Loyola of Los Angeles Law Review

Volume 48
Number 3 *Developments in the Law: Election Law; Developments in the Law: Law of War*

Article 10

Spring 2015

Silencing the Call to Arms: A Shift Away From Cyber Attacks as Warfare

Ryan Patterson

SILENCING THE CALL TO ARMS: A SHIFT AWAY FROM CYBER ATTACKS AS WARFARE

Ryan Patterson∗

Cyberspace has developed into an indispensable aspect of modern society, but not without risk. Cyber attacks have increased in frequency, with many states declaring cyber operations a priority in what has been called the newest domain of warfare. But what rules govern? The Tallinn Manual on the International Law Applicable to Cyber Warfare *suggests existent laws of war are sufficient to govern cyber activities; however, the* Tallinn Manual *ignores fundamental problems and unique differences between cyber attacks and kinetic attacks. This Article argues that several crucial impediments frustrate placing cyber attacks within the current umbra of warfare, chiefly the problems of attribution, categorizing uses of force under the* jus ad bellum*, and compliance with the armed-conflict principles of distinction and proportionality and the law of neutrality. Consequently, identifying a victim-state's recourse becomes risky and problematic. For the vast majority of cases, this Article proposes departing from the warfare paradigm and suggests states pursue alternative remedial approaches. By domestically prosecuting cybercrimes, seeking reparations for violations of non-intervention, and enhancing national cybersecurity, states can effectively mitigate cyber attacks without the risks and obstacles associated with treating cyber attacks as warfare.*

∗ J.D., May 2015, Loyola Law School, Los Angeles; B.A. English, University of California, Berkeley, May 2008. I sincerely thank Professor David Glazier for his guidance and expertise, and my Developments Editor, Rosemarie Unite, for her excellent editorial support. Most importantly, a special thank you to my wife, Debbie, for her constant love and encouragement.

TABLE OF CONTENTS

I. INTRODUCTION

Imagine that the United States is under attack. Not by aircraft, tanks, or submarines, but by something altogether different. In just hours, government websites are shut down. Access to banking, news, and social media websites is disrupted. Cable television and mobile communications experience blackouts in large swaths. E-commerce grinds to a standstill. To say that such an attack would impart chaos on American society would not be hyperbole, given the country's staggering reliance on the Internet.[1] Nor is this reliance specific to the United States; countries around the world have seen exponential growth in Internet usage.[2] With such widespread Internet reliance, the development of malicious cyber tactics,[3] network exploitation, and critical system vulnerabilities was inevitable.

Over the past several years, many high-profile cyber attacks have caught the world's attention. In 2007, Estonia was the victim of a three-week cyber attack that first shut down government websites, and then spread to websites of newspapers, television stations, schools, and banks, repeatedly rendering them inoperable for hours and days at a time.[4] The effects were noteworthy, since at that time Estonia was considered the most wired country in Europe, with nationwide wi-fi and a near paperless "e-government" that conducted ninety percent of its bank and election services online.[5] Similarly, the country of Georgia suffered attacks in 2008 that triggered

1. As of June 30, 2012, about 245 million Americans use the Internet. *Internet Usage, Facebook Subscribers and Population Statistics for All the Americas World Region Countries June 30, 2012*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats2.htm (last visited Oct. 23, 2013). This figure represents a population penetration of seventy-eight and one-tenth percent. *Id.*

2. Of the roughly seven billion people on the planet, 2.4 billion use the Internet. *World Internet Usage and Population Statistics*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm (last visited, Oct. 23, 2013).

3. *See* David Sanger & Eric Schmitt, *Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure*, N.Y. TIMES, July 26, 2012, http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html (reporting that "[t]he top American military official responsible for defending the United States against cyberattacks said . . . there had been a 17-fold increase in computer attacks on American infrastructure between 2009 and 2011, initiated by criminal gangs, hackers and other nations.").

4. Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS AND CLARK L. REV. 1023, 1024–25 (2007); Steven Lee Myers, *Cyberattack on Estonia Stirs Fear of 'Virtual War'*, N.Y. TIMES, May 18, 2007, http://www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html?_r=0.

5. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 193–94 (2009).

widespread Internet outages and forced many government websites to blazon Russian nationalistic propaganda.[6] In 2010, the Stuxnet virus, collaboratively generated and executed by Israel and the United States, temporarily shut down one-fifth of the centrifuges used to purify uranium at Iran's Natanz nuclear facility.[7] And finally, in 2013, a group of pro-Syrian government hackers known as the Syrian Electronic Army defaced a United States Marines Corps recruitment website with a letter urging marines to "concentrate on the real reason every soldier joins their military, to defend their homeland," in response to the United States' involvement in the Syrian conflict.[8]

Such high-profile attacks have led many nations around the world to realize the need for expanded cybersecurity and to develop the capability to conduct offensive cyber operations of their own, in what many believe has become the next frontier in modern warfare.[9] President Obama declared cyber threats to be one of the most serious threats to national security, public safety, and economic stability,[10] spurring the 2009 commission of the United States Cyber Command

6. Marco Roscini, *World Wide Warfare*—Jus Ad Bellum *and the Use of Cyber Force*, 14 MAX PLANCK Y.B. U.N. L. 85, 90 (2010); John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

7. *See generally* David E. Sanger, *Obama Order Sped Up Wave Of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-againstiran.html?pagewanted=all&_r=1&&gwh=355753CAC7448E51CB1B05A46ECE9BBC; Jonathan Fildes, *Stuxnet Virus Targets and Spread Revealed*, BBC NEWS TECH. (Feb. 15, 2011, 1:51 PM), http://www.bbc.co.uk/news/technology-12465688 (describing the Stuxnet attack).

8. John Bacon, *Pro-Syrian Group Hacks U.S. Marines Website*, USA TODAY, Sept. 2, 2013, http://www.usatoday.com/story/news/nation/2013/09/02/marines-hackers-syrian-electronic-army/2755265/. Along with the propaganda effort, the Syrian Electronic Army assailed the New York Times and the Washington Post with a rash of distributed denial-of-service (DDoS) attacks. *Id.*

9. *See* NILS MELZER, CYBERWARFARE AND INTERNATIONAL LAW 2011, at 3 (2011), *available at* http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf (stating "military reliance on computer systems and networks . . . open[ed] a 'fifth' domain of war—fighting next to the traditionally recognized domains of land, sea, air and outer space"); Roscini, *supra* note 6, at 97–98 (noting many nations now commission "uniformed hackers" in their military, including China, Israel, Germany, the United Kingdom, and the United States); Leslie Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 LOYOLA L.A. INT'L & COMP. L. REV. 303, 305 (2010) ("As modern society increasingly relies on global and domestic information structures, these structures tend to become targets during war and other hostilities.").

10. THE WHITE HOUSE, NATIONAL SECURITY STRATEGY 27 (2010), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

(USCYBERCOM), whose stated goal is to safeguard the integrity of the U.S. military computer systems.[11]

If cyber attacks continue to be characterized with military rhetoric as "cyberwarfare," it raises the question of which legal rules govern these activities. The answer will dictate a victim state's available remedies or responses under international law, and inform state and non-state actors how to lawfully conduct cyber activities. Ostensibly, a few choices exist: apply traditional law of war rules (as developed through existing treaties and customary international law (CIL)), develop new rules through an international treaty specific to "cyberwarfare" activities, or adopt alternative frameworks beyond the warfare paradigm.[12]

Many Law of Armed Conflict (LOAC) scholars propose that cyber attacks should be treated like advancements in conventional kinetic weaponry and may therefore qualify as uses of force under the law governing the use of armed force by states in international relations (*jus ad bellum*).[13] This means cyber attacks that met the threshold definition of a use of force would be unlawful under the U.N. Charter, which prohibits members from using or threatening to use force in their international relations,[14] and recognizes the inherent right of self-defense against force that qualifies as an armed attack.[15] Scholars also contend that cyber attacks are subject to the law governing the means and methods of warfare (*jus in bello*, or LOAC),[16] which requires that military hostilities follow such foundational principles as distinction,[17] proportionality,[18] and the law of neutrality during an armed conflict.[19]

---

11. Tod Leaven & Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny*, 12 N.C.L.J. & TECH. ON. 1, 1–2 (2010).

12. *Id.*

13. *See, e.g.*, MELZER, *supra* note 9; Catherine Lotrionte, *Symposium: International Law and the Internet: Adapting Legal Frameworks in Response to Online Warfare and Revolutions Fueled by Social Media: State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825 (2012); Roscini, *supra* note 6; Swanson, *supra* note 9.

14. *See* U.N. Charter art. 2, para. 4.

15. *Id.* art. 51. *See infra* Part III for a full discussion on cyber attacks as potential uses of force under the *jus ad bellum*.

16. MELZER, *supra* note 9, at 4.

17. Requiring that attackers "at all times distinguish between the civilian population and combatants, and between civilian objects and military objectives." Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

At the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, a group of international experts has gone further and published the *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[20] which is intended as a restatement and manual similar to the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* and the *Manual on International Law Applicable to Air and Missile Warfare*.[21] The *Tallinn Manual* analyzes cyber operations using existent *jus ad bellum* and *jus in bello* rules, with mostly successful results.[22] However, such extrapolation is not without problems. Several crucial impediments present themselves, which frustrate placing cyber attacks within the umbra of warfare—the greatest being the problem of attribution.[23] With the increasing participation of non-state actors in attacks against states around the world, the bounds of the LOAC have already become strained as experts debate whether, and how, the traditional LOAC rules apply to such non-state actors.[24] The difficulty of determining identities in cyberspace, where civilian hacker groups can conduct cyber attacks utilizing personal computers, makes this inquiry all the more perplexing.[25] Victim states may find themselves unsure which state should be held

18. Requiring that inadvertent or incidental civilian casualties and damage (collateral damage) not be excessive in relation to the anticipated military advantage. *Id.* art. 51.

19. Obligating neutral states to prevent their territory from being used by belligerents in an international armed conflict, and requiring belligerents to respect a neutral state's territory as inviolable by refraining from prohibited conduct in the neutral territory. Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, arts. 1, 5, Oct. 18, 1907, 36 Stat. 2415 [hereinafter Hague Convention]. *See infra* Part IV for a full discussion on whether cyber attacks may comply with the *jus in bello*.

20. Int'l Grp. of Experts, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013), *available at* http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 [hereinafter TALLINN MANUAL].

21. *Id.* at 1. *See* PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH AT HARVARD UNIV., MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2009), *available at* http://ihlresearch.org/amw/HPCR%20Manual.pdf; SAN REMO MANUAL ON MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Louise Doswald-Beck ed., 1995).

22. TALLINN MANUAL, *supra* note 20.

23. *Id.* at 1.

24. *See* Collin S. Allan, *Attribution Issues in Cyberspace*, 13 CHI.-KENT J. INT'L & COMP. L. 55 (2013); Lotrionte, *supra* note 13, at 855. The U.N. Security Council has implied the LOAC can in fact apply to non-state actors (authorizing the United States to use self-defense measures against al-Qaeda under Article 51 of the U.N. Charter); however, the contours of such application remain in debate. Lotrionte, *supra* note 13.

