Vanderbilt Journal of Transnational Law

Volume 50
Issue 1 *January 2017*

Article 5

2017

Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners

Eric Boylan

NOTES

Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners

ABSTRACT

This Note examines the applicability of the law of armed conflict, and particularly the concept of proportionality, to cyber attacks. After exploring deviations in terminology that may lead to confusion in the field, it considers the difficulties associated with applying an area of law first implemented in the post-World War II era to technologies that have only become vitally important in recent years. Delving into some of the facets of cyber technology that make it unique as a potential battleground, this Note examines why those qualities make the law of proportionality particularly difficult to apply. Acknowledging that the law of armed conflict, although perhaps inapt, is nonetheless compulsory, this Note ends with several suggestions that may assist military commanders in conducting cyber operations in a way that comports with the law as it exists today.

TABLE OF CONTENTS

I. INTRODUCTION 218
II. BACKGROUND: CYBER ATTACKS AND PROPORTIONALITY 221
A. *Defining Cyber Attack* 222
B. *Defining Proportionality* 227
III. ANALYSIS 229
A. *The Applicability of Proportionality and the Law of Armed Conflict to Cyber Warfare* 229
B. *Difficulties in the Application of Proportionality to Cyber Attacks* 230
1. Dual-Use Systems 231
a. Increased Impact on Civilian Infrastructure 232
b. Difficulties in Discerning Civilian from Military 233
2. Knock-on Effects 234
IV. SOLUTIONS FOR MILITARY PRACTITIONERS 237
A. *Conduct a Thorough Analysis Before the Attack* 238

B. *Retain a Specialist* 239
C. *Conduct the Attack in a Way That Is Not an "Attack"* 241
V. CONCLUSION: A SOLUTION THROUGH INTERNATIONAL AGREEMENT 242

I. INTRODUCTION

In early 2007, the Baltic nation of Estonia was well on the way to earning its recently acquired nickname, "eStonia": the country had used computer networks to automate and integrate nearly every aspect of its governance and society.[1] Estonian citizens banked, voted in parliamentary elections, and even paid for parking using interconnected computer systems.[2] The internet phone company Skype headquartered there.[3] The nation was a veritable utopia of the burgeoning internet culture and a "window into the future."[4]

All of that changed on April 27, 2007, when the nation suffered what was then the most widespread cyber attack in history, and possibly the first instance of international cyber war.[5] In only a few hours, the nation's media websites, banking sites, and government computers all suffered black outs.[6] Attackers targeted all of Estonia's major commercial banks, telecoms, media outlets, and some essential servers.[7] Using Distributed Denial-of-Service (DDos) attacks, the assaults lasted twenty-two days and effectively crippled the nation's electronic infrastructure.[8] By flooding the Estonian computer systems with an enormous number of requests, the attackers were able to effectively overload the systems and thereby deny service to legitimate users.[9] Nearly every Estonian citizen felt the impact, and the populace

1. *See* 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) ("By 2007, Estonia had instituted an e-government in which ninety percent of all bank services, and even parliamentary elections, were carried out via the Internet.").

2. *See id.*

3. *Id.* at 194.

4. *Id.*

5. *See id.* ("Never before had an entire country been targeted on almost every digital front all at once.").

6. *See id.* at n.10 ("All major commercial banks, telecoms, media outlets, and name servers--the phone books of the Internet--felt the impact, and this affected the majority of the Estonian population.").

7. *Id.*

8. *See* Ira E. Hoffman, *International Cooperation in Combating Cyberthreats and U.S. Law*, 47 MD. B. J. 36, 38 (2014) ("[I]n April 2007, the first series of sustained Distributed Denial-of-Service cyberattacks, lasting 22 days, were launched.").

9. *See id.* ("The attacks. . . flooded computer, servers, routers and websites supporting government ministries, political parties, banks, internet service providers ("ISPs") and telecommunications companies, and blocked legitimate users.").

reacted with hostility[10] Rioting and social upheaval followed. The unrest resulted in one death and injuries to 150 people.[11]

Some believe the Russian government was responsible for the attack, although Estonia's neighbor to the east has never accepted responsibility for the events, and the allegations have not been proven.[12] Given the state of political tension that existed between the two nations preceding the attacks—Russian officials bristled at the Estonian government's displacement of a Soviet-era war statue, among other perceived transgressions—and considering the difficulty in identifying individuals over computer networks, this theory remains a possibility.[13] Others have firmly held that no link to the Russian government exists and that "numerous, albeit unaffiliated, hackers" perpetrated the attacks.[14]

It was the first major cyber attack aimed against a state, and possibly the first instance of international cyber war, if Russia was in fact to blame. The attack alerted the world to what kinds of damage and destruction would be possible without an enemy force ever setting foot on a rival nation's soil.[15] Perhaps most surprisingly to those in elements of the international security community, Estonia's attackers affected all of this chaos solely through computer networks.[16] The attack caused reverberations throughout the international community and provided the impetus for numerous changes in policy and practice for many international entities.[17] The North Atlantic Treaty Organization (NATO), for instance, established a Cooperative Cyber Defence Centre of Excellence and headquartered it in Tallinn, the capitol of Estonia.[18]

---

10. *See* Shackelford, *supra* note 1, at 194 ("In a matter of days the cyber attacks brought down most critical websites, causing widespread social unrest and rioting, which left 150 people injured and one Russian national dead.").

11. *Id.*

12. *See id.* ("At the time, Russia was suspected of the attacks.").

13. *See id.* at 205 ("The removal of the monument infuriated even Russians outside Estonia.").

14. Hoffman, *supra* note 8, at 38.

15. *See* Shackelford, *supra* note 1, at 194 ("Regardless of who was actually to blame, this was the first large-scale incident of a cyber assault on a state. It was but a taste of what information warfare ("IW") can do to a modern information society.") (citation omitted).

16. *See id.* at 193 ("A computer network was responsible for everything.").

17. *See* Hoffman, *supra* note 8, at 38 ("Still, the realization that cyberattacks could threaten the national security of an entire country was a 'true wake-up call for NATO,' including its leading member, the United States.").

18. Antonia Chayes, *Rethinking Warfare: The Ambiguity of Cyber Attacks*, 6 HARV. NAT'L SEC. J. 474, 511 (2015).

The Estonia example shows the potential power of cyber warfare operations.[19] In an incredibly short amount of time, a hostile force with relatively little technological capability or funding can cripple a nation's infrastructure, impede the effective use of civilian and military systems, and completely alter the state of affairs on an international level.[20] If the world did not know it before, one fact became strikingly clear after the Estonia attacks: cyber attacks can be powerful tools.[21]

This does not mean, however, that cyber operations need always be used to perpetrate chaos. Although the Estonia example shows what deleterious events can unfold when malicious actors implement cyber attacks against a civilian population, cyber operations can provide an equally powerful and legitimate tool when used by nations with righteous motivations. Many nations have begun to develop these tools as parts of their military repertoire.[22] The American military, for example, has started to build a robust program of offensive and defensive cyber capabilities.[23] Those who would see themselves as "the good guys," however, can only be good if they operate within the boundaries of the law. Nations must operate within the requirements the international community has agreed upon to denote the limits of acceptable practice: the law of armed conflict. This Note attempts to provide some insight into the difficulties of applying the law of armed conflict to cyber warfare, and to provide some suggestions to military commanders who wish to engage in cyber operations within the bounds of lawful combat.

Much of the law of cyber warfare today is governed by the application of laws—largely by analogy—that were written before the advent of modern computing technology.[24] The absence of laws

---

19. *See* Shackelford, *supra* note 1, at 195 ("As with nuclear radiation, cyberwar can destroy a modern state without drawing blood.").

20. *Id.* at 194.

21. *See id.* ("Indeed, the attacks were so widespread and the results so grave that Aaviksoo considered invoking Article 5 of the North Atlantic Treaty Organization ("NATO"), which states that an assault on one allied country obligates the alliance to attack the aggressor.").

