as "destroying the read–only memory controlling the boot sequence of the machine where it resides."[223] As such, it could be argued that Flame does not—in its present state—constitute a use of force because it does not have any potential to do damage; that being said, Flame could easily be turned into a destructive agent.[224] When, if ever, should upgrading a CNO to have destructive capabilities be considered a threat of force, violating Article 2(4) of the U.N. Charter?

It could be argued that a CNO that is conducting cyber–espionage but has the capability to launch a cyber–attack is analogous to initial troop movements or the massing of troops on a border. The CNO is prepared and capable of launching a cyber–attack similar to the way troops amassed on a border are

216. *See id.*at 84.
217. *See id.* at 78–79.
218. *Id.*
219. *Id.*
220. Wortham, *supra* note 161, at 652–53.
221. Lin, *supra* note 215, at 79.
222. Erdbrink, *supra* note 34; *Kaspersky Lab*, *supra* note 34.
223. *See,* Herbert S. Lin, *supra* note 215, at 79.
224. *See id.*

prepared and capable of an attack; the CNO is waiting for a command to attack the same as traditional troops. Some scholars propose that because of the instantaneous ability to upgrade a CNO to have destructive potential, cyber–espionage should be treated as a possible armed attack from the very beginning.[225] Despite the arguments for why cyber–espionage such as Flame should be considered a threat of force or use of force under Article 2(4), most scholars, nations, and analysts assert that when a CNO is only collecting information it is cyber–espionage. Therefore, cyber–espionage, just like traditional espionage, would not be, under traditional principles of international law, considered a threat of force or use of force under Article 2(4) until the CNO takes action beyond collecting data.[226]

An additional consideration when analyzing cyber–espionage is whether a nation that is victim to cyber–espionage may ever act in anticipatory self–defense. It would appear that cyber–espionage, by itself, would never trigger anticipatory self–defense because cyber–espionage is not instantaneous—there is no immediate threat.[227] Cyber–espionage is not overwhelming because alone, it does no harm. Cyber–espionage leaves ample time for deliberation because it does not create an immediate danger.[228] However, cyber–espionage paired with an exposed vulnerability in the computer software may justify the use of anticipatory self–defense.[229] If a CNO has infected a computer and is conducting cyber–espionage, if the CNO has uncovered a weakness in the operations system that is vulnerable to attack from the CNO, and if intelligence uncovers that the vulnerability will be exposed for an imminent attack, then a nation may be able to respond in anticipatory self–defense.[230] The threat is immediate because intelligence has

225. Melnitzky, *supra* note 163, at 566–68 (arguing that the distinction between corruption of data such as in a cyber–attack and the theft of data in cyber–espionage is an "overly mechanical distinction" that ignores the basic principle of the effects based approach—the effect is what matters).

226. *See* Melnitzky, *supra* note 163, at 564.

227. *Cf.* Wortham, *supra* note 161, at 656–57 (arguing that because the threat of an attack needs to be immediate a nation recognizing a computer network vulnerability while conducting cyber–espionage will not trigger the ability to act in anticipatory self–defense).

228. *Cf. id.* (stating the additional requirements for anticipatory self–defense: (1) an urgent need to act defensively against the attack, and (2) that no workable alternative to self–defense exists).

229. *Id.*

230. *See id.*

uncovered that the attack will be launched imminently. The threat is overwhelming because there may be no time for computer operators to protect the computer from the attack. The immanency of the attack leaves no moment for deliberation.

Under these specifically tailored circumstances, a nation may be able to respond in anticipatory self–defense to cyber–espionage coupled with an exposed vulnerability.[231] It is important to mention that this ability to respond in anticipatory self–defense is undermined if the nation has time to create network defenses which will protect the system from the cyber–attack. Applying the circumstances surrounding the Flame virus, targeted nations would not be able to respond in anticipatory self–defense unless Flame was updated with the capability to conduct a cyber–attack, the computer system had an exposed vulnerability, and government intelligence had uncovered that those responsible were going to expose the vulnerability for an imminent attack. None of these requirements have been met for the Flame operation meaning that the affected nations would not be able to legally respond with anticipatory self–defense under the *Caroline* Criteria.