25. Allan, *supra* note 24, at 55.

responsible, assuming the cyber attack is traceable at all.[26] For example, the route traveled by the 2007 cyber attacks on Estonia was traced through Russia and several of its government institutions, but also traversed 177 other countries along the way.[27]

While the *Tallinn Manual* has been successful in elucidating how many traditional LOAC rules and principles apply to cyber attacks, its failure to address some glaring incongruities necessitates either supplementary international development or a departure from the warfare model altogether. Current manifestations of cyber attacks rarely achieve militaristic ends, but rather take the form of espionage, crime, or political and economic coercion.[28] This Article contends that because the nature of a cyber attack often precludes proper legal analysis under the *jus ad bellum* and the *jus in bello*, the effort of the *Tallinn Manual* and other LOAC experts to summarily insert the growing phenomenon into the war paradigm is premature. Instead, this Article argues, alternative legal regimes should be used to respond to cyber threats until international rules specific to cyber attacks develop. Part II of this Article provides an overview of relevant definitions and the unique setting of cyberspace. Consequently, Part III evaluates how cyberspace's principal architecture may render attribution of cyber attacks to states impractical. Part IV reviews the categorization of attacks as uses of force under the *jus ad bellum*, and how cyber attacks generally fall short of the definition. Part V examines the conduct of hostilities under the *jus in bello*, exploring how cyber attacks may comply with the principles of distinction, proportionality, and obligations under the law of neutrality. Finally, Part VI analyzes how alternate legal regimes, including domestic law enforcement and the international principle of non-interference, may prove more effective frameworks to govern malicious cyber activities.

II. DEFINING "CYBERWARFARE" AND ITS UNIQUE NATURE

To properly discuss the legal ramifications of international cyber attacks against states, working definitions of pertinent terms are

26. *Id.*

27. *Id.* While the legal countermeasures available to Estonia at the time remain unclear, the complicated route the cyber attacks followed clearly illustrates the attribution quagmire. Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 530 (2012).

28. TALLINN MANUAL, *supra* note 20, at 4.

warranted. The term "cyberspace" is used to describe the "space of virtual reality; the notional environment within which electronic communication (especially via the Internet) occurs."[29] Cyberspace encompasses email, the Internet, file transferring, as well as other programs that connect computer users.[30] Terminology specific to cyber activities has been developed to assist in categorizing the breadth of possible operations.[31] At the broadest level, any "reduction of information to electronic format" and its passage "between physical elements of cyber infrastructure" constitutes a "computer network operation" (CNO).[32] In the context of malicious cyber activities, CNOs can then be subdivided into three categorizations: (1) computer network attack (CNA),[33] (2) computer network exploitation (CNE),[34] or (3) computer network defense (CND).[35] CNEs are efforts "focused on intelligence collection and observation rather than on network disruption,"[36] and are presumed lawful under international law, which does not prohibit espionage.[37] CNAs and CNDs, on the other hand, "aim at altering or destroying the information contained in the targeted computer or computer network with the purpose of incapacitating . . . and/or of causing damage extrinsic to the targeted computer/network."[38] This Article discusses only CNAs and CNDs that potentially rise to the level of a use of force under *jus ad bellum* or are employed in an armed

29. *Cyberspace*, OXFORD ENG. DICTIONARY ONLINE, http://www.oed.com/view/Entry/240849?redirectedFrom=cyberspace& (last visited Dec. 16, 2013).

30. Gervais, *supra* note 27.

31. *See generally* MELZER, *supra* note 9, at 5 (summarizing categories of cyber operations).

32. *Id.*

33. Any cyber operation "aiming to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or to the computers and networks themselves." *Id.* (internal quotations and citations omitted).

34. Any cyber operation "enabling . . . intelligence collection to gather data from target or adversary automated information systems or networks." *Id.* (internal quotations and citations omitted).

35. Any cyber operation "taken to protect, monitor, analyse, detect, and respond to unauthorized activity within . . . information systems and computer networks." *Id.* (internal quotations and citations omitted).

36. Roscini, *supra* note 6, at 92. Examples of CNEs include stealing sensitive information such as IDs and passwords from computers through the use of "trap doors" (that allow external users to unknowingly access computer software) and "sniffers" (remote programs that intercept data transmitted over a network). *Id.* at 93.

37. *Id.*

38. *Id.*

conflict subject to the *jus in bello*.[39] The most prevalent forms of CNAs and CNDs are hardware and software corruption through the use of viruses and worms,[40] or distributed denial of service (DDoS).[41]

The U.S. Army's Cyber Operations and Cyber Terrorism Handbook defines a cyber attack as "[t]he premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives . . . [o]r to intimidate any person in furtherance of such objectives."[42] However, that definition is very broad, exceeding the bounds of what the LOAC considers to be an attack.[43] A narrower definition would proscribe "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them."[44] Yet these common definitions fail to demonstrate the essential notion of what constitutes an attack—an act of violence.[45] The *Tallinn Manual*, commensurate with LOAC definitions, defines a cyber attack as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction

39. Included are CNAs and CNDs deployed either by military combatants targeting a state, or non-state actors whose conduct is attributable to a state. The CNO designations are not exclusively military terms and may encompass otherwise private activities that do not implicate international law. *Id.*

40. *Id.* Viruses and worms are self-replicating programs that "can be installed . . . through chipping, hacking, or by simply e-mailing them." *Id.* A virus "attaches itself to a legitimate program on the target computer" and alters its function, other programs' functions, as well as the programs of computers connected to the host computer via a network. *Id.* A worm does not alter resident programs, but "captures the addresses of . . . target computer[s] and resends messages throughout the system so to cause a general slowdown and potentially a crash." *Id.*

41. A DDoS attack is accomplished when many computers simultaneously inundate a target network with large volumes of requests, rendering the network incapacitated. *Id.* A common cyber attack tactic, several notorious DDoS attacks have been conducted in the past several years, such as the coordinated website takedowns of Bank of America, Citibank, Wells Fargo, and JP Morgan Chase in 2012. Ellen Nakashima & Danielle Douglas, *More Companies Reporting Cybersecurity Incidents*, WASH. POST, Mar. 2, 2013, http://www.washingtonpost.com/world/national-security/more-companies-reporting-cybersecurity-incidents/2013/03/01/f7f7cb68-8293-11e2-8074-b26a871b165a_story.html.

42. U.S. ARMY TRAINING & DOCTRINE COMMAND, DCSINT HANDBOOK NO. 1.02, CRITICAL INFRASTRUCTURE THREATS AND TERRORISM, at VII-2 (2006).

43. *See infra* Part III.

44. Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422 (2011).

45. An "attack" is an "act[] of violence against the adversary, whether in offence or defence." Additional Protocol I, *supra* note 17, art. 49.

of objects."[46] In addition, the *Tallinn Manual* explains that "acts of violence" are not strictly confined to kinetic force, but that CIL recognizes many non-kinetic effects that can constitute attacks.[47] It is typically the consequences of an action, not its nature, that determine whether it is an attack; thus non-violent operations may be encompassed should their consequences prove destructive.[48] Furthermore, a cyber operation need not *directly* result in death, injury, or damage to qualify as an attack; indirectly damaging consequences would suffice.[49] Indeed, it would be an absurd technicality to exclude a cyber operation that indirectly leads to widespread death and destruction from being labeled an attack, where a kinetic attack that directly leads to the same result would be sufficient.[50]

Thus, for the purposes of this Article, cyber attacks are considered the "hostile use of cyber force" consistent with weaponized CNAs and CNDs meant to incapacitate, degrade, damage, or destroy a computer, computer network, website, data resident therein, or cause extrinsic damage to the target computer or network.[51]

However one formulates the definition of a cyber attack, it is essential to recognize the medium's technological nature. Fundamental to properly evaluating cyber attacks as warfare is a basic understanding of how information is transmitted via the Internet. Digital transmissions through cyberspace can be far-reaching and span the globe near instantaneously, with the tools required being widely available and relatively easy and cheap to acquire.[52] The Internet itself is not a physical structure, but a

46. TALLINN MANUAL, *supra* note 20, at 106.

47. For example, chemical, biological, or radiological attacks usually do not have kinetic effects, but are universally agreed as constituting "attacks" under the LOAC. *Id.*

48. Article 51 of Additional Protocol I expressly characterizes attacks as causing "loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof." Additional Protocol I, *supra* note 17, art. 51. By emphasizing the consequences of an attack without expressly delineating the form of an attack, it is suggested that the LOAC sought to encompass many different means that could result in destructive ends.

49. *See* TALLINN MANUAL, *supra* note 20, at 107.

50. *See id.*

51. Roscini, *supra* note 6, at 96.

52. *Id.* at 87–88; *see also* MELZER, *supra* note 9, at 5 ("Cyberspace not being subject to geopolitical or natural boundaries, information and electronic payloads are deployed instantaneously between any point of origin and any destination connected through the electromagnetic spectrum.").

"network of networks," or inter-network, and communication links following specific rules, or protocols, that allow computers and computer networks to exchange information.[53] The public Internet is just one of many thousands of inter-networks, which include many private inter-networks utilized by businesses and governments to connect remote locations.[54]

To communicate with one another, millions of individual host computers and computer networks utilize the Transmission Control Protocol/Internet Protocol (TCP/IP) to send and receive data.[55] Before being transmitted over the Internet, a host computer breaks up a data message, such as an email or video file, into many small packets, which are then independently routed to a recipient machine.[56] Through such "packet switching," each individual data fragment travels from the host computer to any number of other interconnected computers, networks, and routers composing the Internet until all of the packets reach their destination, often out of order, where the recipient machine reconstitutes the packets back into a single message.[57] The routes of individual packets are wholly unpredictable, with each packet potentially taking any one of a nearly innumerable array of alternate paths between routers around the world.[58] In this way, the Internet is decentralized, with no central server managing the traffic, nor any single entity wielding control or state wielding jurisdiction over all information conveyed.[59] By adopting the TCP/IP protocol for formatting, addressing, transmitting, routing, and receiving information packets, the Internet is a "survivable" network where each connected computer takes part in the transmission of information.[60] Unlike a system with a single master routing process, cyberspace can continue to function even if individual machines connected to it become damaged or incapacitated.[61]

---

53. PATRICIA L. BELLIA ET AL., CYBERLAW PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 17 (4th ed. 2011).

54. *Id.*

55. *Id.*

56. *Id.* at 19.

57. *Id.* at 18–19; *see also* MELZER, *supra* note 9, at 5.

58. *See* BELLIA ET AL., *supra* note 53, at 18.

59. *Id.* at 17; Gervais, *supra* note 27, at 529.

60. *See* BELLIA ET AL., *supra* note 53, at 18.

61. *Id.*

In contrast to traditional domains of warfare, cyberspace itself is the only entirely man-made domain.[62] As a result, it is maintained and operated by private and public entities, and can change in character very rapidly due to advancements in technology.[63] Among other technological attributes, the rapid pace at which cyberspace is expanding and cyber operations become more sophisticated has made the application of the LOAC difficult and unwieldy.[64]

III. THE PROBLEM OF ATTRIBUTION

Though cyberspace is theoretically accessible to all, tracing information transmitted through it can be particularly difficult.[65] Tactics such as IP spoofing[66] and the use of botnets[67] allow users to hide or counterfeit the true origin of an operation, making identification of perpetrators and attribution to states unreliable.[68] Two layers of anonymity must then be unraveled: (1) determining the identity of the individual operator of the cyber attack, and (2) determining whether the operator is a state actor (for example, a member of the military) or non-state actor whose conduct is attributable to the state.[69] In situations where the cyber attack clearly emanated from a state actor, attribution is simple; however, most cyber attacks tend to be conducted by individual non-state actors, which renders attribution extremely difficult.[70]

When the origin of an unlawful cyber attack has been traced to non-state actors, a victim state would need to prove another state exhibited sufficient control over the non-state actors before holding that state responsible.[71] However, the appropriate threshold of control required is a point of contention.[72] In traditional military

62. MELZER, *supra* note 9, at 5.
63. *Id.*
64. *Id.*
65. *Id.*
66. IP spoofing is the creation of data packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computer system. *Id.* at 5 n.6.
67. A botnet is an interconnected series of compromised computers used for malicious purposes. A computer becomes a bot when it runs a file that has bot software embedded in it. *Id.* at 5 n.7.
68. Roscini, *supra* note 6, at 96.
69. *See id.*
70. *See* Lotrionte, *supra* note 13, at 855.
71. *Id.*
72. *Id.*

contexts, two tests have been developed to determine whether actions by private non-state actors can be attributed to a supporting state.[73] The "effective control" and "overall control" tests are difficult to apply in a CNA context, though, and represent too high of a bar to effectively determine when a state may be responsible for the cyber attacks of a non-state actor.[74]

In *Nicaragua v. United States*,[75] the International Court of Justice (ICJ) administered an "effective control" test to determine that the actions of Nicaraguan rebels, including the killing, wounding, and kidnapping of Nicaraguan citizens, could not be attributed to the United States.[76] Despite the United States' supplying the rebels with arms and helping to plan offenses, the ICJ found the exhibited level of control insufficiently complete.[77] Thus, the United States could not be held accountable for the war crimes as a belligerent.[78] In its ruling, the ICJ set a very high standard for holding a state responsible for the actions of non-state actors.[79] "The effective control test requires a state to essentially be in total control of the non-state actors, and . . . specifically direct or enforce violations of international law."[80] Despite recognizing that the United States planned, collaborated, financed, trained, and supplied at least one of the rebel groups, the court was unable to conclude that rebels were acting on the United States' behalf because of the lack of total control.[81]

Thirteen years after *Nicaragua*, the International Criminal Tribunal for the Former Yugoslavia (ICTY) decided *Prosecutor v. Tadić*,[82] in which it implemented an "overall control" test with a less stringent threshold than the effective control test.[83] In determining whether to impute the acts of non-state actors to a state, the ICTY decided it "must be proved that the State wields overall control . . .