22. *See* Tod Leavena & Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny*, 12 N.C. J.L. & TECH. ONLINE 1, 1–2 (2012) ("United States Secretary of Defense Robert Gates commissioned the United States Cyber Command ("USCYBERCOM") on June 23, 2009, in order 'to coordinate Pentagon efforts in the emerging battlefield of cyberspace and computer-network security.'").

23. Jim Garamone, *Cybercom Chief Discusses Importance of Cyber Operations*, U.S. DEP'T OF DEFENSE, (April 14, 2015), http://www.defense.gov/News-Article-View/Article/604453 [https://perma.cc/QPP4-ZJXU] (archived Dec. 18, 2016) ("Cyber is an operational domain, and military leaders are going to have to understand its importance and the opportunities and challenges of operating in the domain, Navy Adm. Michael S. Rogers said.").

24. See TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 5 (Michael N. Schmitt ed., 2013) ("There are no treaty provisions that deal directly with 'cyber warfare.' Similarly, because State cyber practice and publicly available expressions of *opinio juris* are sparse, it is sometimes difficult to definitively

specifically written or designed to deal with the nuances of cyber warfare, combined with the prevalent application of other fields that are only tangentially related, leads to a host of issues for practitioners in the realm of cyber warfare.[25] The difficulty in applying laws that were written before the concept of cyber warfare existed is that it may hinder military practitioners who engage, or seek to engage, enemy forces through the use of cyber attacks.[26]

In Part II, this Note provides a background on both cyber warfare as it is conceived today and on the law of proportionality. It discusses first the definition of the term "cyber attack" as it has been suggested by multiple sources, and the differences in those suggestions, along with the difficulties in reconciling them. It then reviews the idea of "proportionality" and its importance in the law of armed conflict.

In Part III, this Note analyzes the application of the proportionality rule to cyber attacks and the difficulties associated with this application. These include difficulties arising from the prevalence of dual-use systems (both because of the increased impact on civilian infrastructure and because of the complications in discerning what is military from what is civilian) and the difficulties presented by the requirement to predict knock-on effects.

In Part IV, this Note offers three suggestions that may assist a military commander who is considering using a cyber attack as a form of military engagement, so that the commander may be in compliance with current international law. First, a thorough analysis should be conducted prior to the attack. Second, a specialist in the realm of computer technology should be retained and consulted for the purposes of advisement. Finally, the cyber attack may be conducted in a way that is not an "attack," and thus not be susceptible to the law of armed conflict.

II. BACKGROUND: CYBER ATTACKS AND PROPORTIONALITY

The international legal community first began to take note of cyber operations in the late 1990s.[27] After the United States Naval

---

conclude that any cyber-security customary international law norm exists.") [hereinafter TALLIN MANUAL].

25. *See* Chayes, *supra* note 18, at 510 ("However, until international agreements alter the law, or the International Court of Justice rules on such issues, many of the novel legal questions that cyber attacks pose will be answered by creative, if contrived, adaptation of historic doctrines.").

26. *See id.* at 506 ("Since ambiguity is likely to continue, definitive allocation of governmental responsibility among civilian and military agencies will remain a question in many situations.").

27. TALLINN MANUAL, *supra* note 24, at 1.

War College held the first major legal conference on the subject in 1999, the world began to see the breadth of cyber operations' impact in the Estonia attack in 2007,[28] attacks against Georgia during its war with Russia in 2008, and the Stuxnet worm in 2010,[29] among other smaller events.[30]

The law of international armed conflict, much older than the cyber operations that it arguably governs, has its roots in the Hague Conventions of 1899 and 1907 and the Geneva Conventions.[31] Specifically, the concept of proportionality dates back to Additional Protocol I, signed in 1977.[32] Although the definitions of both "cyber attack" and "proportionality," may vary in a given context, some discussion of each, as it stands on its own, may be useful before an exploration of their interaction and compatibility, or lack thereof.

A. *Defining Cyber Attack*

The terminology that surrounds cyber warfare remains in a nascent state partly because cyber warfare is a relatively new field.[33] Legal experts, institutions, and military practitioners have offered a number of definitions of various terms to describe technologies that are often in flux. This undeveloped terminology includes one definition central to the practice: what is a cyber attack?

There are several reasons why arriving at a concise terminology should be of importance to the international legal community. First, the legal regime should keep pace with the technological realm it seeks to govern.[34] While there is a possibility that "cyber practice may quickly outdistance agreed understandings as to its governing legal regime," an established set of terms and definitions may allow the law to remain applicable.[35] Further, those individuals in the field who conduct, or seek to conduct cyber operations rely on legal definitions to ensure that their actions remain within the bounds of the law and within accepted international norms.[36] Without a working definition of

---

28. *See supra* Part I.

29. *See infra* subsection III.B.2.

30. TALLINN MANUAL, *supra* note 24, at 1–2.

31. Convention Between the United States and Other Powers Respecting the Laws and Customs of War on Land, Oct., 18, 1907, 36 Stat. 2277; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

32. *Id.*

33. *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 823 (2012) ("Existing definitions of 'cyber-attack' and related terms vary widely.").

34. *See id.* ("The absence of a shared definition has made it difficult for analysts from different countries to develop coordinated policy recommendations and for governments to engage in coordinated action.").

35. TALLINN MANUAL, *supra* note 24, at 3.

36. *See* Hathaway et al., *supra* note 33, at 832 ("[A] distinction is crucial to domestic and international efforts to implement cyber-security, because it more

cyber attack, a commander is unable to know what a cyber attack is, whether his actions constitute a cyber attack, and most importantly, whether his actions are legal.

Two definitions of cyber attack seem to be more fully accepted than others. In 2011, the United States Cyber Command issued the first official military definition: "a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions."[37] Then, in 2013, the Tallinn Manual on the International Law Applicable to Cyber Warfare (the Tallinn Manual), perhaps the definitive contemplation of the international law as it applies to cyber warfare, offered a compelling alternative, defining a cyber attack thusly: "[a] cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[38] Both definitions offer succinct phrasing that attempts to capture broad swaths of substance, but their meanings may not be immediately clear. Because each noun, verb, and adverb carries operative weight, these sentences that may initially seem straightforward are in fact packed with significance. The breadth of these definitions has consequently caused disagreement.

It is important to note that the term "cyber attack" is not limited to those events that may come most quickly to the minds of laypersons. Many Americans, if they were to hear the term "cyber attack," might think first of something like the theft of personal information by back-alley agents, or of the Sony Pictures film studio "hack" as archetypal examples.[39] Although those events may fall within the meaning of the term (they may not, depending on the definition being used), cyber attacks are not limited to small-scale activity, nor are they exclusively the province of "hackers" or rogue criminal agents.[40] Instead, they have thus far quite often been seen to be the actions of established nations engaging in a new kind of warfare on a new type of battlefield.

---

effectively tailors the legal approach to the threat posed and focuses resources on true national security threats.").

37. Memorandum from Gen. James E. Cartwright on Joint Terminology for Cyberspace Operations 5 (Nov. 2011), http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf [https://perma.cc/LZG3-W263] (archived Jan. 6, 2017). *See also* Hathaway et al., *supra* note 33, at 832–37 (discussing additional definitions).

38. TALLINN MANUAL, *supra* note 24, at 106.

39. *See* Andrea Peterson, *The Sony Pictures hack, explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/ [https://perma.cc/3H3S-V3NM] (archived Dec. 18, 2016) (describing the Sony hack).

40. *See* TALLINN MANUAL, *supra* note 24, at 106–10 (defining "cyber attack").