Schmitt has proposed that anticipatory self–defense may be used if three factors are present: (1) the CNO is part of an overall operation that will culminate in an armed attack; (2) the CNO is an irrevocable step toward an armed attack; (3) the action in self–defense occurs at the last possible moment to counter the attack.[232] This approach poses a very high standard which cyber–espionage operations would not ordinarily reach.[233] A cyber–espionage operation would rarely, if ever, constitute an irrevocable step toward an armed attack; therefore, under Schmitt's approach, a state would not be able to act in anticipatory self–defense to a cyber–espionage operation.

Flame is a CNO which has the primary purpose of conducting cyber–espionage. Under a traditional analysis, Flame does not constitute a threat or use of force or an armed attack under the U.N. Charter. Some scholars have proposed that because of the CNO's unique ability to upgrade from conducting cyber–espionage to cyber–attacks and the inability to determine the intent of a CNO, cyber–espionage should be

231. *See id.*
232. Schmitt, *supra* note 70, at 936.
233. *See* Kesan, *supra* note 13, at 516–17.

considered a threat of use of force or a use of force under Article 2(4). While this proposition is supported by some analysts, most scholars and nations find that cyber–espionage is the same as traditional espionage and should be viewed as a violation of domestic criminal law. Additionally, while cyber–espionage in itself cannot trigger anticipatory self–defense, cyber–espionage coupled with a computer network vulnerability may trigger the ability to use anticipatory self–defense under the *Caroline* Criteria. Applying the Schmitt approach cyber–espionage would rarely, if ever, trigger the ability to use anticipatory self–defense.

VI. CONCLUSION

Correct identification of CNOs as a threat or use of force, armed attack, a crime, or espionage depends on the scale of the attack, attribution, intent, and consequences. The unique nature of CNOs makes it difficult to determine which legal paradigm is applicable and what response is legally appropriate. As the capabilities and application of CNOs continue to expand, the international community will be faced over and over again with the task of determining which legal paradigm should be applied to CNOs.

So what should the international community do to deal with the threat posed by CNOs? The remainder of this article will analyze the three main approaches proposed to regulate CNOs: (1) a non–proliferation treaty, (2) a treaty or code of conduct containing normative rules and legal obligations, and (3) development of state practice in a way that will create customary international norms which the existing international legal regime cannot address.

A. NON–PROLIFERATION TREATY

Michael Rake, chairman of BT Group PLC,[234] and many other scholars have suggested that a cyber–non–proliferation treaty, similar to those for weapons of mass destruction, must be developed.[235] Supporters of a non–proliferation treaty suggest that the ability of cyber–attacks to completely dismantle a state demands the implementation of a non–

234. BT Group PLC is one of the world's leading telecommunications companies. Associated Press, *Web Summit Considers Cyber–Nonproliferation Pact*, WASH. POST, Jun. 1, 2011, http://www.washingtontimes.com/news/2011/jun/1/web–summit–considers–cyber–nonproliferation–pact/.

235. *Id.*

proliferation treaty.[236] There are currently several treaties, export control regimes, and codes of conduct which address the non–proliferation of weapons of mass destruction.[237] These non–proliferation treaties make the distinction "between the nuclear haves and the nuclear have–nots."[238] They require that those nations which have nuclear weapons reduce their arsenal and not impair other nation's peaceful use of nuclear energy while those nations which do not have nuclear–weapons agree not to develop them.[239] Scholars have suggested that a cyber–non–proliferation treaty is not realistic because there is no way of making a distinction between those who have cyber–weapons and those that do not.[240] Furthermore, ensuring that nations do not develop this technology would be impossible because the actual possession of cyber–attack technology can be difficult to detect; such technology can be developed and tested in secret.[241] The implementation of a cyber–non–proliferation treaty, therefore, is not a workable solution for the threat posed by CNOs.

B. CYBER–TREATY OR CODE OF CONDUCT CONTAINING NORMATIVE RULES

There are several different approaches which may be used for developing an international treaty. A treaty may be created which bans cyber–attacks altogether. This treaty would be similar to the Mine Ban Treaty which bans the use, stockpiling, production, and transfer of landmines because of the harm that landmines cause civilians.[242] Similar to landmines a multi–national cyber–treaty banning cyber–attacks would have support because of the potential negative impact such an attack

236. *See id.*

237. Advisory Council, *supra* note 70, at 29. Multilateral treaties concerning weapons of mass destruction include: 1968 Nuclear Non–Proliferation Treaty (NPT), 1972 Biological Weapons Convention (BWC), 1993 Chemical Weapons convention (CWC), and the 1996 Comprehensive Nuclear Test–Ban Treaty (CTBT). The Hague Code of Conduct Against Ballistic Missile Proliferation (HCOC) is also a code of conduct which focuses on weapons of mass destruction. *Id.*