73. Allan, *supra* note 24, at 60.

74. *Id.*

75. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 181 (June 27) [hereinafter *Nicaragua*].

76. Allan, *supra* note 24, at 65–66.

77. *Id.* at 66.

78. *Id.*

79. *Id.* at 67.

80. *Id.*

81. *Id.*

82. Prosecutor v. Tadić, Case No. IT-94-1-A, Judgment (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

83. Lotrionte, *supra* note 13, at 855–56.

by equipping and financing . . . [and] by coordinating or helping in the general planning of [the] military activity," but concluded that the state did not necessarily have to give "instructions for the commission of specific acts contrary to international law."[84] The ICTY also qualified the test by highlighting the importance of location, requiring additional evidence of genuine control over direction and planning if the unlawful acts are committed in the territory of a state other than the controlling state.[85] The court also required a higher level of control for non-militarily organized groups than for militarily organized groups, necessitating that the former be given specific instructions by the state that lead to unlawful acts, or that the state endorse such acts after the fact.[86] In contrast to the effective control test, the overall control test is a more lenient standard that, in some circumstances, does not require that a state exhibit complete control over every action by the non-state actors.[87] Rather, the overall control test generally requires that a state finance, equip, and generally plan military activities of non-state actors before subsequent unlawful actions can be attributed to the state.[88]

In the context of a cyber attack, however, attempting to apply either test to prove attribution of state responsibility will likely fail. For example, the 2008 cyber attacks on Georgia are presumed to be the work of organized crime groups working on the Russian government's behalf; nonetheless, under either test it would be impossible to legally attribute the actions to Russia.[89] First, no evidence has been found connecting Russia and the organized crime groups, or the hackers employed.[90] Second, limited facts exist demonstrating the Russian government exhibited any control over the botnets used to attack websites.[91] Although Russia engaged in traditional military operations contemporaneous to the cyber attacks, that corroborative evidence alone is insufficient to establish attribution.[92] Under the effective control test, there is woefully

84. Prosecutor v. Tadić, Case No. IT-94-1-A, Judgment, ¶ 131 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).
85. Allan, *supra* note 24, at 69.
86. *Id.* at 70.
87. *See* Lotrionte, *supra* note 13, at 855–56.
88. *Tadić*, Judgment, ¶ 131.
89. Allan, *supra* note 24, at 57.
90. *Id.* at 75.
91. *Id.*
92. *See id.*

insufficient evidence that the Russian government exhibited the requisite degree of control over the cyber attacks. Application of the overall control test leads to a similar result.[93] Even under this less-stringent test, the tenuous connection between the Russian government and the organized crime groups impedes attribution because insufficient evidence exists to establish that Russia equipped, financed, or helped plan the cyber attacks, or that it endorsed them after the fact.[94] Considering the hackers who carried out the attacks at the organized crime groups' direction likely used their own equipment, Internet connections, and malware, searching for links to the Russian government appears futile.

Besides, scholars disagree whether either *Nicaragua* or *Tadić* are internationally controlling, which makes their application to cyber attack conflicts even more dubious.[95] The *Tallinn Manual* glosses over the attribution problem, merely noting the *Nicaragua* and *Tadić* tests without prescribing anything to mitigate the obstacles associated with applying the tests to cyber attacks.[96] Failing to address anonymity in cyberspace and the prevalent lack of evidence of state control quickly renders further analysis of cyber attacks under the *jus ad bellum* or *jus in bello* unproductive.

Ultimately, there will likely be frequent uncertainty whether a victim-state of a cyber attack is targeting the correct state for counter-measures. To avoid committing their own violations of international law, a victim-state may therefore allow non-attributable cyber attacks perpetrated at the direction of states to go unchecked and unpunished. Plus, the low cost of cyber attacks, the ease with which they can be carried out, and the fact that cyber attacks can be forged to appear to originate from an unrelated country frustrate the existing attribution regime to the point of potentially precluding further analysis under the *jus ad bellum* or *jus in bello*.

---

93. *Id.* at 76.

94. *Id.*

95. *See* Lotrionte, *supra* note 13, at 856 (noting that "after 9/11, international law held Afghanistan accountable because it failed to uphold its duties to prevent al Qaeda from harming other states from its territory . . . [and] . . . liable for terrorists attacks carried out by a non-state actor that no one argued was an agent of Afghanistan").

96. TALLINN MANUAL, *supra* note 20, at 32 and n.48. (preferring the effective control test under the commentary to Rule 6).

IV. WHETHER CYBER ATTACKS CAN RISE TO THE LEVEL OF A USE OF FORCE OR ARMED ATTACK UNDER THE *JUS AD BELLUM*

Assuming attribution is not a problem, then determining whether a cyber attack is unlawful requires an understanding of how force is defined in international law, and if a cyber attack is capable of reaching the threshold level to meet that definition.[97] U.N. Charter Article 2(4) prohibits member states from engaging in "the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[98] While Article 2(4) does not expressly define "force," a reading of the U.N. Charter makes clear that "at either end of the spectrum, it is apparent what is force and what is not force."[99] On one end, traditional military force using conventional military weapons clearly constitutes a use of force.[100] On the other end, political or economic coercion does not constitute a use of force,[101] as the purpose of the United Nations and the U.N. Charter "is to maintain international peace and security" and "to save succeeding generations from the scourge of war."[102] By excluding economic and political coercion from the definition of force, the drafters indicated that uses of force in violation of Article 2(4) focus strictly on military instruments.[103] The boundary between a use of force and a non-use of force therefore lies within the area between an exercise of traditional military coercion and an exercise of political or economic coercion.[104] Although the U.N. Charter is binding only on member states, the prohibition against the threat or use of force has been accepted as customary international law and binds all states regardless of U.N. membership.[105]

---

97. *See* Gervais, *supra* note 27, at 535–36.

98. U.N. Charter art. 2, para. 4.

99. Reese Nguyen, *Navigating* Jus Ad Bellum *in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1113 (2013) (emphasis omitted).

100. *See id.* at 1113–14 (noting that under the U.N. Charter "force" encompasses "armed force" and the "use of conventional military weapons").

101. *Id.* at 1114. "State practice supports these understandings: the United States, among other nations, has used forms of economic and political coercion since the early days of the Charter largely without legal challenge." *Id.*

102. Gervais, *supra* note 27, at 536.

103. *Id*. at 537.

104. Nguyen, *supra* note 99, at 1114.

105. *Id.* at 1112–13.

The ICJ has stated that U.N. Charter Articles 2(4) and 51, which recognizes the inherent right of self-defense against armed attacks,[106] apply to "any use of force, regardless of the weapons employed."[107] Although non-binding, ICJ advisory opinions are persuasive legal authority[108] in the international community and suggest the *jus ad bellum* encompasses all forms of force, including tactics used in cyberspace.[109] Accordingly, the United States takes the position that during peacetime, a cyber attack may qualify as a use of force.[110]

The drafters of the U.N. Charter deliberately excluded economic coercion from the definition of force in Article 2(4), focusing instead on military instruments.[111] The U.N. Charter's *travaux préparatoires* and the drafting histories of subsequent U.N. resolutions also indicate that traditional military coercion is the quintessential example of force.[112] However, the Charter does not explicitly define this distinction, which is further obfuscated by another necessary differentiation between a use of force and an armed attack.[113] An armed attack is a use of force so egregious that the victim would be justified in responding with force in self-defense.[114] A state may lawfully resort to self-defense only when a use of force reaches this level, which is consistent with the ICJ's stance[115] that "there is a substantive distinction between the 'use of force' and an 'armed attack.'"[116] Conventional notions suggest that "even small-scale bombings, artillery, naval or aerial attacks qualify as 'armed attacks' activating Article 51, as long as they result in, or are capable of

106. U.N. Charter art. 51.

107. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244, ¶ 39 (July 8).

108. *Advisory Jurisdiction*, INT'L CT. JUST., http://www.icj-cij.org/jurisdiction/index.php?p1=5&p2=2 (last visited Oct. 23, 2013).

109. *See* Lotrionte, *supra* note 13, at 854 ("A cyber operation that constitutes a use of force under Article 2(4) is an internationally wrongful act.").

110. *See* THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 9 (2011) ("The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior—in times of peace and conflict—also apply in cyberspace.").

111. *See* Nguyen, *supra* note 99, at 1114.

112. *Id.*

113. *Id*. at 1115.

114. *See* Shackelford, *supra* note 5, at 230–31.

115. *Nicaragua*, *supra* note 75, ¶ 195 (indicating that the difference between a use of force and an armed attack is one of "scale and effects").

116. Gervais, *supra* note 27, at 542.

resulting in, destruction of property or loss of lives."[117] "By contrast, the firing of a single missile into some unpopulated wilderness as a mere display of force would likely not be sufficient to trigger Article 51, despite violating Article 2(4)."[118] Thus, a victim-state seeking to use force in self-defense for a cyber attack must prove: (1) the attack rose to a level analogous to a traditional armed attack by military forces, and (2) the attack can be attributed to a state.[119] U.N. Security Council Resolutions 1368[120] and 1373[121] also suggest that attacks by individual non-state actors can trigger the right to self-defense.[122] In either case, as mentioned in Part III above, attributing a cyber attack to either a state or an individual non-state actor becomes extremely difficult when online anonymity and IP tracing may not necessarily implicate a culprit.[123]

The *Tallinn Manual* freely admits "cyber activities that occur below the 'use of force' (as this term is understood in the *jus ad bellum*) . . . have not been addressed in any detail."[124] This curious admission ignores the indefinite line CNAs and CNDs straddle between forceful and non-forceful coercion.[125] Specifically, because current manifestations of cyber attacks—such as DDoS disruptions, tracking malware, website defacement, etc.—can be non-destructive, such attacks would not rise to the level of a use of force under the *jus ad bellum*.[126] Cyber attacks' effects could greatly vary as they become more sophisticated, with potential results ranging from minor disruptions (website inoperability) to more debilitating or even

117. *Id.* at 543.

118. *Id.*

119. Shackelford, *supra* note 5, at 230–31. See Part II, *supra*, for a discussion on the difficulties of attributing cyber attacks to states.

120. S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001).

121. S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

122. *See* S.C. Res. 1368, *supra* note 120 (condemning the September 11, 2001 terrorist attacks that took place in New York, Washington, D.C., and Pennsylvania, and recognizing the inherent right of self-defense); S.C. Res. 1373, *supra* note 121 (reaffirming the recognition of the inherent right of self-defense in response to terrorist acts such as that of September 11, 2001).