Many commenters and authorities have conceptualized a cyber attack as closely analogous to a military attack.[41] A cyber attack could be one that is conducted by a small state against a larger state, or by a larger state against a smaller one, or it could be an event perpetrated in the context of non-international armed conflict.[42] Further, a cyber attack is not necessarily criminal in nature.[43] The use of a cyber attack can be a legitimate tool employed by militaries of established nations within the rules of armed conflict, if they are conducted in the proper fashion.[44] Just as a firearm or a fighter jet is not inherently criminal, a cyber attack does not carry with it a moral connotation. The rightness or wrongness of a cyber attack depends on a complex network of legal and moral questions that must be addressed and are subject to a great deal of interpretation. Whether a cyber attack is normatively "good" or "bad" depends much less on the nature of the cyber attack itself, and much more on the identity of the actor behind the attack, the motivations that propel his actions, and whether the actor has abided by international norms in conducting the attack. In fact, cyber attacks may present a desirable alternative to more violent actions that would alternately be available to military commanders.[45]

Still, disagreement over the definition of a cyber attack persists.[46] Although the Tallinn Manual and the U.S. Government have offered definitions of the term that seek to be definitive, there remains disagreement about the wording that should be used in order to capture the most important aspects of a cyber attack, without employing a definition that is overly broad.[47] As with any definition, the language chosen creates a category that may be either under- or over-inclusive. To the extent that policy decisions depend on this categorization, the agreement on a definition carries importance.[48]

---

41. *See, e.g.*, Hathaway et al. *supra* note 33, at 823–32 (describing cyber attacks as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption").

42. *See* TALLINN MANUAL, *supra* note 24, at 106–10 (defining "cyber attack").

43. *See id.* at 3 ("One of the challenges States face in the cyber environment is that the scope and manner of international law's applicability to cyber operations . . . has remained unsettled since their advent.").

44. *Id.*

45. *See* Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A. F. L. REV. 121, 158 ("This example demonstrates the non-physical destruction aspect of cyber warfare operations, which in many cases will reduce the expected collateral damage to civilians and civilian property.")

46. For example, Hathaway et al. describe competing definitions of cyber attacks. *See* Hathaway et al., *supra* note 33, at 823. In the first, cyber attacks are defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." *Id.* The second defines the same term as a "deliberate attempt to disable or destroy another country's computer networks." *Id.*

47. *Id.*

48. *See id.* ("The absence of a shared definition has made it difficult for analysts from different countries to develop coordinated policy recommendations and for governments to engage in coordinated action.").

Some commenters have suggested varyingly broad and narrow definitions, with treatments fluctuating depending on the political motives behind the attack, who carries out the attack, and what the attack intends to accomplish. [49] Definitions diverge in their assessments of the political motives behind the attack, and depend on the subjective intent of the actor behind the attack. [50] While some commenters endorse a definition of cyber attacks that encompasses any attempt to disturb a nation's computer infrastructure, others would narrow the definition to exclude cyber crime.[51] In other words, if the purpose of the attack is mere theft or lawlessness, it would not rise to the level of a cyber attack.[52] These commenters would instead reserve the term cyber attack for those attacks that are politically motivated.[53]

Another distinction, based on who carries out the attack, is perhaps the most controversial.[54] Some definitions of a cyber attack would encompass only those attacks instigated by nation states or their direct agents.[55] While this definition, likely grounded in conventional definitions of war that envisioned two nations under distinct banners engaging in symmetric, open warfare, attempts to paint a bright-line rule in defining cyber attacks, it omits the crucial possibility that non-state actors would perpetrate a cyber attack.[56] In the contemporary environment, where the tools necessary to conduct a cyber event are prevalent and readily available to both states and non-state actors, other commenters see a real possibility that non-state actors may be common players in the realm of cyber warfare, and those commenters would broaden the definition to include those attacks perpetrated by non-state actors.[57]

A third distinction would depend on the effects of the action taken.[58] Some commenters reduce the definition of a cyber attack to

---

49. *Id.*

50. *Id.*

51. *See id.* ("These definitions, however, do not distinguish between a cyber-crime, cyber-attack, and cyber-war.").

52. *Id.*

53. *Id.*

54. *See id.* at 824 ("[One definition] limits the definition to attacks perpetrated by nation-states, thereby excluding entirely plausible scenarios in which attacks are carried out by non-state actors.").

55. *Id.*

56. *Id.*

57. *See id.* at 831 ("[C]yber-attacks are a particularly attractive weapon for terrorists and other non-state actors.").

58. *See id.* at 828 ("The objective of a cyber-attack must be to undermine the function of a computer network.").

those actions which "undermine the function" of a computer system.[59] This would include attacks that attempt to disrupt the operating system of a computer or attempt to limit the usefulness of the system by impacting the accuracy of the information the operating system interprets.[60] This definition, however, would leave out many actions that others include in defining a cyber attack, such as cyber espionage or cyber exploitation.[61] Attacks that aim to gain access to secure files, to divulge secret information, or to monitor actions on a computer would not be considered cyber attacks under this definition.[62] Only those actions that clearly aim to disrupt the functioning of a computer system would qualify as cyber attacks.[63]

A definition that does not include the theft of secure information is probably narrower than what is generally accepted in the community today.[64] The U.S. Cyber Command definition includes an attack that "intend(s) to disrupt and/or destroy an adversary's . . . assets." The Tallinn Manual definition includes an attack that is "reasonably expected to cause . . . damage or destruction to objects."[65] Both definitions could reasonably be interpreted to include acts of cyber espionage.[66] Considering the broad range of uses and employments of computer systems in today's society, if the definition is limited in such a way as to exclude these kinds of actions, the cyber attack terminology could lose much of its meaning and viability.[67]

These competing definitions lead to a lack of clarity in the field and increased confusion for practitioners. Further, varying definitions create difficulty in assessing whether a proposed cyber action constitutes an "attack," and whether it is subject to the law of armed conflict.[68] If military practitioners are unsure whether their actions constitute a cyber attack, they may not know whether their actions are subject to the law of armed conflict.[69]

---

59. *Id.* at 826 (recommending the following definition: "A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose").

60. *Id.*

61. *See id.* at 829 ("By contrast, neither cyber-espionage nor cyber-exploitation constitutes a cyber-attack because these concepts do not involve altering computer networks in a way that affects their current or future ability to function.").

62. *Id.*

63. *Id.*

64. *See supra* notes 24–26.

65. *Id.*

66. *Id.*

67. *See* Hathaway et al., *supra* note 33, at 830 ("Although all of these incidents of cyber-espionage compromised the security of a computer network for the purpose of carrying out a military objective, they did not 'undermine the function' of a computer system and thus were not cyber-attacks as defined here.") (internal citation omitted).

68. *See id.* at 822 ("Activities in cyberspace defy many of the traditional categories and principles that govern armed conflict under the law of war.").

69. *Id.*

B. *Defining Proportionality*

Proportionality is one of the four broadly recognized principles that govern the use of force under the law of armed conflict.[70] Along with necessity, distinction, and unnecessary suffering, the rule of proportionality provides a foundational tenet of lawful armed conflict by which military practitioners must abide if they wish to conduct themselves in a permissible manner. [71] Unlike the terminology surrounding cyber warfare and the nebulous nature of the definition of cyber attack, the definition of proportionality is relatively straightforward and well agreed upon.[72]

The rule of proportionality has its roots in Article 51(5)(b) of the Geneva Conventions' Additional Protocol 1 which states that any act is indiscriminate which "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[73] The concept has been summed up thusly: "[t]he costs of the use of lethal force must be outweighed by the value of what the lethal force is meant to accomplish, the military objectives of the use of force." [74] In other words, it is unlawful for a military commander to resort to the use of lethal force unless the foreseeable collateral damage is *proportional* to the military advantage to be gained.

While it is a well-accepted rule of international law that military actions may not target or intentionally cause destruction or damage to civilians or civilian objects, the fact that civilian assets are incidentally harmed during a military attack does not automatically make the attack illegal.[75] Such incidental damage is commonly referred to as "collateral damage." [76] Although collateral damage is usually

---

70. *See* Matthew L. Beran, *The Proportionality Balancing Test Revisited: How Counterinsurgency Changes "Military Advantage,"* ARMY LAW, Aug. 2010, at *1 n.2 ("The four universally-recognized principles governing the use of force in the law of armed conflict are military necessity, distinction (also known as discrimination), proportionality, and unnecessary suffering.").