238. *Id.*

239. *Id.*

240. *Id.*

241. *Id.*

242. *See* Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti–Personnel Mines and on Their Destruction art. 1, Sep. 18, 1997, 2056 U.N.T.S. 211.

would have on civilians.[243] Any use of force in self–defense under the U.N. Charter requires that it meet the requirements of military necessity, distinction between civilians and military targets, proportionality, and avoidance of unnecessary suffering.[244] Because cyber–attacks can "escape" from their original target and affect civilians, it could be argued that such attacks do not distinguish between civilians and non–civilians.[245] In addition, they may cause civilians unnecessary suffering because when such viruses "get loose" they may cause unnecessary damage to programs and institutions which are vital to civilian infrastructure. Scholars and nations have therefore proposed the creation of a treaty banning the use of cyber–attacks because of these potentially devastating effects.

A second approach would be to develop a treaty or code of conduct which deliberately addresses what type of conduct would be considered a cyber–attack and what responses would be appropriate under the circumstances. A treaty such as this would complement and clarify existing regulations regarding use of force in the U.N. Charter and customary international law.[246] Russia has advocated for the establishment of a cyber–attack treaty for over ten years.[247] In addition, the International Telecommunications Union Secretary General Hamadoun Toure has been a vocal supporter of a treaty in which countries would agree not to make a cyber–attack against another state.[248]

Scholars contend that a treaty which bans the use of cyber–attacks or limits their use is not realistic because there is currently no way to ensure compliance.[249] CNOs can be developed in secret and tested in secret. In addition, they can

243. *See* Misha Glenny, *A Weapon We Can't Control*, NY TIMES, Jun. 25, 2012, http://www.nytimes.com/2012/06/25/opinion/stuxnet–will–come–back–to–haunt–us.html?_r=0.

244. Melnitzky, *supra* note 163, at 560–61.

245. *Cf.* Glenny, *supra* note 243 ("[O]nce released, virus developers generally lose control of their inventions, which will inevitably seek out and attack the networks of innocent parties.").

246. Handler, *supra* note 56, at 236.

247. *Id.*

248. *UN Chief Calls for Treaty to Prevent Cyber War*, GoogleNews Jan. 30, 2010, http://www.google.com/hostednews/afp/article/ALeqM5h8Uvk–jpSvCWT–bqYSg1Ws4I4yAA.

249. Handler, *supra* note 56, at 237; *cf.* Shackelford, *supra* note 60, at 993 ("Despite the support for this approach, both the details for how such a treaty would function and whether there is sufficient political will to make it a reality remain uncertain.").

be coded and routed in a way which makes state attribution nearly impossible. Nations can therefore not be monitored in any meaningful way to ensure state compliance with the treaty.[250] Any code of conduct containing normative rules would be undermined by the inability to monitor and attribute responsibility.

C. DEVELOPMENT OF STATE PRACTICE

Stephanie Handler proposes that instead of developing a cyber–treaty, "[a] better option is to focus on developing state practice in a rational way that develops patches where the existing legal regime is not optimally suited to cyberspace operations."[251] Handler claims that a focus on state practice that corresponds to current international law will help develop new customary international law norms.[252] Since it is unlikely that states will come together to create a cyber–treaty, customary international law, developed through state practice, will be the primary method for the formation of cyber–space laws.[253] In addition to state practice, the decisions and opinions of international courts regarding CNOs will assist in the development of international law norms. The development of customary international law in the area of cyber–space operations will take time. For now, scholars must take a wait–and–see approach to see how states react to cyberspace operations and their fast–developing technologies.

250. Handler, *supra* note 56, at 237.

251. *Id.* at 238.

252. *Id.*

253. Hannah Lobel, *Cyber War Inc.: The Law of War Implications of the Private Sectors Role in Cyber Conflict*, 47 TEX. INT'L L.J. 617, 638 (2012); *see* Steven G. Bradbury, Keynote Address at the 2011 Harvard *National Security Journal* Symposium: Cybersecurity: Law, Privacy, and Warfare in a Digital World (Mar. 4, 2011), *available at* http://harvardnsj.com/2011/04/the–developing–legal–framework–for–defensive–and–offensive–cyber–operations.