123. A state's infrastructure may be used unknowingly by private "hacktivists" because IP routing is ad hoc, unpredictable, and capable of transferring packets through multiple countries to its destination. *See supra* notes 66–70 and accompanying text. Additionally, IP "spoofing" may fraudulently implicate an innocent state or individual. *Id.*; *see* Lotrionte, *supra* note 13, at 831 (noting "international law has not provided a clear standard for when a victim state may use force in self-defense against a non-state actor").

124. TALLINN MANUAL, *supra* note 20, at 4.

125. *See* Nguyen, *supra* note 99, at 1084, 1114.

126. *See* Nguyen, *supra* note 99, at 1127.

destructive consequences, such as: disabling power generators; cutting off military command, control, and communication systems; train derailments; airplane crashes; nuclear reactor meltdowns; or weapons malfunctions.[127] However, to analogize most current CNAs with kinetic military force as implied by Article 2(4) would expand the definition far beyond what the drafters intended.[128] Because the drafters excluded economic, ideological, and political coercion from the definition of force, their intent to focus on military instruments is evident.[129] Even in the unlikely event a cyber attack does meet the use-of-force definition, another question arises: whether the use of force rises to the level of an armed attack, thereby triggering a state's right to forcefully respond in self-defense to end the ongoing violation.[130]

A tangential problem arises when a CNA that appears facially non-destructive indirectly leads to loss of life or property.[131] Though rare, these types of CNAs would qualify as uses of force because they are analogous to traditional military coercion that lead to loss of life or property, but the same cannot be said when the CNA's effects are equivocally economic and military coercion.[132] In any case, several states have adopted the view that "cyber force is a type of armed force,"[133] accepting the premise that cyber operations can function on the same plane as traditional military force and thus falls under the purview of the *jus ad bellum*.[134]

The need to make sense of this categorical quagmire and identify what cyber activities qualify as uses of force and armed

127. Roscini, *supra* note 6, at 87–88.

128. Gervais, *supra* note 27, at 537.

129. *Id.*

130. For example, in the case of the 2007 Estonia attacks, to date no international consensus exists as to whether the Estonian government's options for retaliation would have been traditional military force, cyber attacks in-kind, or other non-violent measures such as reparations. Shackelford, *supra* note 5, at 196.

131. Gervais, *supra* note 28, at 543.

132. *Compare id.* at 537 (noting that cyber weapons can have versatile and innumerable effects that complicate categorization, but to treat "all forms of cyber attack as a use of force would require an implausibly broad reading of Article 2(4) that includes non-physical damage"), *with* Roscini, *supra* note 6, at 107–08 (analogizing that "if the Stock Exchange or other financial institutions were to be bombed . . . this would certainly be considered a use of armed force, and not economic coercion, even though the economic consequences of the action would by far outweigh the physical damage . . . one cannot see why the same conclusion should not apply when the Stock Exchange . . . is shut down by a cyber attack").

133. Roscini, *supra* note 6, at 108. The United States is among such states. *Id.* at 108–09.

134. *See id.* at 107–09.

attacks has led to the development of several analytical approaches: (1) an instrument-based approach, (2) a target-based approach, and (3) an effects-based approach.[135] The *Tallinn Manual* specifically references the effects-based approach,[136] but all three are rife with their own idiosyncratic flaws.

A. The Instrument-Based Approach

The instrument-based approach looks at the mode of attack and whether the weapon used possesses "physical characteristics traditionally associated with military coercion."[137] Thus, "The more analogous a new weapon is to conventional forms of military force, the more likely its operation will constitute a 'use of force' or 'armed attack.'"[138] This approach is derived from a textualist reading of the U.N. Charter.[139] "The Charter uses the terms 'use force,' 'armed force,' and 'armed forces' interchangeably," specifying that "armed force is action by air, sea, or land forces," which includes "demonstrations, blockade, and other operations by air, sea, or land forces" but does not include "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[140]

Under this reading, it would appear the Charter's drafters understood that force meant traditional military armed force and excluded other forms of coercion.[141] This view is strengthened by the U.N. Resolution on the Definition of Aggression, which includes armed invasions, port blockades, bombardments, and armed violations of territory.[142] Each of these examples involves physical force and violations of territoriality.[143] By this definition then, cyber attacks are not capable of rising to the levels of uses of force or armed attacks because computer code is neither a physical nor a

135. Nguyen, *supra* note 99, at 1117.
136. TALLINN MANUAL, *supra* note 20, at 45.
137. Hollis, *supra* note 4, at 1041.
138. Nguyen, *supra* note 99, at 1117.
139. *Id.*
140. *Id.* at 1118 (internal quotation marks omitted).
141. *Id.*
142. *Id.*; Definition of Aggression, G.A. Res. 29/3314, art. 3, U.N. Doc. A/RESRes/29/3314 (Dec. 14, 1974).
143. Nguyen, *supra* note 99, at 1118.

conventional military force.[144] By narrowly restricting the definition of force, the instrument-based approach is rigid and inflexible, requiring that new, unconventional forms of attack be dealt with through new international agreement, which may take decades to accomplish.[145]

To illustrate the instrument-based approach's shortcomings, the DDoS attacks upon Estonia in 2007 and the use of the Stuxnet worm on Iran's nuclear facility in 2010 would not be considered uses of force, despite having inflicted widespread disruption, because they were not accomplished using conventional kinetic weaponry.[146] Even cyber attacks that result in tangible physical destruction would be outside the purview of the *jus ad bellum* under this approach.[147] Given the ubiquitous nature of cyberspace and its critical position in modern society, this narrow approach swiftly loses any usefulness and relevance.

B. The Target-Based Approach

The target-based approach takes the opposite tack: it looks at the object of attack, and "automatically treats *any* cyber attack against critical . . . infrastructure as an armed attack because of the potential for severe consequences if such [infrastructure were] disabled."[148] Under this approach, emphasis is put on the status of the target, with "critical infrastructure" given privileged significance.[149] If an attack is made on critical infrastructure, it would trigger a state's right to self-defense, regardless of whether it comports with traditional military force.[150]

The problem with the target-based approach, however, is that each state individually defines what constitutes its critical infrastructure.[151] The United States, for example, designates sixteen sectors as critical infrastructure, including "food and agriculture, banking and finance, commercial facilities, communications,

144. *Id.*
145. *Id.*
146. *Id.* at 1119.
147. *See id.* at 1118. Cyber attacks are neither physical, nor conventional military weapons and "[t]he instrument-based view differentiates based on the nature of the assault, regardless of the consequences." *Id.*
148. *Id.* at 1117, 1119 (emphasis added).
149. *Id.* at 1119.
150. *Id.* at 1120.
151. *Id.* at 1119.

healthcare, and transportation" facilities.[152] While this approach takes into consideration a CNA's potential for non-physical disruption of national security, it is extremely broad.[153] Under this approach, nearly any cyber attack other than one targeting an individual personal computer would qualify as an armed attack.[154] If states can designate almost anything as critical infrastructure, the significance of the threshold between a use of force and an armed attack is obliterated.[155] Any cyber attack upon critical infrastructure, no matter how innocuous, would trigger a victim-state's right to self-defense, likely increasing the number of forceful exchanges between states.[156]

Moreover, such a broad approach incorrectly assumes that every invasion of a critical infrastructure demonstrates hostile intent to attack.[157] As previously mentioned, computer network exploitations (CNEs) are presumed lawful and do not demonstrate an intent to inflict damage, but are simply intelligence-gathering techniques.[158] Yet under a target-based approach, they would be considered armed attacks if perpetrated against a critical infrastructure.[159] Again, this approach may lead far too many states to invoke otherwise unreasonable Article 51 self-defense reprisals for cyber attacks with effects that clearly do not warrant such a response.[160]

For example, the cyber attacks on Estonia in 2007, despite having resulted in no physical damage, injury, or death, would be considered an armed attack under this rubric.[161] As a result, Estonia would have been entitled to forceful self-defense measures in retaliation for rendering newspaper and other websites temporarily

152. *Id.* at 1119–20; *Presidential Policy Directive 21: Critical Infrastructure, Security and Resilience*, THE WHITE HOUSE (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

153. Nguyen, *supra* note 99, at 1120.

154. *Id.* at 1121.

155. *See id.*

156. *See id.*

157. *Id.*.

158. *See supra* note 34 and accompanying text.

159. *See* Nguyen, *supra* note 99, at 1121. Under this approach, even cyber attacks designed for data-mining and information theft (espionage) could justify anticipatory self-defense. *Id.*

160. *See id.* (noting that any cyber attack, regardless of benignity, would permit responsive force); Gervais, *supra* note 27, at 541 ("[A target-based approach] raises the possibility of wrongly escalating force in response to a low-level cyber attack.").

161. Nguyen, *supra* note 99, at 1121.

inoperable.[162] The Syrian Electronic Army's benign attacks on Twitter, Skype, The New York Times, and CNN in 2013 would have also justified the United States in exercising self-defense measures.[163] Whether retaliatory measures would be strictly limited to CNAs or would also allow traditional military force is unclear, but in the event of the latter, such disproportionality between attack and response could trigger international repercussions.[164] Under the target-based approach, the Stuxnet virus that temporarily shut down Iran's nuclear facility may have constituted an armed attack, permitting Iran to use forceful counter-measures against both the United States and Israel, which would likely have escalated already-simmering tensions into full-scale war.[165] Despite its ability to accommodate the unorthodox attributes of cyber operations, the target-based approach would likely foster far more trouble than it prevents.

C. The Effects-Based Approach

Finally, the effects-based approach analyzes the consequences of an attack to determine whether it rises to the level of a use of force or armed attack.[166] The *Tallinn Manual* uses the "scale and effects" test as promulgated in *Nicaragua*.[167] This approach involves analogizing the effects of a cyber attack with the effects of a conventional weapons attack, filtering out "the most grave forms of the use of force . . . from other less grave forms."[168] Therefore, a cyber attack that produces physical destruction similar to that produced by a kinetic attack is more likely to qualify as an armed attack, while one that produces political or economic coercion will not (in accordance with U.N. Charter policy).[169] However, *Nicaragua* did not specify the factors used to make such a determination.[170] Furthermore, the

162. *See id.*

163. Christine Haughney & Nicole Perlroth, *Times Site Is Disrupted in Attack by Hackers*, N.Y. TIMES, August 28, 2013, http://www.nytimes.com/2013/08/28/business/media/hacking-attack-is-suspected-on-times-web-site.html; Nicole Perlroth, *Hunting for Syrian Hackers' Chain of Command*, N.Y. TIMES, May 18, 2013, http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted=all.

164. *See* Gervais, *supra* note 27, at 541.

165. *See* Nguyen, *supra* note 99, at 1121.

166. *Id.* at 1121–22.

167. TALLINN MANUAL, *supra* note 20, at 55.

168. *Nicaragua*, *supra* note 75, para. 191.

169. Nguyen, *supra* note 99, at 1122.

170. TALLINN MANUAL, *supra* note 20, at 55.

ICJ does not have binding authority on any parties other than the parties involved in the particular case adjudicated.[171] As a result, the "scale and effects" test is not necessarily the mandated test for categorizing uses of force and armed attacks, but in the context of cyber attacks it has become the most widely accepted.[172]

Michael Schmitt, editor of the *Tallinn Manual*, developed the most prominent effects-based approach consisting of six factors: (1) severity, (2) immediacy, (3) directness, (4) invasiveness, (5) measurability, and (6) presumptive legitimacy.[173] Under these criteria, the stronger the first five factors are, the more likely a cyber attack would be deemed a use of force; however, the stronger the sixth factor is, the less likely it is to be a use of force.[174] Although the effects-based approach carves a middle ground between the rigid instrument-based approach and the overbroad target-based approach, this particular test allows almost any cyber attack to be argued on the side of force.[175] Little clarification of the weight afforded each factor is provided, other than Schmitt himself citing severity as the most significant.[176]

In addition, such analysis may lead to contradictory interpretations of the same event. A CNA against a state lacking effective cybersecurity may cause enough damage to rise to the level of an armed attack, yet the same CNA against another state with robust cybersecurity might not.[177] Such a subjective approach may prove to be an impractical method to place cyber attacks on the same plane as conventional weaponry. On the other hand, a state with adequate cybersecurity may have little need to resort to self-defense measures afforded under Article 51 if a CNA proves ineffective or even goes unnoticed. A state vulnerable to cyber attacks that suffers legitimate harm, though, may rely heavily on Article 51, which may be its only practical deterrent to being victimized.