71. *See id.* ("The principle of proportionality requires the commander to conduct a balancing test to determine if the incidental injury, including deaths to civilians and damage to civilian objects, is excessive in relation to the concrete and direct military advantage expected to be gained.").

72. *See* MICHAEL NEWTON & LARRY MAY, PROPORTIONALITY IN INTERNATIONAL LAW 15 (2014) ("Ours is the 'era of proportionality' in the sense that one encounters proportionality as an integral aspect of legal and moral discourse in virtually every legal system.").

73. Protocol I, *supra* note 31.

74. *See* NEWTON & MAY, *supra* note 72, at 3.

75. TALLINN MANUAL, *supra* note 24, at 159.

76. *See id.* at 159 ("Incidental death or injury to civilians or damage to or destruction of civilian objects, is often termed 'collateral damage.'").

undesirable from a normative standpoint, the fact that an attack results in civilian casualties, or the destruction of civilian property does not make the attack illegal *per se*, it only invokes the rule of proportionality.[77] This rule states that the legality of an attack instead depends on the "relationship between the harm an attacker reasonably expects to incidentally cause to civilians and civilian objects and the military advantage that he or she anticipates as a result of the attack."[78]

An example may offer some clarity. In early 2009, while members of the Afghan military conducted a nine-hour firefight against insurgent forces in Farah, Afghanistan, ground units called the U.S. Air Force and Navy to provide assistance in the form of airstrikes.[79] The second of multiple airstrikes targeted a building occupied by the insurgent forces, dropping two 500-pound bombs and two 2000-pound bombs from U.S. aircrafts.[80] Although neither the ground commander nor the aircrew could confirm the absence or presence of civilians in the buildings, the ground commander ordered the strike. [81] The airstrikes allegedly resulted in 147 deaths, many of them civilian.[82] It was the deadliest case of civilian casualties since the opening of the American occupation in 2001.[83]

A later investigation conducted by U.S. Central Command found that the law of proportionality had been violated. [84] Because the commander who ordered the airstrikes had no knowledge as to whether or not civilians were present inside the buildings, he was unable to conduct the necessary weighing of military advantage against the possibility of civilian loss of life and damage to property.[85] This was an unfortunate and avoidable event illustrative of the necessity and prudence of a proportionality test that should precede a military attack.

Proportionality can be a complex and potentially confusing concept to apply even in the most plainly conventional of scenarios.[86] In a contemporary conflict, however, the confusion is multiplied by the presence of insurgents, guerilla tactics, and non-state actors, all of

77. *Id.*
78. *Id.*
79. Beran, *supra* note 70, at *5.
80. *Id.*
81. *Id.*
82. Carlotta Gall & Taimoor Shah, *Villagers in Afghanistan Describe Chaos of U.S. Strikes*, N.Y. TIMES (May 15, 2009), http://www.nytimes.com/learning/students/pop/articles/15farah.html [https://perma.cc/L7HU-AKYZ] (archived Dec. 19, 2016).
83. *Id.*
84. Beran, *supra* note 70, at *5–6.
85. *Id.* at *6.
86. *See id.* at *4 ("[N]o further guidance, in the form of definitions or examples, is provided to commanders, who are left with only the plain meaning of the words.").

which add variables and unknowable aspects to the equation.[87] Further, the application of an already unwieldy principle such as proportionality to an increasingly cloudy field such as cyber warfare may lead to even more uncertainty.

It is also important to note that the principle of proportionality bars attacks based only on civilian casualties; it does not aim to provide a "fair fight" between combatants.[88] The proportionality rule limits the lawfulness of an attack if the attack would have an unduly impact on a civilian population, and the rule does not bar an attack regardless of the effect that it would have on an enemy force.[89] Even if the proposed attack would cause significant casualties to an enemy force, it would not be barred by a proportionality test so long as the effects on civilians are outweighed.[90]

Further, the harms to be considered in a proportionality review are only those that would cause damage to civilian objects or physical harm to civilian personnel.[91] Not to be included in the equation are irritation, strife, fear, or inconvenience, all of which may conceivably be brought on by a cyber attack.[92] Unless these lesser consequences amount to "damage to civilian objects" they should not have bearing on a proportionality test.[93] There is some gray area, however, where it comes to the reduced functionality of a civilian computer system and whether that effect should be considered in a proportionality review.[94]

III. ANALYSIS

A. *The Applicability of Proportionality and the Law of Armed Conflict to Cyber Warfare*

While it seems to be settled law that an "attack" (in the military sense) would be governed by the law of armed conflict, and thus subject to a proportionality standard, there has been relatively vigorous debate

87. *See generally id.* (arguing that counterinsurgency changes the proportionality calculus).

88. *See* Eric Talbot Jensen, *Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1171 (2003) ("It is not an attempt to ensure a 'fair fight' between combatants.").

89. *See id.* ("In other words, there is no requirement that a combatant limit his force when engaging another combatant.").

90. *Id.*

91. *See* TALLINN MANUAL, *supra* note 24, at 160 ("The rule envisages a situation where a cyber attack on a military objective will result in harm to civilian objects . . . or to civilians.").

92. *See id.* ("Such consequences do not qualify as collateral damage.").

93. *Id.*

94. *See id.* ("[T]he notion of 'damage to civilian objects' might, in certain circumstances, include deprivation of functionality.").

in recent years as to whether or not all hostilities in the realm of cyber warfare, in fact, constitute "attacks."[95] At least one commenter has argued that the term "attack" should be reserved for an action that results in death, damage, destruction, or injury, and therefore, many cyber crimes would not be considered "attacks."[96] If this is in fact the case, no proportionality standard would need to be applied to a cyber attack because, by its own terms, the rule of proportionality is applicable only to "attack[s]."[97] On the other hand, another commenter would apply a broader definition, arguing that any action aimed at civilians amounts to an "attack."[98] In this case, a proportionality analysis would almost certainly be required.[99]

The Tallinn Manual clearly states that the principle of proportionality applies in its full capacity to acts of cyber warfare: "A cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof which would be excessive in relation to the concrete and direct military advantage is prohibited."[100] This seems to be the prevailing view among the community, and even those who would argue for a narrower definition of a cyber attack would likely concede that in some contexts a proportionality analysis would be required.[101] However, because there has been relatively little application of these concepts to actual events, they remain largely hypothetical and these arguments may not become settled until states engage in further cyber activities and flesh out these theoretical positions.

B. *Difficulties in the Application of Proportionality to Cyber Attacks*

The difficulties in applying the law of armed conflict to cyber warfare are potent and numerous. They are brought on by several factors, including the prevalence of "dual use" systems (i.e., those that are used by both military and civilian actors) and the difficulties that may arise in discerning what is civilian from what is military. Additionally, the mere presence of dual-use systems may lead to increased levels of civilian damage. Further, the existence of "knock-

95. *See* Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INT'L L. STUD. 198, 200–01 (2013) (discussing differing viewpoints).

96. *See id.* (citing Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 INT'L REV. RED CROSS 365, 369 (2002)).

97. Protocol 1, *supra*, note 31.

98. *See* Jensen, *supra* note 95 (citing Knut Dörmann, *The Legal Situation of "Unlawful/Unprivileged Combatants,"* 85 INT'L REV. RED CROSS 45, 46, 72–73 (2003); KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS (2004), http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf [https://perma.cc/7WPE-MHJZ] (archived Dec. 19, 2016).

99. *Id.*

100. TALLINN MANUAL, *supra* note 24, at 159.

101. *See e.g.*, Jensen *supra* note 88, at 1174 (discussing the application of proportionality to computer network attacks).

on effects" (those indirect effects that may result from a given action, but are not immediately discernable) and the fact that military commanders must account for them in a proportionality analysis present difficulties.