---

171. *See Frequently Asked Questions*, INT'L CT. JUST., http://www.icj-cij.org/information/index.php?p1=7&p2=2#6 (last visited Jan. 31, 2014).

172. Nguyen, *supra* note 99, at 1122.

173. *Id.* at 1122–23 (citing Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914–15 (1999)).

174. *Id.* at 1123. The sixth factor, presumptive legitimacy, hinges on whether it is a permissible form of coercion or not (e.g., economic versus military). *Id.*

175. *Id.*

176. *Id.*

177. *Id.* at 1124.

The *Tallinn Manual* notes that in some cases, the distinction is clear:

> any use of force that injures or kills persons or damages or destroys property would satisfy the scale and effects requirement. . . . [A]lso . . . acts of cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services, do not qualify as armed attacks.[178]

Yet, the *Tallinn* experts concede that "the law is unclear as to the precise point at which the extent of death, injury, damage, destruction, or suffering caused by a cyber operation fails to qualify as an armed attack."[179] Murkier still is the case of a cyber attack that does not result in direct physical injury, death, damage, or destruction, yet nonetheless has overwhelming negative effects, such as the crashing of a stock exchange.[180] Normally, such non-violent coercion would not be considered an armed attack.[181] Given current large-scale dependence on the Internet, however, such a crash could have a crippling effect on essential functions on which our society and government depend.[182]

The *Tallinn* experts also admit that under the effects-based rubric to date, "no international cyber incidents have . . . been unambiguously and publicly characterized by the international community as reaching the threshold of an armed attack."[183] Among the cyber events in Estonia (2007), Georgia (2008), and Iran (2010), only the Iranian Stuxnet incident presents a close call because it resulted in physical damage that rendered 1,000 of 5,000 centrifuges temporarily inoperable.[184] Yet there is no international consensus that even the Stuxnet event constituted an armed attack.[185] Ultimately, this reality points less to the inadequacy of the effects-based approach as a mode of analysis, and more to the likelihood that "cyberwarfare" is a misnomer and that characteristics

178. TALLINN MANUAL, *supra* note 20, at 55.
179. *Id.* at 56.
180. *Id.*
181. *Id.*
182. *Id.*
183. *Id.* at 57.
184. Nguyen, *supra* note 99, at 1098 n.132.
185. *See* TALLINN MANUAL, *supra* note 20, at 57.

of CNAs and CNDs may place them outside the bounds of the *jus ad bellum*.

V. CYBER ATTACKS AND COMPLIANCE UNDER THE *JUS IN BELLO*

The *jus in bello* (or LOAC) regulates the conduct of hostilities during an armed conflict.[186] Formed through a long-standing history of international treaties and CIL, the LOAC articulates the rules states rely on to determine whether their forceful conduct is lawful.[187] Central to the LOAC are the principles of distinction and proportionality and the law of neutrality.[188] In the context of cyberspace, questions arise concerning the proper means and methods of deploying CNAs so as to be in compliance with the LOAC's fundamental principles.[189] Part A of this section evaluates three sub-issues pertaining to the principle of distinction and proportionality: (1) how cyber combatants can distinguish their combatant status, (2) how combatants can distinguish between civilian and military objectives in cyberspace, and (3) whether cyber attacks are indiscriminate. Finally, Part B analyzes whether the architecture of cyberspace renders neutrality compliance unfeasible.

A. Whether Cyber Attacks Comply with the Principles of Distinction and Proportionality

A foundational principle of the LOAC is the principle of distinction, which requires attackers to "distinguish between the civilian population and combatants, and between civilian objects and military objectives" at all times.[190] This ensures that "the civilian population and individual citizens shall enjoy general protection against dangers arising from military operations"[191] without being made "the object of attack."[192] Even so, some civilian casualties are permissible as collateral damage during a military operation if the attacker made reasonable efforts to balance other foundational

186. Nguyen, *supra* note 99, at 1083 n.22 (citing Chris af Jochnick & Roger Normand, *The Legitimation of Violence: A Critical History of the Laws of War*, 35 HARV. INT'L L.J. 49, 52 (1994)).

187. Gervais, *supra* note 27, at 535.

188. *Id.* at 563.

189. *Id.* at 549.

190. Additional Protocol I, *supra* note 17, art. 48.

191. *Id.* art. 51.

192. *Id.*

principles of military necessity and humanity.[193] Such allowance for collateral damage lies at the heart of the principle of proportionality.[194] Inadvertent or incidental civilian casualties and damages that are not excessive in relation to the anticipated military advantage are lawful.[195] However, should a planned attack be expected to result in excessive civilian casualties or damage, commanders are required to cancel, suspend, or re-plan the attack.[196]

Conducting attacks in cyberspace makes complying with the principles of distinction and proportionality problematic.[197] The line between military and civilian targets in a cyber attack can be blurred and difficult to discern.[198] This is because cyberspace relies heavily on private civilian infrastructure.[199] Cyberinfrastructure is "spread and networked across the entire planet," making civilian and military cyberinfrastructure tightly interconnected.[200]

Accordingly, several issues need to be analyzed to determine whether cyber attacks comply with the principles of distinction and proportionality including: (1) whether cyber combatants properly distinguish themselves as military combatants, (2) whether cyber combatants properly distinguish between military and cyber objectives, and (3) whether cyber attacks are indiscriminate.

1. Distinguishing Cyber Combatant Status

The LOAC gives only lawful combatants the legal right to participate directly in hostilities.[201] Lawful combatants receive immunity from prosecution for acts that might otherwise incur criminal liability under domestic law, such as the right to kill enemy forces or attack military objectives.[202] Typically, uniformed members

193. Established by CIL, military necessity is the principle that permits states engaged in armed conflict to use only the degree of force, not otherwise prohibited by the LOAC, required to achieve the legitimate purpose of the conflict. *Id.* art. 51. The principle of humanity forbids the infliction of suffering, injury, or destruction not actually necessary for the accomplishment of legitimate military purposes. *Id.* art. 35.

194. *See* Gervais, *supra* note 27, at 569.

195. *See* Additional Protocol I, *supra* note 17, art. 51.

196. *See id.*

197. Gervais, *supra* note 27, at 565.

198. *Id.*

199. MELZER, *supra* note 9, at 30.

200. *Id.*

201. Additional Protocol I, *supra* note 17, art. 43.2.

202. Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 190 (2006).

of the military are considered lawful combatants, so long as: (1) they are commanded by a person responsible for subordinates; (2) they wear a fixed emblem recognizable at a distance; (3) they carry their arms openly; and (4) they conduct their operations in accordance with the laws and customs of war.[203] In this way, military combatants are required to "distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack."[204] Because this requirement is typically met by wearing military uniforms and openly carrying weapons, compliance may not be readily discernible in cyberspace: combatants can launch cyber attacks unobserved, and the weaponized nature of data transmissions can go undetected.[205]

The *Tallinn Manual* correctly states that if cyber operations are to be treated as warfare, then combatants engaged in cyber operations should not be exempt from displaying their combatant status.[206] The *Tallinn* experts also noted that CIL offers no definitive exceptions to this rule, regardless of circumstances.[207] However, some *Tallinn* experts did express support for a possible exception under CIL, namely that the requirement only applies where failure to wear a fixed distinctive sign would reasonably prevent an attacker from distinguishing between civilians and combatants.[208] Under such an exception, the requirement should only apply in circumstances where civilian and military persons and facilities co-exist and a heightened risk of mistaken civilian targeting is present.[209] Omitted from the discussion is whether a cyber attack itself should be marked to signal military status, similar to the marking of warships or military aircrafts.[210] Military forces are obligated to distinguish themselves from civilians, and common practice dictates that states

203. Regulations Respecting the Law and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277; Annex to Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2295, 205 Consol. T.S. 277.

204. Additional Protocol I, *supra* note 17, art. 44.3.

205. *Id.*

206. TALLINN MANUAL, *supra* note 20, at 99.

207. *Id.* Regardless of factors such as "distance from the area of operations or clear separation from the civilian population," compliance with this requirement must be met to maintain combatant status. *Id.*

208. *Id.*

209. *Id.*

210. *See id.*

further distinguish protected persons and sites within their military.[211]

The *Tallinn Manual* narrowly views distinguishing combatant status as merely requiring *uniformed* cyber combatants.[212] Some critics argue that requiring cyber combatants to wear uniforms is inadequate and nonsensical in the cyberspace context.[213] But a few simple alternatives exist to facilitate CNA compliance, such as creating universally recognized electronic identifiers that signal the status of persons or facilities that generated the transmission.[214] One straightforward solution might require the usage of a ".mil" extension for transmissions emanating from networks associated with the military.[215] Although this method may be ripe for abuse, the same can be said for traditional identifiers like military uniforms (or the lack thereof).[216] Here, the rules governing lawful ruses and unlawful perfidy will dictate the bounds of covertness that a cyber combatant may lawfully employ.[217]

Ruses are permissible strategies under the LOAC, and include the use of camouflage, decoys, mock operations, and misinformation to lead an enemy to make tactical mistakes.[218] Deception is key to a ruse's effectiveness.[219] In cyberspace, a ruse may take the form of a misinformation campaign, implemented by intentionally making misleading military documents unsecure in a military database.[220] In contrast, perfidy is prohibited by the LOAC and involves "[a]cts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the [LOAC], with intent to betray that confidence."[221] Common examples of perfidy include feigning civilian, or other non-combatant status.[222] Thus, requiring open display of a ".mil" extension may impinge on a cyber combatant's ability to remain covert in its cyber attack,

211. Brown, *supra* note 202, at 196.
212. TALLINN MANUAL, *supra* note 20, at 99.
213. Gervais, *supra* note 27, at 560.
214. Brown, *supra* note 202, at 196.
215. *Id.*
216. *Id.*
217. Gervais, *supra* note 27, at 559–60.
218. *Id.* (citing Additional Protocol I, *supra* note 17, art. 37).
219. *Id.*
220. *Id.*
221. *Id.* at 560 (citing Additional Protocol I, *supra* note 17, art. 37).
222. *Id.*

rendering the cyber attack non-perfidious and in compliance with the LOAC.[223]

A more sophisticated method of distinguishing cyber combatant status may be using an identifying line of code, which may preserve the ability to employ lawful ruses in cyberspace.[224] A cyber combatant could employ a cyber attack utilizing an otherwise innocuous extension, such as ".com," while the source code is embedded with a line distinguishing the communication as military in nature.[225] Similar to camouflage, the cyber attack can exercise deception and maintain status as a lawful ruse.[226] Covertness does not necessarily transform an otherwise lawful attack into a violation of the LOAC, so long as the attack remains on the lawful side of perfidy.[227] The same principles should apply in cyberspace, as the "[LOAC rules] are designed to regulate the use of force and moderate its consequences," thereby maintaining order to war and ensuring trust that combatants are utilizing the same protocol.[228] By requiring states to comply with simple identifying techniques in their CNAs, the LOAC would be satisfied,[229] cyber combatants would preserve their combatant immunity,[230] and civilians would be able to discern between weaponized CNAs and normal civilian data transmissions.[231]

2. Distinguishing Between Civilian and Military Objectives

Cyberinfrastructure is characterized by a structural reliance upon civilian infrastructure.[232] Consequently, probable targets of a cyber attack are likely to be "dual-use" objects, sharing both a civilian purpose and a military purpose during an armed conflict.[233] As a

223. *See* Brown, *supra* note 202, at 196; Gervais, *supra* note 27, at 560 (citing Additional Protocol I, *supra* note 17, art. 37).

224. Gervais, *supra* note 27, at 560.

225. *See id.*

226. *Id.* at 559 (citing Additional Protocol I, *supra* note 17, art. 37).

227. *Id.* at 561.

228. *Id.*

229. *Id.* at 560.

230. Brown, *supra* note 202, at 190.

231. Gervais, *supra* note 27, at 560.

232. MELZER, *supra* note 9, at 30.

233. *Id.*; Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, 87 U.S. NAVAL WAR C. INT'L LAW STUD. 89, 96 (2011). A civilian object that serves a military purpose during an armed conflict becomes a military object eligible for attack. Some traditional examples of dual-use infrastructure include bridges and power grids. Gervais, *supra* note 27, at 568.

result, attackers must take a higher level of precaution in identifying dual-use objects as potential military objectives, as well as take reasonably feasible steps to minimize civilian casualty and damage.[234] Complying with the principles of distinction and proportionality while conducting cyber attacks is complicated by the fact that civilian cyberinfrastructure may be unpredictably used for military purposes.[235] Such variance would make it difficult to determine precisely when and where dual-use objects are contributing to military action, as well as if their destruction would provide a military advantage.[236]

Because cyberinfrastructure is composed of dual-use objects, a wide array of targets may qualify as military objectives.[237] For example, a military's reliance upon "software and hardware produced for the civilian population" could make the manufacturers vulnerable as legitimate "war-supporting military objectives."[238] Further, because cyberspace is now an integral aspect of the U.S. economy, many financial institutions with cyber presence could be characterized as "war-sustaining objects" and thus military objectives.[239] Some cyber attacks will easily comply with the principle of distinction, such as targeting a strictly military air traffic control system.[240] Other attacks will clearly violate the rule, such as targeting hospitals, museums, or places of worship.[241] The difficulty lies in cases somewhere in the middle, where dual-use facilities are at play.[242]

The *Tallinn Manual* recapitulates existing CIL rules regarding distinction and proportionality, with the caveat that "determination[s]

234. MELZER, *supra* note 9, at 30 (citing Additional Protocol I, *supra* note 17, arts. 57, 58). Such precautions include choosing military objects with minimal potential for collateral damage (and conversely, abstaining from disproportionate attacks), attempting to remove civilian population and objects from the vicinity of military objectives (via warning, evacuation, etc.), and avoiding military objectives near densely populated areas (where feasible). Additional Protocol I, *supra* note 17, arts. 57–58.

235. MELZER, *supra* note 9, at 30–31.

236. *Id.*

237. Indeed, 95 percent of all military communications use civilian networks at some stage of their transfer. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 852–53 (2012).

238. Schmitt, *supra* note 233, at 96–97.

239. *Id.* at 97.

240. Hathaway et al., *supra* note 237, at 852.

241. *Id.*

242. *Id.* at 852–53.

of whether an object is a civilian object protected from attack, and not a military objective, must be made on a case-by-case basis."[243]

Interestingly enough, a majority of *Tallinn* experts agreed that data should not be considered a military objective.[244] However, the majority of *Tallinn* experts did acknowledge that a cyber operation that targets data alone may qualify as an attack if it affects the functionality of the resident computers or network.[245] A minority of *Tallinn* experts balked at the delineation, since mere deletion of "extremely valuable and important civilian datasets would potentially escape the regulatory reach of the [LOAC]."[246] For these experts, the severity of the harm was paramount, but the majority characterized this concern as *de lege ferenda*.[247]

On the topic of cyberspace's dual civilian and military nature, the *Tallinn* experts recognized that "all dual-use objects and facilities are military objectives, without qualification;"[248] however, they downplay the extensive ramifications of that statement. The *Tallinn* experts acknowledged that "[i]t may be impossible to know over which part of the network military transmissions . . . will pass," but rejected the inevitable conclusion that the entire Internet could be deemed a military objective in time of war as "so highly unlikely as to render the possibility purely theoretical."[249] Theoretical or not, destroying the entire Internet as a military objective is analogous to destroying an entire array of roads when it is unknown which one the enemy will take.[250] To dismiss that possibility appears shortsighted given that data packets take unknowable paths through cyberspace.[251] This hypothetical doomsday scenario for the entire Internet might simply be an inevitable result of transposing LOAC rules onto cyberspace. Without more specific rules limiting the targeting of dual-use objects to individual networks or segments of networks, targeting the Internet as a whole could be plausible should the military advantage outweigh the civilian harm. However, the

243. TALLINN MANUAL, *supra* note 20, at 125.
244. *Id.* at 127.
245. *Id.*
246. *Id.*
247. *Id.* What the law ought to be (*de lege ferenda*), as opposed to what the law is (*de lege lata*). BLACK'S LAW DICTIONARY (9th ed. 2009).
248. TALLINN MANUAL, *supra* note 20, at 134.
249. *Id.* at 135–36.
250. *Id.* at 135.
251. For a discussion of packet switching, see *supra* Part II.

principle of necessity may prove sufficient to appropriately limit CNAs to the minimum level reasonably calculated to provide a military advantage.[252] Because the Internet is utilized for sensitive civilian purposes such as emergency response, disaster relief, and medical diagnosis and records, any damage or loss of life resulting from disabling the Internet would have to be considered in determining whether the cyber attack is proportional,[253] which might preclude an "all or nothing" Internet-wide assault.

3. Avoiding the Use of Inherently Indiscriminate Cyber Attacks

Indiscriminate attacks are prohibited by the LOAC.[254] Such attacks are those not directed at a lawful military objective, cannot be directed at a lawful military objective, or employ a means that cannot be controlled such that the nature of the attack would affect military objectives and civilian objects alike.[255] Attacks that are deemed indiscriminate constitute war crimes.[256]

In the cyberspace context, the question arises whether cyber attacks, or at least a subset of them, are per se indiscriminate. Some types of malware (for example, viruses and worms) that are targeted at military systems might inadvertently spread from the military objective to civilian objects.[257] The Stuxnet virus, for example, escaped Iran's Natanz nuclear facility due to a programming error and spread across the open Internet,[258] leading to infections in civilian Iran, Indonesia, and India.[259] Although such collateral damage may be controlled or mitigated, it remains unclear how much damage would be justified in a cyber attack on a dual-use military

252. *See supra* note 193 and accompanying text; TALLINN MANUAL, *supra* note 20, at 136 (emphasizing that "particular attention must be paid to the requirement to conduct operations in a manner designed to minimize harm to the civilian population and civilian objects" and that "[a]n attack on the Internet itself . . . might equally run afoul of the principle of proportionality").

253. TALLINN MANUAL, *supra* note 20, at 136.

254. Additional Protocol I, *supra* note 17, art. 51.

255. *Id.*

256. Rome Statute of the International Criminal Court, July 17, 1998, UN Doc. A/CONF. 183/9, art. 8.

257. MELZER, *supra* note 9, at 30.

258. Sanger, *supra* note 7.

259. *W32.Stuxnet*, SYMANTEC ENTERPRISE SECURITY RESPONSES, http://www.symantec.com /security_response/writeup.jsp?docid=2010-071400-3123-99 (last visited Nov. 16, 2013).

objective that serves a significant civilian function.[260] Customary international law indicates that the higher precautions required when targeting a dual-use object may provide sufficient deterrence against employing a potentially indiscriminate CNA.[261] But because cyber infrastructure is globally interconnected, a cyber attack that employs self-propagating means may unpredictably affect civilian objects regardless of the amount of precaution an attacker employs, suggesting that certain CNA techniques (for instance, viruses and worms) should be deemed inherently indiscriminate and thus prohibited.[262] The notion conflates the nature of the CNA with the way information is transmitted ad hoc across the Internet. Though a CNA may be carefully crafted, the indeterminable route to a target may bring the CNA in contact with unknown, vulnerable machines and access points, making TCP/IP indiscriminate, not necessarily the CNA itself.[263] Unfortunately, states may have to accept that a cyber attack's legality is infused with more uncertainty than planned traditional attacks.[264] Such was the conclusion of the *Tallinn* experts, who found the uncertainty to be an ordinary consequence not unlike that which applies to conventional weaponry deemed uncontrollable or insufficiently precise.[265]

A related problem is determining the degree of harm to a civilian object sufficient to violate the principle of distinction.[266] Implicit in this inquiry is the question of whether data itself constitutes an object within the meaning of the LOAC,[267] making increasingly strange the *Tallinn* experts' declaration that data should not be considered a military objective. Any cyber operation, whether espionage, exploitation, attack, or defense, will involve at least temporarily deleting or changing data existent on the targeted system.[268] In fact, because most cyber attacks use non-destructive

260. *See* MELZER, *supra* note 9, at 30 (contemplating whether a belligerent would be justified in "incapacitat[ing] a domain name server directing global internet traffic, or [destroying] a major intercontinental submarine cable, in order to prevent their use for hostile cyber operations if more than 90% of the data transmitted are of civilian nature").

261. *See id.*

262. Gervais, *supra* note 27, at 570.

263. *Id.* at 538 ("The weakness of this model is that the effects of cyber attacks may be indiscriminate and uncontrolled once unleashed.").

264. Hathaway et al., *supra* note 237, at 851.

265. TALLINN MANUAL, *supra* note 20, at 145–46.

266. MELZER, *supra* note 9, at 31.

267. *Id.*

268. *Id.*

means, such as DDoS attacks, data manipulation will likely be the major form of collateral damage observed.[269] Excluding data from eligibility as a military objective seems nonsensical, considering its deletion or manipulation may prove an exceedingly effective military advantage.[270] An additional inquiry is what degree of unavoidable civilian harm is sufficient to make a cyber attack disproportionate.[271] If the data manipulation is minimal, temporary, or otherwise unharmful, even a breach onto the open Internet resulting in widespread collateral damage could be deemed *de minimis*. Some data manipulation CNAs, such as DDoS attacks, represent hardly any risk at all of collateral damage or indiscriminate targeting because they are not self-propagating and are directed at a specific IP address.[272] However, more harmful cyber attacks that result in great civilian harm, such as worms or viruses meant to disrupt critical systems like the electrical grid, may unlawfully violate the principle of proportionality, despite the object of attack being data instead of a building or physical structure.[273] Thus, it seems plausible that data can and should be construed as a valid military objective limited by the same principles of distinction and proportionality applicable to traditional physical military objectives.

B. Cyber Attacks as Potential Violations of the Law of Neutrality

During an international armed conflict, a neutral state is obligated to prevent its territory from being used by belligerents in the conflict.[274] Likewise, the belligerents must respect a neutral

269. *See id.*

270. The aim of cyber attacks is not always physical destruction of hardware, and thus the threshold for violating civilian object immunity should also necessarily encompass non-physical harms. *See id.* (noting "data should be regarded as an object which may not be directly targeted unless it fulfills all defining elements of a military objective"). *But see* Schmitt, *supra* note 233, at 96 (proposing the characterization of all data as objects "overbroad" and that "the determinative question is whether the consequences attendant to its destruction involve the requisite level of harm to protected physical objects or persons").

271. TALLINN MANUAL, *supra* note 20, at 136.

272. *See id.* at 131–32. ("This method of cyber attack would violate Rule 50 because the attacker treats the military computers as a single target and by doing so harms the civilian computers when it was not necessary to do so.").

273. *Cf.* Gervais, *supra* note 27, at 570 (noting that viruses and worms can "quickly spiral out of control, infiltrating civilian systems and causing damage to property that far surpasses the intent of the cyber attacker," and that "the relative inability of a cyber attack to discriminate raises questions of its lawfulness").