1. Dual-Use Systems

Dual-use systems are those systems that serve both a military and a civilian purpose. They are especially prevalent in the realm of cyber technology. [102] While militaries often use easily distinguishable facilities when it comes to conventional resources, cyber networks are commonly much more intertwined between civilian and military uses.[103] Although these dual-use systems can certainly be legitimate military targets, they present a number of unique challenges to a commander conducting a proportionality review.[104]

Examples include power plants that supply electricity to both civilian and military users, air traffic control systems that service both civilian and military aircrafts, and communication networks on which both civilian and military users operate.[105] Such systems are relatively common outside of the realm of cyberspace, and even more common within it.[106] The Global Positioning System (GPS) is a system that was created to serve military purposes, and originally served only military users, although recently it has been developed and integrated into civilian devices to the point that the technology has become nearly ubiquitous.[107]

It is important to recognize that a dual-use system can certainly be a viable military target. [108] While the civilian capability may influence and alter the proportionality analysis, that is not to say that a civilian use precludes a target's susceptibility to lawful attack.[109] It has been generally recognized that two requirements must be met before a dual use system may be a legitimate military target: first, the target must make an effective contribution to the enemy's military

---

102. HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 193 (2012).

103. *See id.* at 194 ("Some systems initially designed for military use have become so integrated into civilian society that any interference or disruption caused by computer network attacks would have serious effects on civilians.").

104. *Id.*

105. *Id.*

106. *Id.* at 194.

107. *Id.*

108. *See id.* at 193 ("[F]rom the standpoint of international humanitarian law, once an object meets the definition of a military objective it becomes liable to attack.").

109. *See id.* at 193–94 ("The discussion of any civilian aspect or purpose of that object or piece of technology should therefore be considered as part of the proportionality equation . . . .").

action, and second, the target's destruction must provide a definite military advantage to the attacker.[110] Further, an attack against a dual-use system must pass a proportionality test.[111] However, once those prerequisites have been met, a dual-use system may be the lawful target of an attack, unlike a system that is purely civilian in nature.

One often-recounted example of the lawful targeting of a dual-use system took place during the 1991 Persian Gulf War.[112] U.S. intelligence discovered that Saddam Hussein's forces employed infrastructure that provided electricity to both the command and control nodes of the hostile Iraqi forces *and* to the civilian population.[113] This infrastructure constituted a dual-use system because it served both a military and a civilian purpose, providing service to both military and civilian users.[114] U.S. forces chose to destroy the target, which was a lawful action.[115] Because the military advantage to be gained by destroying the infrastructure outweighed the harm to be caused to the civilian populace, the targeting of the infrastructure passed a proportionality review and was permissible within the law of armed conflict.[116]

While dual use systems may be legitimate military targets, two distinct problems arise in the contemplation of proportionality and cyber attacks: the likelihood that impacts on civilian infrastructure will be increased and the difficulty presented in discerning what parts of dual-use systems are civilian from what parts are military.

a. Increased Impact on Civilian Infrastructure

Because of the prevalence of dual-use systems in the realm of cyber technology, and due to the overlap between civilian and military networks, cyber attacks are likely to have an increased impact on civilian infrastructure. An increased impact on civilian infrastructure may make a proportionality test more difficult to pass, since the potential damage to civilians could be greater. Although a proportionality analysis may be more difficult to conduct, that does not mean that a target is illegitimate. However, if the impact on civilian infrastructure is increased to the point that it outweighs the military

110. *See* Schaap, *supra* note 45, at 156–57 (2009) ("First, the target must make an effective contribution to the enemy's military action. Second, its destruction must provide a definite military advantage to the attacker.").

111. *See id.* ("However, just as with a non dual-use object, a proportionality test must be performed to ensure the collateral damage to civilians or civilian objects is not excessive in relation to the concrete and direct military advantage anticipated.").

112. *Id.* at 163.

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

advantage to be gained, this would constitute an attack violative of the law of armed conflict.

One commenter suggests that those who would target civilian infrastructure may find dual-use targets more attractive because attackers may benefit doubly from the resulting damage.[117] Attackers would incur benefits from both the damage done to military objectives, and also from damage done to the civilian population. [118] If the resulting damage against a civilian population is intentional, however, the attack probably violates the principle of distinction, whereby an attacker must distinguish, and not target, civilian entities.[119] Article 52(2) of Additional Protocol I states in part that, "[a]ttacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action . . . . "[120] Therefore, military commanders who do not want to violate this convention must go to great lengths to ensure that the pending attack does not violate the rule of proportionality.

b. Difficulties in Discerning Civilian from Military

Additionally, difficulties are likely to arise in discerning civilian from military infrastructure because of the prevalence of dual-use systems. This leads to a two-part problem. First, military commanders may be unable to discern the difference in the infrastructure itself. Second, they may be unable to tell what impact their attacks will have on the civilian infrastructure so as to make a complete proportionality calculation.

Discerning military from civilian infrastructure is critical to a thorough proportionality review for obvious reasons: a military commander about to engage in an attack must know the identity and capabilities of the system he is considering attacking if he is to reasonably predict the effects of his attack. This analysis is increasingly difficult in an environment where civilian and military personnel commonly use computer systems simultaneously.[121]

---

117. *See* DINNISS, *supra*, note 102, at 195 (hypothesizing an attacker who may be thusly motivated).

118. *See id.* ("The attacker not only benefits from the destruction . . . of the target's military value, but also from cumulative effects on the civilian population.").

119. *See* TALLINN MANUAL, *supra* note 24, at 110–11 (defining distinction thusly: "'the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy").

120. Protocol I, *supra* note 31.

121. *See* DINNISS, *supra*, note 102 at 194 ("Most computer technology, hardware and software, has become dual-use.").

One example might be a satellite system that is being used for GPS guidance.[122] If it is known that a satellite system is being used for both civilian and military purposes, a military commander may be unable to discern to what degree it is being used for each. Given the hazy and fast-paced nature of military operations, a commander may only have intelligence to inform him that the satellite is providing guidance to a military system, and may not know what other functions it performs. This would make it difficult to conduct a proportionality analysis. If the commander does not know what civilian use the system has, it would be difficult or impossible to estimate the effects of an attack.[123] In contrast with conventional systems, which a commander may easily understand at first glance, cyber systems are often grasped less easily.

This brings about an additional problem, one that has largely been hypothetical in the context of cyber warfare thus far, but may present a real dilemma in the future.[124] When the International Group of Experts gathered in Estonia to construct the Tallinn Manual, they disagreed as to what an attacker must do if he suspects, but is unsure, that civilian damage might occur.[125] As may be evident, this has particular relevance in the realm of cyber warfare, where predicting damage can be particularly difficult.[126] A minority of those experts believed that a lower probability of damage would allow an attacker to go forward with an attack that would result in less military advantage.[127] The majority disagreed, saying that "once collateral damage is expected, it must be calculated into the proportionality analysis as such; it is not appropriate to consider the degree of certainty as to possible collateral damage."[128]

2. Knock-on Effects

Knock-on effects, also called second- and third-order effects, are the indirect consequences that flow from the direct results of a given

122. *See id.* at 194 ("[T]he Global Positioning System (GPS) is a US military system which has become integrated into many civilian applications from aircraft traffic control to cell phones and laptops and even the internet itself.").

123. *See id.* ("Disruption of the service through jamming or blocking or spoofing the signal via computer network attack would cause massive disruption and potentially endanger civilian lives.").

124. *See* TALLINN MANUAL, *supra* note 24, at 163 ("There was a discussion among the International Group of Experts over whether and to what extent uncertainty as to collateral damage affects application of the rule.").

125. *Id.*

126. *See id.* ("The issue is of particular relevance in the context of cyber attacks in that it is sometimes very difficult to reliably determine likely collateral damage in advance.").