274. Hague Convention, *supra* note 19, art. 5.

state's territory as "inviolable"[275] and refrain from prohibited conduct within its boundaries.[276] This law of neutrality can be interpreted to include operations in cyberspace.[277] A neutral state's obligation to enforce its neutrality, then, is triggered by the nature of the transmission: as a weapon (impermissible) or as a communication (permissible).[278] Data sent via the Internet can take either form, and the transmission's true nature may not be discernible without inspection.[279] Impliedly, a neutral state might be required to actively monitor, intercept, and filter all transmissions that enter its cyberinfrastructure.[280] Longstanding CIL, however, does not require a neutral state to actively prevent belligerents' use of "telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[281] Data transmissions cannot be geographically routed with any accuracy to avoid the use of a neutral state's telecommunications infrastructure.[282]

Neutral states are thus exempted from enforcing a prohibition against belligerents' use of "telegraph or telephone cables or of wireless telegraphy."[283] In the end, the law of neutrality may require neutral states to prevent belligerents from conducting hostile cyber attacks from within their territory, but not from passing externally originating cyber attacks through its publicly accessible cyberinfrastructure.[284]

The *Tallinn Manual* supports the interpretation that a neutral state does not have an obligation to prevent belligerent use of its cyberinfrastructure for communications.[285] However, the *Tallinn*

275. *Id.* art. 1.

276. Such prohibited conduct includes "mov[ing] troops, or convoys of either munitions of war or supplies across the territory of a neutral Power" and "(a) erect[ing] on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea; (b) us[ing] any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages." *Id.* arts. 2–3.

277. MELZER, *supra* note 9, at 20.

278. *Id.*

279. *Id.* ("From a technical point of view the accurate answer is that, depending on the precise nature and design of the cyber operation in question, either option can be the case.").

280. *Id.*

281. Hague Convention, *supra* note 19, art. 8.

282. MELZER, *supra* note 9, at 20.

283. *Id.* at 5. Data packets are sent ad hoc, meaning routes are unpredictable and not pre-determined. *See* BELLIA ET AL., *supra* note 53, at 18.

284. MELZER, *supra* note 9, at 20.

285. *See* TALLINN MANUAL, *supra* note 20, at 252.

experts disagreed about whether a state violated the *Tallinn Manual* by transmitting a cyber attack across neutral cyberinfrastructure, or whether a neutral state must prevent passage of a cyber attack across its cyberinfrastructure.[286] The attributes of cyberspace make compliance with this rule unusually complex. Because CNAs and CNDs may utilize "zombie computers located in one country to harm networks in another country—without [the] knowledge of any individual, much less the government," two challenges present themselves.[287] First, a country may be unaware that its neutrality is threatened at all.[288] Second, lawful responses to violations of the law of neutrality depend upon correctly identifying the country of origin.[289] As a result, the impracticability of attribution in cyberspace may preclude complete neutrality analysis.[290]

Cyber combatants using "zombie computers" or IP spoofing may be conducting cyber attacks from within a neutral state, but to the neutral state the origin of the cyber attacks may look external or the nature of the transmission may look communicative.[291] Thus, the neutral state may be unaware that its obligation to maintain neutrality has been triggered, or it may be unable to identify which state it should direct preventative measures against once known.[292] Further clarification is required, then, of attribution and the law of neutrality as they relate to cyber attacks to facilitate proper application of the LOAC. Such development might remove impediments to attribution and any subsequent LOAC analysis.[293]

VI. ALTERNATIVES TO THE *JUS AD BELLUM* AND *JUS IN BELLO* WHEN RESPONDING TO CYBER ATTACKS

When a cyber attack cannot accurately be categorized as a use of force, attribution to a state is impossible, or violations of conducting hostilities are inconclusive, there are several alternate means by which a victim state may seek relief or respond. The most practical include: (1) prosecuting CNAs or CNDs as crimes under domestic

286. *Id.* at 252–53.
287. Hathaway et al., *supra* note 237, at 856.
288. *Id.*
289. *Id.*; *see also supra* Part III.
290. Hathaway et al., *supra* note 237, at 856.
291. *See id.*
292. *See id.*
293. *See id.*

law; (2) seeking reparations for violating the non-interference principle; and (3) improving domestic cybersecurity. The alternatives are discussed in order of individual efficacy and relative feasibility.

A. Domestic Prosecution for Cybercrimes

A state may seek to treat cyber attacks as criminal acts, rather than violations of international law.[294] If so, domestic law enforcement would be the appropriate means to address the attack, similar to prosecuting domestic criminals "committing fraud and stealing identities online."[295] In fact, most harmful cyber operations are acts of cyber crime, such as identity theft and espionage, and relatively few cyber attacks would truly implicate either the *jus ad bellum* or *jus in bello*.[296]

The United States has several statutes that criminalize various cyber activities, including the Computer Fraud and Abuse Act of 1984[297] and the Economic Espionage Act of 1996.[298] These laws criminalize "fraud involving devices, computers, or email; malicious interference in communication lines, stations, or systems; electronic communication interception; illicit access to electronic communications and records; and recording of dialing, routing, addressing, and signaling information."[299] Despite their breadth, these domestic laws had been limited by their extraterritorial inapplicability.[300] The USA PATRIOT Act of 2001, though, broadened the ban against access device fraud and computer fraud to encompass perpetrators outside the jurisdiction of the United States.[301] Expanding the U.S. domestic law that is currently outside the scope of the PATRIOT Act may enable full prosecution of any and all cyber attacks targeted against the United States or its citizens.[302] Legislators could amend other statutes bearing on cyber attacks to expressly include extraterritorial reach, which, if

294. Lotrionte, *supra* note 13, at 828–29.
295. *Id.*
296. *Id.* at 838.
297. 18 U.S.C. § 1030 (2006).
298. *Id.* § 1831.
299. Hathaway et al., *supra* note 237, at 874.
300. *See id.*
301. *Id*. at 874–75.
302. *Id.* at 877.

reciprocated internationally, could increase enforcement and legitimacy.[303]

Similarly, the 2001 Council of Europe Convention on Cybercrime,[304] to which the United States became a party in 2006, represents the first international effort to criminalize various computer activities.[305] The Cybercrime Convention established a "common criminal policy aimed at the protection of society against cybercrime."[306] The Cybercrime Convention includes offenses related to illegal access, data interference, and system interference of computer data and systems, and requires party states to adopt domestic legislative measures establishing criminal offenses and penalties for such acts.[307] Parties to the Convention must also cooperate with each other in investigations and proceedings.[308] Such cooperation may also limit parties' ability to conduct cyber attacks that contravene the Convention's intent.[309]

As of January 2012, thirty countries are parties to the Cybercrime Convention, while sixteen others are merely signatories.[310] According to the Vienna Convention on the Law of Treaties, a party to a treaty consents to be bound by all provisions of the treaty, unless the party makes express reservations to specific provisions.[311] On the other hand, signatories that have not yet ratified a treaty are not bound by the specific provisions of the treaty, but they are nevertheless bound not to violate the treaty's general objective and purpose.[312] Thus, a party state to the Cybercrime Convention may be deterred from launching a cyber attack against another party state, knowing that such conduct would trigger sanctions under the would-be victim state's domestic laws.[313] Signatory states may also be deterred because a cyber attack against a party state would blatantly defeat the Cybercrime Convention's

303. *Id.*
304. Convention on Cybercrime, Council of Europe, E.T.S. No. 185, Nov. 23, 2001 (entered into force July 1, 2004) [hereinafter Cybercrime Convention].
305. Hathaway et al., *supra* note 237, at 862–63.
306. Cybercrime Convention, *supra* note 304, pmbl.
307. Hathaway et al., *supra* note 237, at 863.
308. *Id.* at 863–64.
309. *Id.* at 864.
310. *Id.* at 863 n.200.
311. Vienna Convention on the Law of Treaties art. 17, May 23, 1969, 1155 U.N.T.S. 331.
312. *Id.* art. 18.
313. Cybercrime Convention, *supra* note 304, art. 13.

general purpose to protect society against cybercrime through internationally cooperative prosecution.[314] Unfortunately, the deterrent effect on signatories may be rendered toothless by the fact that there are no clear repercussions for breach of the Convention's general purpose.[315] Despite such limitations, the Cybercrime Convention represents the most developed international cybercrime framework in existence.[316] Further, it offers a starting point for developing a fully comprehensive international cybercrime regime capable of avoiding the pitfalls of attribution and use of force categorization that burden the *jus ad bellum*.[317]

In contrast to the LOAC, a state may pursue the cybercrime route because a CNA may not rise to the level of a use of force or is traced to a private individual(s) whose conduct could not be attributed to a state.[318] Indeed, treating cyber attacks as cybercrime may prove preferable or even necessary when the attacks are neither serious nor large enough to merit international attention.[319] Therefore, although current international laws may not be sufficient to effectively counter cyber-attacks, it is certainly possible to use current domestic criminal law to combat cyber attacks in the United States.[320] Until the international uncertainty surrounding cyber attacks as acts of war is resolved, it makes sense for the criminal justice system, not the national defense, to adjudicate alleged violations.[321] Furthermore, treating cyber attacks as domestic crimes may increase international cooperation, as is required under the Cybercrime Convention or other extradition laws.[322] By contrast, under the LOAC, neutral states may be hesitant to assist victim states for fear of violating neutrality principles. Cybercrime prosecution is also advantageous because domestic laws can be implemented in a much quicker, more efficient, and effective manner than developing

314. Hathaway et al., *supra* note 237, at 864.
315. *See id.*
316. *Id.*
317. *See id.*
318. *See* Leaven & Dodge, *supra* note 11, at 17.
319. *See id.*
320. *Id.*
321. Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 55 (2009).
322. *See, e.g.*, Cybercrime Convention, *supra* note 304.

an international treaty[323] and would be applicable to all perpetrators, not just the treaty parties.

Consequently, prosecuting a CNA as a cybercrime circumvents the problem of attempting to categorize the attack as a use of force under the *jus ad bellum*, only to find the attack attributable to an individual and not a state.[324] A victim state would avoid wasting effort and resources meticulously studying the CNA, gathering evidence to support state attribution, and preparing a lawful LOAC compliant response to the CNA.[325] Instead, the effort and resources could be used to domestically prosecute the individual associated with the IP address responsible for originating the CNA—a much easier task than proving state responsibility through the demanding *Nicaragua* or *Tadic* tests.[326]

The United States has advocated for increased focus on domestic countermeasures, while discouraging the development of a cyberwarfare international treaty.[327] Treating cyber attacks as criminal acts recognizes domestic prosecution's efficacy and begins to shift the paradigm away from warfare.[328] If further domestic development occurs, such as extending extraterritorial reach to domestic statutes bearing on cybercrime or the Cybercrime Convention globally proliferating, "cyberwarfare" might eventually be confined to the *jus in bello*, where a CNA's place as a military tool is more apparent and the legal issues are less significant and pervasive than in the *jus ad bellum*.

B. Reparations for Violations of State Responsibility and the Principle of Non-Intervention

Despite a cyber attack potentially failing to rise to the level of a use of force, international law dictates that such an action may still be unlawful as a violation of state responsibility and the principle of non-intervention.[329] While not explicit in the U.N. Charter, Article

323. Leaven & Dodge, *supra* note 11, at 17.
324. *See id.*
325. *Id.* at 18.
326. *See id.*
327. *Id.* at 20.
328. *See id.* at 21.
329. Lotrionte, *supra* note 13, at 858; Hathaway et al., *supra* note 237, at 842; *see also* Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT SECURITY LAW 211 (2012) (arguing that cyber attacks that are coercive in nature will violate non-intervention principles embedded in international law).