127. *Id.*

128. *Id.*

action.[129] Second- and third-order consequences are especially difficult to discern in a cyber context. Much has been made of knock-on effects in the area of proportionality review, but it seems to be settled law that when commanders conduct a proportionality analysis they must account not only for the direct effects to be caused by the attack, but also for these follow-on effects.[130]

For example, a military commander who considers targeting a rail depot will certainly consider the primary effects of his proposed attack, perhaps that the rail depot will no longer be able to transport military goods to the local militia.[131] But if the rail depot also services the surrounding civilian community, targeting the rail depot may have knock-on effects as well.[132] Trains will no longer be able to transport goods required to keep the local economy afloat, and they will no longer be able to transport civilian personnel to the surrounding area.[133] This may affect the loyalties of the local populace, turning the tide of public opinion in the area against the commander, and may make the commander's mission more difficult to accomplish than if he had never targeted the rail depot in the first place. These unintended consequences are known as knock-on effects. Although they may be difficult to assess, a commander must attempt to quantify these effects in a proportionality analysis before conducting an attack.[134] In the context of cyber operations, however, this may be increasingly difficult for several reasons.

First, the interconnectedness of modern cyber systems leads to an increased difficulty in estimating the effects of an attack. Today more than ever, computer systems are linked to each other directly and indirectly across vast systems of networking.[135] Because computer systems are so interconnected, information can, and does, travel between networks at distances that make it difficult to predict the ripple effects of an action with any precision.[136] This problem is

129. *See* Jensen, *supra* note 88, at 1176.

130. *See generally id.* (discussing the legal standard for review of computer network attacks as opposed to kinetic attacks).

131. *See id.* at 1157 (describing the rail depot example).

132. *See id.* at 1177–78 (describing possible knock on effects of the rail depot attack).

133. *Id.*

134. *See id.* at 1172 ("[The commander] must determine if the expected incidental injury or damage to civilian objects is excessive to the military advantage of destroying that rail hub and military equipment.").

135. *See* MARK GRAHAM & STEFANO DE SABATA, INTERNET TUBE: AN ABSTRACTION OF THE GLOBAL SUBMARINE FIBRE-OPTIC NETWORK (2014), http://geography.oii.ox.ac.uk/?page=internet-tube [https://perma.cc/28KA-9U8Y] (archived Dec. 18, 2016) ("Today, an entire network of fibre-optic cables connects almost every corner of the world, enabling the hyper-connected world that many of us take for granted.").

136. *Id.*

furthered by the international application of networking and the fact that computer systems often traverse one or more nations with one or more languages.[137] The multi-national, multi-linguistic aspects of modern computing make understanding the reach of a given system increasingly difficult. Today's computing systems' employment of broad networks, across vast areas of time and space, makes it difficult to estimate the ways in which a cyber attack may affect those outside the initial sphere of influence.[138]

Second, the speed at which computer systems operate presents an equally worrisome obstacle to the adequate estimation of second- and third-order effects. Computers today operate at speeds that might have been inconceivable only a short time ago.[139] Where central processing units once occupied only two-thousand transistors, they have increased in recent years to house nearly two billion.[140] Undoubtedly, this increased ability to process information at great speeds has led to huge advancements in the availability and applications of electronic devices in modern life.[141] The fact that computers operate faster now than ever before has also made the predictability of a potential cyber attack's influence more unknowable. Information travels faster and further than it ever has, and ripple effects can be very difficult to predict.

The inability to predict end outcomes was evident in the Stuxnet case.[142] The Stuxnet malware virus was reportedly released by a joint U.S.-Israeli operation in an attempt to infect and destroy Iranian nuclear centrifuges.[143] After gaining access to the Iranian networks, the malware performed two functions.[144] It forced the centrifuges to speed up and slow down at such a rate as to cause them to destroy themselves, and the virus caused the computer systems to send signals to operators that the centrifuges were operating normally.[145] While the

---

137. *See* Daniel Sorid, *Writing the Web's Future in Numerous Languages*, N.Y. TIMES (Dec. 30, 2008), http://www.nytimes.com/2008/12/31/technology/internet/31hindi.html?partner=rss&emc=rss&_r=0 [https://perma.cc/7WHU-95ZW] (archived Dec. 19, 2016) ("The next chapter of the World Wide Web will not be written in English alone . . . Already, more than half of the search queries on Google come from outside the United States.").

138. *Id.*

139. *See* Dean Takahashi, *Forty Years of Moore's Law*, SEATTLE TIMES (Apr. 18, 2005), http://www.seattletimes.com/business/forty-years-of-moores-law/ [https://perma.cc/F6GB-LMBL] (archived Dec. 16, 2018) ("The result is a world unimaginable four decades ago: Computers once the size of refrigerators fit in the palm of your hand.").

140. *Id.*

141. *See id.* ("It is why technology has infiltrated the lives of everyday people, from iPods and Xboxes to camera pills that wirelessly transmit photos of patients' digestive tracts.").

142. *See generally* Jensen, *supra* note 95 (discussing the implications and potential illegality of the Stuxnet attacks).

143. *Id.* at 203.

144. Jeremy Richmond, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842, 844 (2012).

145. *Id.*

virus was successful in its presumed goal (causing damage and destruction to the centrifuges), the virus allegedly was leaked to computers outside the intended network.[146] Although no other damage outside of the centrifuges was reported, the leak led to public knowledge of the previously secret virus.[147]

The Stuxnet case is illustrative of the difficulties practitioners may encounter in estimating knock-on effects posed by the interconnectedness of cyber systems, even those posed to well-funded, high-level operations. If a highly-sophisticated attack, purportedly perpetrated secretly by the governments of two of the most technologically advanced nations in the world, can fall prey to an inability to foresee knock-on effects, then it is evident that the obstacle is a real one that could affect any potential cyber operation.

IV. SOLUTIONS FOR MILITARY PRACTITIONERS

Cyber operations may provide military commanders a preferable alternative to conventional attacks for several reasons.[148] First, and most importantly, they may provide the same military advantage without posing a risk to the lives of friendly forces, enemy forces, or civilians.[149] Second, they may be able to accomplish the same goals as a conventional strike at a far smaller monetary cost.[150] Without the expenditure of ammunition, fossil fuels, or man-hours normally associated with a conventional attack, a cyber attack can reduce the expenditures of money and resources. There is also a possibility that cyber attacks can achieve military goals with lessened physical destruction and socio-political implications, but these benefits are less certain.[151]

While some military commanders view cyber operations as a less dangerous and more cost-effective tool, the operations must still be carried out within the structure of the international law of armed conflict.[152] Following are several recommendations to commanders who wish to utilize these potentially beneficial tools within that legal framework.

---

146. Jensen, *supra* note 95, at 207–08.

147. *Id.*

148. *See* Schaap, *supra* note 45, at 158 ("Some obvious benefits include less physical destruction, less cost than other types of traditional warfare, and the ability to still achieve the same results with less risk to military personnel.").

149. *Id.*

150. *Id.*

151. *See id.* ("This example demonstrates the non-physical destruction aspect of cyber warfare operations, which in many cases will reduce the expected collateral damage to civilians and civilian property.").

152. *See* TALLINN MANUAL, *supra* note 24, at 13 ("[T]he Experts unanimously concluded that general principles of international law applied to cyberspace.").

A. *Conduct a Thorough Analysis Before the Attack*

For those versed in the law of armed conflict, it may be commonly understood that commanders must conduct a proportionality review before commencing an attack. However, in the realm of cyber operations, this may be easier said than done.

Leading up to a cyber attack, it may be appealing to a commander to forgo a thorough proportionality review in favor of a more cursory, expedited undertaking. After all, in the context of cyber operations, a military commander may view a cyber attack as less likely to result in damage to civilians or civilian objects than a conventional, kinetic attack.[153] If the commander views these negative results as less probable, he may view the accompanying proportionality review as less essential than it would be if he were to carry out a kinetic attack. This is likely a mistake. Given the unpredictable nature of cyber operations, even the most well-planned cyber attack may have far-reaching consequences. In the Stuxnet case, for example, the virus was inadvertently released onto public computers after it had affected targeted Iranian centrifuges.[154] Although this result was likely unforeseen by the attackers, a thorough review may have prevented the outcome. Because of this kind of unpredictability, it is essential to conduct a thorough proportionality review prior to a cyber attack.

Article 57 of Additional Protocol I is titled "Precautions in the Attack" and states that "[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[155] In this context, the term "military operations" is even broader than the term "attack," and poses a requirement on militaries to exert caution as to civilians and civilian objects, even when not in the throes of battle.[156] This, known as the "constant care standard," shows the high level of care that military commanders must be held to at all times during military operations.[157]

In the cyber warfare context, the constant care standard likely requires commanders to maintain situational awareness at all times and to remain vigilant as to the effects of their actions, especially as they may potentially affect civilians.[158] This may be difficult in a cyber context, however, where any action taken on a computer network can

153. *See supra* note 148 and accompanying text.

154. *See supra* notes 142–47 and accompanying text.

155. Protocol I, *supra* note 31.

156. *See* Jensen, *supra* note 95, at 202 ("The term 'military operations' is obviously meant to be much broader than the term 'attack' and imposes a general legal requirement on militaries even when not attacking.").

157. *See id.* ("[I]t seems clear that exercising constant care would at least mean that a commander cannot ignore effects on civilian population.").

158. *See id.* ("When employing a cyber tool or conducting cyber operations, the commander would need to maintain oversight of the tool and be ready to adjust operations if the tool or operation began to have effects that the commander determined would have an illegal impact on civilians.").

affect civilians and "virtually every cyber operation will traverse, affect, employ or damage civilian cyber infrastructure of some kind."[159] If this high level of vigilance is required of commanders when they are not conducting attacks *per se*, and merely conducting cyber operations that fall short of attacks, the level of caution should be appropriately increased when a commander orders a cyber attack. [160] A proportionality review should be near the top of a commander's list of actions and a crucial step in the process under these circumstances.

Regardless of the difficulties that may be presented by the complexity of today's networks, the unpredictability of an attack on civilian infrastructure or the potential of dual-use systems, military commanders are required to perform a proportionality analysis before engaging in an attack. As discussed, if a commander's planned action amounts to an attack, it unquestionably should be subject to a proportionality review, but this may be difficult for several reasons. Modern computer networks operate across vast distances and speeds nearly incomprehensible to the human mind. Nonetheless, commanders must take the necessary pains to assess the likely outcomes of the actions they take.

B. *Retain a Specialist*

A question remains as to whether military commanders are positively required to retain a network specialist to assist in proportionality reviews related to cyber operations.[161] Especially in the midst of an ongoing kinetic conflict, it may be difficult to have a computer specialist on hand in the field who is capable of providing reliable advice to a military commander concerning the potential effects of a proposed cyber attack.[162]

Ordinarily, military commanders are under obligations to both obtain the best possible intelligence and to act in good faith once that intelligence has been gathered.[163] In the context of traditional, kinetic attacks, mainstream military officers can often achieve these objectives.[164] Military staff officers are often trained and proficient in

---

159. *Id.* at 203.

160. *Id.* at 202–03.

161. *See* DINNISS, *supra* note 102, at 206 ("Michael Schmitt has also queried the extent to which specialized computer expertise must be available during the targeting process to assess possible collateral damage and incidental injury.").

162. *Id.*

163. *See id.* at 207 ("[Commanders] are also under an obligation to obtain the best possible intelligence . . . .").

164. *See id.* at 206 ("[I]n traditional kinetic attacks, properly trained mainstream military officers can usually conduct reliable collateral damage estimates based on their knowledge of the weapons system involved and its effects . . . .").

the use of traditional weapon systems such that they should be able to provide a commanding officer with collateral damage estimates in support of a proportionality analysis, when an attack is the traditional, kinetic type.[165] However, if a commander wishes to employ a cyber attack, the training and ability to conduct such an estimate may lie beyond the abilities of a traditional staff officer.[166]

Commanders have several options in deciding how to handle the role of the computer specialist at the staff officer level. One possibility would be for the commander to look outside of the uniformed forces to find a capable specialist. Another would be that the military trains uniformed officers to accomplish these tasks. Lastly, a commander may wish to go it alone, and do the best he or she can without the aid of a computer specialist.

Only the last of those options seems untenable. Because military leaders are responsible for obtaining intelligence before taking action, they probably have a responsibility to employ a specialist to aid a proportionality review, whether that specialist is drawn from civilian or military personnel. It seems likely that a military capable of conducting a cyber attack with significant impacts on civilian infrastructure would have the resources at its disposal to train and equip a specialist capable of assisting in a proportionality review, whether that individual is a uniformed officer or not. However, this may be expensive.

Employing a specialist, a person that is monetarily expensive to train and sustain, is a costly proposition. One of the major advantages that the use of cyber attacks provides to commanders, as an alternative to kinetic attacks, is their ability to effect the same outcomes as a kinetic attack without expending the same level of resources.[167] If employing a specialist is required before a commander may conduct a proportionality test, this cost may offset the monetary advantage of a cyber attack.

Further, even if a commander never decides that a cyber attack is necessary or desirable, the commander must still retain the specialist. This may lead to the expenditure of resources on the training and equipping of personnel who might never become useful. Although, if the other advantages of a cyber attack are also weighed into the equation (the absence of lost lives and the lack of destruction of property), the monetary expense of employing a specialist seems less consequential. If this is the case, and employing a specialist assists the commander in achieving those two goals, then the inconvenience and monetary costs of doing so is likely outweighed.

---

165. *Id.*

166. *See id.* ("[I]n computer network attacks highly specialised expertise would be required.").

167. *See supra* note 148 and accompanying text.

C. *Conduct the Attack in a Way That Is Not an "Attack"*

If the law of armed conflict does not apply where actions do not constitute an "attack," then commanders may be able to take actions that are not subject to proportionality review. [168] At least one commenter has taken a strong stance that this is in fact the case, arguing that "very few activities in cyber warfare will actually amount to an attack and will therefore not be governed by the principles of attack, such as proportionality."[169] Further, military commanders take actions on a regular basis that do not amount to attacks. Intelligence gathering operations and reconnaissance operations represent actions which can affect the battlefield, but do not constitute attacks against an enemy force. Cyber actions of this type are probably not attacks and are probably not subject to proportionality reviews. If commanders can achieve the goals as dictated by the situation through actions that are not attacks, then they may circumvent the requirement to conduct a proportionality review.

However, this advice may best be left until a fuller definition of cyber attack is fleshed out. As has been discussed, the current definition of cyber attack leaves much to be desired in terms of clarity, and what one legal practitioner may consider an "attack," another may not.[170] Because military commanders will be judged with the benefit and burden of hindsight, relying on a definition that has been accepted by only part of the legal community may be unwise. This is especially true because a commander's actions may have broad consequences if he takes what is later considered to be a military attack without having engaged in a proportionality review, possibly leading to his own prosecution.

Another possibility is to attack a military system *through* a civilian system.[171] The Stuxnet virus utilized this technique.[172] In that instance, the virus was first released into five gateway targets before it penetrated Iranian centrifuges.[173] Arguably, like a tank passing through a village before targeting a military objective, no proportionality review need take place as to the civilian portal, as no

168. *See* Jensen, *supra* note 95, at 199.
169. *Id.*
170. *See supra* Section II.A.
171. *See* DINNISS, *supra* note 102, at 201 ("This raises particular issues with attacks in which civilian networks or systems are targeted and used as gateways to get inside networks which are legitimate military objectives.")
172. *Id.* at n.95.
173. *Id.*

attack has yet taken place.[174] This of course requires that the software not release its payload until it reaches the legitimate military target.[175] Some commenters would argue, however, that this technique constitutes targeting the civilian portal, and thus this technique should be considered illegitimate.[176]

Finally, a commander often has the option to limit his attack to only affect the military portions of a system or network.[177] If, for instance, a commander has difficulty in mapping a computer system and cannot determine what portion of the system is civilian and what portion is military, or if he has had difficulty predicting the knock-on effects that will result from the attack he is considering, then the commander may wish to limit his attack to some smaller, more knowable portion of the system. In this way, the commander may prevent second- and third-order effects from reaching civilian infrastructure, and prevent an indiscriminate, illegitimate attack.