2(1) impliedly invokes the concept, stating that "[t]he Organization is based on the principle of the sovereign equality of all its Members."[330] The principle has been affirmed by the ICJ in *Nicaragua*[331] and is considered an established principle of CIL.[332]

The prohibition against intervention "is a corollary of every state's right to sovereignty, territorial integrity and political independence."[333] Prohibited interference constitutes what the ICJ referred to in *Nicaragua* as "matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy."[334] Similar to the duty to respect a state's neutrality and its territorial sovereignty, the principle of non-intervention should apply to cyberspace as well.[335] Intentionally intruding into a state's cyberspace and interfering with a state's ability to maintain its sovereignty in the virtual realm could represent a violation of international law, whether it rises to the level of use of force or not.[336] Establishing a violation of the non-intervention principle will thus require determining whether the cyber attack was intended to coerce a policy change upon matters the victim state is entitled to freely determine.[337] To illustrate, the 2007 DDoS attacks on Estonia were inflicted upon both the private and public sectors, including websites run by the Prime Minister, his political party, the office of the President, Parliament, and the State Audit Office, for approximately three weeks.[338] The attacks were partially motivated by the government's decision to relocate a monument, a decision that "remains the free choice of any government."[339] Consequently, despite the DDoS attacks failing to rise to the level of a use of force

330. U.N. Charter, art. 2, para. 1.

331. *Nicaragua*, *supra* note 75, ¶ 205.

332. Buchan, *supra* note 329, at 211.

333. OPPENHEIM'S INTERNATIONAL LAW 428 (Robert Jennings and Arthur Watts, eds., 9th ed. 1992).

334. *Nicaragua*, *supra* note 75, ¶ 205.

335. *See* Buchan, *supra* note 329, at 211.

336. *Id.*; *see also* Kastenberg, *supra* note 321, at 56–57 (explaining that if a neutral state takes no action in policing individual cyber-attacks, it loses its cyber-neutral status); Leaven & Dodge, *supra* note 11, at 22 (arguing that because "cyberwarfare may be properly categorized as subject to 'legislative action' under the United Nations, the United Nations Security Council may be able to act affirmatively").

337. Buchan, *supra* note 329, at 223, 226.

338. *Id.* at 225–26.

339. *Id.* at 218, 226.

under U.N. Charter Article 2(4), they likely qualified as an unlawful intervention upon Estonia's sovereignty.[340]

Though enforcing such a violation may prove difficult in states that emphasize an almost unlimited right of free speech, such enforcement presents a mechanism by which those states whose sovereignty has been interfered with are entitled to reparations and non-military counter-measures.[341] A non-interference approach removes one of the major prongs under the *jus ad bellum*: categorizing the cyber attack as a use of force or armed attack.[342] Assuming state attribution is possible, a victim state can avoid the frustration and consequences associated with incorrectly defining ambiguous cyber attacks, such as unlawfully resorting to forceful self-defense.[343] Instead, CNAs might be treated as a basic breach of CIL, utilizing an existent, simple remedial scheme.[344] A victim state that suffers immense disruption by another state's CNA, but otherwise experiences no death, damage, or destruction, similar to Estonia in 2007, could have an immediately clear basis for seeking sanctions or reparations.[345]

C. Greater Investment in Cybersecurity

Although the underlying physical structure of the Internet is expensive to develop as well as maintain, committing to keeping it secure may prove more valuable than the time, energy, and resources needed to pursue international relief from cyber attacks. The global cyberinfrastructure is necessarily located within numerous sovereign states that could, though a drastic measure, disconnect their entire populations from the Internet and prevent foreigners from accessing Internet resources operated from within those states.[346] State sovereignty grants a state the right to control access to its territory, which impliedly includes Internet access within its boundaries.[347] Clearly, "pulling the plug" on the Internet would likely be a last

340. *Id.* at 214–15.
341. *See id.* at 226.
342. *See id.* at 211–12, 227.
343. *See id.* at 227.
344. *See generally* Buchan, *supra* note 329, at 211 (noting that coercive attacks violate the non-intervention principle).
345. *See id.* at 226.
346. Lotrionte, *supra* note 13, at 844–45.
347. *Id.* at 845.

resort against only the most calamitous of cyber attacks.[348] In this case, a state may risk losing exportation and financial transaction capability, public goodwill, or fragmentation of the Internet along territorial boundaries.[349]

Less inimical cybersecurity measures exist for a state to implement, which could lower cyber threat response time and mitigate a cyber attack's damage. Rather than total disconnection, a state may opt to limit Internet access and actively monitor its content for potentially malicious threats.[350] Nevertheless, in states where the Internet is perceived as a public good, such Orwellian surveillance may prove politically controversial and financially detrimental.[351] Or perhaps in an effort to safeguard civilian cyberinfrastructure, state militaries could take major systems and networks offline and onto closed-circuit networks.

The United States has commissioned cybersecurity outfits, such as the United States Cyber Command (USCYBERCOM), to protect sensitive infrastructures from harmful cyber attacks.[352] Established June 23, 2009, USCYBERCOM seeks "to coordinate Pentagon efforts in the emerging battlefield of cyberspace and computer-network security."[353] The mission statement of USCYBERCOM includes goals to "prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace and deny the same to our adversaries."[354] However, Lieutenant General Keith Alexander, director of USCYBERCOM, maintains that "[t]his is not about efforts to militarize cyberspace, . . . [r]ather it's about

348. *Id.* at 846.

349. *See id.* China, as an example, has the ability to disconnect itself from the global Internet and operate an internal domestic form of the Internet. *Id.* The United States has also debated developing an Internet "kill switch." *Id.* (citing Declan McCullagh, *Renewed Push to Give Obama an Internet "Kill Switch"*, CBS NEWS (Jan. 24, 2011), http://www.cbsnews.com/news/renewed-push-to-give-obama-an-internet-kill-switch/).

350. *See* Lotrionte, *supra* note 13, at 846–47. "[S]overeign states . . . have the power and legal authority to establish laws and institutions within their territories to provide for national public goods—such as Internet access—as well as to take action to ensure the safety and welfare of the nation and its citizens." *Id.* (citing JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD, 65–86 (2006)).

351. *See id.* at 850.

352. Leaven & Dodge, *supra* note 11, at 1–2.

353. *Id.* at 2.

354. *Id.*

safeguarding the integrity of our military system."[355] Whether genuine or not, the comments echo a more effective, practical approach to dealing with cyber attacks based upon protecting sensitive networks from CNA effects. Determining the character and extent of defense measures can be a precarious balancing act. Lieutenant General Alexander was also the director of the National Security Agency (NSA) from 2005 to 2014.[356] The NSA came under intense public scrutiny for secret surveillance programs that collected records, metadata, and other information about telephone calls and electronic communications—including communications made by Americans—in the name of national security.[357] Once knowledge leaked of the existence of the surveillance programs, as well as the secret Foreign Intelligence Surveillance Court responsible for issuing the judicial warrants approving the surveillance,[358] Lieutenant General Alexander and the NSA faced accusations of rampant unwarranted government spying.[359]

Though the NSA surveillance represents an example of overly zealous cyberdefense, it contains lessons for modifying cyberdefense policies. In the future, government cyberdefense programs may prove more effective at balancing state security interests and public privacy interests if they are made transparent and narrowly tailored to specific cyber threats and network vulnerabilities, rather than secret, seemingly indiscriminate bulk surveillance.[360] Crafting a more nuanced strategy that targets actual threats will improve overall efficacy and instill trust in the public that the government is not callously discarding notions of online privacy for the sake of strengthening national cybersecurity.

Overall, shifting the focus away from categorizing cyber attacks as warfare may also incentivize innovation. This may lead to more

355. *Id.*

356. David Sanger & Thom Shanker, *N.S.A. Director Firmly Defends Surveillance Efforts*, N.Y. TIMES, Oct. 12, 2013, http://www.nytimes.com/2013/10/13/us/nsa-director-gives-firm-and-broad-defense-of-surveillance-efforts.html?_r=0.

357. *Id.*

358. Todd Lindeman, *The Foreign Intelligence Surveillance Court*, WASH. POST., June 7, 2013, http://www.washingtonpost.com/politics/the-foreign-intelligence-surveillance-court/2013/06/07/4700b382-cfec-11e2-8845-d970ccb04497_graphic.html (noting that an astonishing 99.97 percent of surveillance warrant requests—more than 14,000 in total—have been granted in the court's 23-year history).

359. Sanger & Shanker, *supra* note 356.

360. *See* Hathaway et al., *supra* note 237, at 876.

effective means to mitigate DDoS attacks, viruses, worms, and other common CNAs.[361] A possible strategy might be to abandon a top-down bureaucratic approach to security and move towards a defense system that requires civilian participation.[362] Because the computers and networks that comprise the Internet are interconnected, network vulnerabilities are not confined to high-value targets.[363] Any unsecure computer can become the source of a cyber attack, so cyberdefense should be as all-encompassing as possible.[364] Adopting a cybersecurity strategy that integrates military and civil defense aspects would allow for more complete elimination of vulnerabilities.[365] Multi-faceted cybersecurity and technological innovation would allow states to compete against cyber attackers on a technological front, rather than a warfront. States may accomplish this shift by "[a]ddressing technical vulnerabilities . . . alongside effective public-private partnerships and market-based incentives such as tax breaks for enhancing security."[366] Implementing baseline norms, requiring that hardware and software developers meet best practices, and incentivizing public-private partnerships to share information about cyber threats may diminish the effects of CNAs to the point where international remedy under the *jus ad bellum* and *jus in bello* is rendered unnecessary.[367]

VII. CONCLUSION

The effort of the *Tallinn Manual* and other LOAC experts to dovetail the expanding use of cyber attacks into the war paradigm appears premature. The problems of attribution and categorizing cyber operations under the *jus ad bellum*, as well as the less pervasive issues of distinction, proportionality, and neutrality in the *jus in bello*, suggest the current manifestations of cyber attacks belie their inclusion as warfare. That is not to say that cyber attacks will not at some point be capable of being properly treated as warfare.

---

361. *See id.* at 884 (noting the cultivation of research communities able to take on next-generation cybersecurity challenges is essential).

362. Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control*, 14 MINN. J.L. SCI. & TECH. 137, 256–57 (2013).

363. *Id.* at 256.

364. *Id.*

365. *See* Scott J. Shackelford, *Towards Cyberpeace: Managing Cyber Attacks Through Polycentric Governance*, 62 AM. U.L. REV. 1273, 1364 (2013).

366. *Id.* at 1355.

367. *Id.* at 1364.

However, at this point in history, that reality just has not yet come to fruition. Cyber attacks as currently understood rarely have militaristic ends in mind, but rather take the form of espionage, crime, or political and economic coercion.[368]

Perhaps "cyberwarfare," then, is a misnomer, and alternative frameworks are better suited to deal with the rise in malicious cyber operations. Instead of utilizing a language of "warfare" and "attacks," using terms such as "cyber-interference" or "cyber-intrusions" should be implemented to reduce the inclination to treat all CNAs as acts of war. The new terminology would conjure notions of cybersecurity, criminal prosecution, and international sovereignty, which are all better suited as remedial schemes than the *jus ad bellum*.

The nature of computer and network interference suggests that alternative regimes are more appropriate to resolve cyber disputes with potent, comprehensive, and effective frameworks befitting the characteristics of cyberspace. Though the *Tallinn Manual* makes significant headway in integrating "cyberwarfare" into the *jus ad bellum* and *jus in bello*, categorization and attribution issues suggest excluding cyber operations from their purview.[369] Domestic criminal prosecution, the principle of non-intervention, and expanded domestic cybersecurity provide faster and more reliable responses to cyber attacks than remedies under the international laws of war—without requiring a victim state grasp at elusive categories or invisible targets.

368. *See, e.g.*, Hollis, *supra* note 4, at 1024 (noting the Estonia cyber attacks in 2007 were a response to the Estonian government relocating a Soviet-era war monument).

369. TALLINN MANUAL, *supra* note 20, at 5; *see supra* Parts III, IV.