V. CONCLUSION: A SOLUTION THROUGH INTERNATIONAL AGREEMENT

As many have noted, the law of cyber warfare is behind the reality of the times, and in order to catch up, an international agreement may be necessary.[178] As compared to other facets of international law, there is little agreement among states on the subject of cyber security, and even less as the law pertains to cyber attacks and cyber warfare.[179] Because many of the questions regarding the law of cyber war are answered only by analogy to existing laws, problems arise when analogies are stretched too thinly.[180] The ideal solution would be international agreement on the subject, and some forays have been made.[181]

NATO has recently developed the Cyber Defense Management Board and the NATO Cooperative Cyber Defense Center of Excellence

---

174. *See id.* at 201 ("A civilian network may be infected with malware, however it may not execute its payload until it reaches a network with the targeted network configuration.").

175. *See id.* ("The civilian system is essentially unharmed . . . but it passes on the malware to the targeted system where the payload executes.").

176. *See id.* ("A query remains whether this is sufficient to hold that the state is directing its military operations against the civilian target, contrary to Article 48; or whether the operation is directed against its final, legitimate military objective . . . .").

177. *See* Jensen, *supra* note 95, at 210 ("[H]e should limit the attack to only those parts of the system for which he does have sufficient information to verify their status as lawful targets.").

178. See Chayes, *supra* note 18, at 500 ("[C]reative attempts have been made to bring cyber attacks under the umbrella of existing international and domestic legal doctrines.").

179. *See id.* at 510 ("Efforts to institutionalize international cooperation are rudimentary.").

180. *See id.* at 500 ("[A]nalogies, however creative and persuasive, are not infinitely elastic.").

181. *See id.* at 510–19 (summarizing attempts at cooperation).

in Tallinn.[182] The Cyber Defense Center headed the establishment of the Tallinn Manual on the International Law Applicable to Cyber Warfare, the preeminent treatise on the subject.[183] These foundations have helped NATO establish an institutional structure to deal with cyber attacks, and have led to international cooperation in the area.[184]

The European Union has adopted a Union-wide directive to improve cooperation on cyber security.[185] While EU nations have previously employed security measures on a largely voluntary basis, the new directive requires nations to meet a minimum threshold of cyber defenses and encourages them to cooperate and communicate with other nations in the European Union on the matter.[186] Canada has launched *Canada's Cyber Security Strategy*, the United Kingdom has developed *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digitized World*, and Russia has recently published its *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space*.[187] These efforts and others are necessary to ensure that cyber attacks are limited to those instances where the proponents have conformed to the law of armed conflict.

While the advent of computer systems and cyber attacks has brought some confusion to the landscape of the law of armed conflict, these likely are growing pains that can and should be worked through over time. As has been shown, there is a lack of clarity not only in the definition of the term "cyber attack," but in the applicability of the law of armed conflict to actions that might fall under that banner. Further, even if it is granted that the proportionality rule should be applied to a given cyber operation, doing so may be exponentially more difficult than it would be to apply the rule in a traditional kinetic context, either because of knock-on effects, dual-use systems, or any of the other unique attributes of computer networks. Several solutions present themselves to commanders. They may wish to conduct a thorough analysis before the attack, to retain a specialist, or to alter the nature of their operation.

None of this is to suggest that the law of armed conflict, *writ large*, is incompatible with cyber operations, or to argue that the

182. *Id.* at 511.

183. *See* TALLINN MANUAL, *supra* note 24, at 1 ("In 2009 the NATO Cooperative Cyber Defense Center of Excellence . . . invited an independent 'International Group of Experts' to produce a manual on the law governing cyber warfare.").

184. *See* Chayes, *supra* note 18, at 511 ("There are conferences and membership training to defend against cyber attack, which has included NATO training the Jordanian army to defend against ISIS cyber attacks.").

185. *Id.* at 511–12.

186. *Id.*

187. TALLINN MANUAL, *supra* note 24, at 2.

fundamentals of the law require redrafting to meet the needs of a newly interconnected world. In fact, just the opposite is likely true. The law of armed conflict's principles operate as a backstop and a failsafe in times of drastic uncertainty. The principles that undergird this body of law, while difficult in application to a new and changing area of technology, function to let those who participate in the conduct of armed conflict know that the way that they do so is in a manner that is legitimate and justified, and within the bounds of the law.

On the other hand, the Estonia attack provides a striking example of what chaos can be sewn when world players go unchecked and use powerful cyber warfare techniques against vulnerable civilian populations. The law of armed conflict, and the continued adherence to it in the context of cyber operations provides a way to prevent such abuses, if these laws can be clearly applied.

Eric Boylan[*]

---

* J.D. Candidate, 2017, Vanderbilt Law School; US Army, 2008–2014; B.A., 2008, University of California, Berkeley. For AAS.

VANDERBILT JOURNAL
of TRANSNATIONAL LAW

The *Vanderbilt Journal of Transnational Law* (*Journal*) (USPS 128-610) is published five times a year (Jan., Mar., May, Oct., Nov.) as part of the International Legal Studies Program by the Vanderbilt University Law School, 131 21st Avenue South, Room 047, Nashville, TN 37203. The *Journal* examines legal events and trends that transcend national boundaries. Since its foundation in 1967, the *Journal* has published numerous articles by eminent legal scholars in the fields of public and private international law, admiralty law, comparative law, and domestic law of transnational significance. Designed to serve the interests of both the practitioner and the theoretician, the *Journal* is distributed worldwide.

The preferred and most efficient means of submission is through ExpressO at http://law.bepress.com/expresso/. However, other modes of submission are accepted in print or by e-mail attachment.

Footnotes must conform with *The Bluebook: A Uniform System of Citation* (most recent edition), and authors should be prepared to supply any cited sources upon request. Authors must include a direct e-mail address and phone number at which they can be reached throughout the review period.

Subscriptions beginning with Volume 49 are $35.00 per year (domestic), $40.00 per year (foreign); individual issues are $10.00 domestic and $11.00 foreign. Orders for subscriptions or single issues may enclose payment or request billing and should include the subscriber's complete mailing address. Subscriptions will be renewed automatically unless notification to the contrary is received by the *Journal*. Orders for issues from volumes prior to and including Volume 16 should be addressed to: William S. Hein & Co., Inc., 1285 Main Street, Buffalo, New York, 14209.

Please send all inquiries relating to subscriptions, advertising, or publication to: Program Coordinator, Vanderbilt Journal of Transnational Law, Vanderbilt Law School, 131 21st Avenue South, Room 152A, Nashville, Tennessee, 37203, Phone: (615) 322-2284, Facsimile: (615) 322-2354, Email Address: faye.johnson@law.vanderbilt.edu.

Class "Periodicals" postage is paid at Nashville, Tennessee, and additional mailing offices. POSTMASTER: Send address changes to Program Coordinator, Vanderbilt Journal of Transnational Law, Vanderbilt Law School, 131 21st Avenue South, Room 152A, Nashville, Tennessee, 37203.

The *Journal* is indexed in *Contents of Current Legal Periodicals*, *Current Law Index*, *Index to Legal Periodicals*, and *Index to Foreign Legal Periodicals*.

Antidiscrimination Policy: The *Journal of Transnational Law* abides by the Vanderbilt University Equal Opportunity Policy, available at http://www.vanderbilt.edu/student_handbook/university-policies-regulations/#equal-opportunity. The viewpoints expressed by authors do not necessarily represent the views of Vanderbilt University Law School.

Cite as: VAND. J. TRANSNAT'L L.

***