PROPORTIONALITY AND ITS APPLICABILITY IN THE REALM OF CYBER-ATTACKS

HENSEY A. FENTON III*

With an ever-increasing reliance on State cyber-attacks, the need for an international treaty governing the actions of Nation-States in the realm of cyberwarfare has never been greater. States now have the ability to cause unprecedented civilian loss with their cyber actions. States can destroy financial records, disrupt stock markets, manipulate cryptocurrency, shut off nuclear reactors, turn off power grids, open dams, and even shut down air traffic control systems with the click of a mouse. This article argues that any cyber-attack launched with a reasonable expectation to inflict "incidental loss of civilian life, injury to civilians, or damage to civilian objects," must be subject to the existing laws of proportionality. This article further examines the broader concept of proportionality, and the difficulties associated with applying a proportionality analysis to an offensive cyber-strike. This paper asserts that the ambiguities and complexities associated with applying the law of proportionality—in its current state and within a cyber context—will leave civilian populations vulnerable to the aggressive cyber actions of the world's cyber powers. Consequently, this article stresses the necessity of developing a proportionality standard within a unified international cyberwarfare convention and asserts that such a standard is required in order to prevent the creation of a pathway towards lethal cyber aggressions unrestrained by the laws of war.

Copyright © 2019 Hensey A. Fenton III

* Duke University School of Law, J.D. expected 2019. The Elliott School of International Affairs at the George Washington University, B.A. International Affairs, Security Policy Concentration. The author would like to thank Major General Charles J. Dunlap Jr., USAF (Ret.) for reading an early draft of this paper and providing their detailed comments. The author is also grateful for comments provided by Dr. Hensey A. Fenton Sr. The author would also like to thank the Editors of the Duke Journal of Comparative & International Law for their hard and professional work.

INTRODUCTION

With an increasing global reliance on digital infrastructure, nations have realized the strategic military advantages associated with offensive cyber-strikes. Despite this emergence of cyber-attacks, a unified international cyber-warfare agreement which adequately applies the existing laws of proportionality, does not exist. Consequently, governments have struggled to apply a *jus in bello* proportionality analysis to these potentially offensive cyber-strikes. This article will argue that any cyber-attack launched with a reasonable expectation to inflict "incidental loss of civilian life, injury to civilians, [or] damage to civilian objects"[1] must be subject to the existing laws of proportionality.

Furthermore, this article will discuss the broader concept of proportionality and the difficulties associated with applying a proportionality analysis to an offensive cyber-strike. In addition, this article will stress the necessity of developing a proportionality standard within a unified international cyberwarfare agreement and assert that such a standard is required in order to prevent the creation of a pathway for lethal cyber aggressions unrestrained by the laws of war.

This Article proceeds in four main Parts. In Part I, I trace the development of proportionality as a legal concept and examine its current

1. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 472 (Michael Schmitt ed. 2017) [hereinafter TALLINN MANUAL 2.0].

place in the law of war. In Part II, I explore the increasing importance of cyber-attacks in modern warfare and discuss varying efforts to determine what actions are considered cyber-attacks. In Part III, I propose innovations to the existing law of war by providing a unified definition for cyber-attack. This unified definition seeks to focus attention on the unique threats posed by cyber-technologies and create a standard that is workable within existing international laws of armed conflict. In Part IV, I assess the applicability of proportionality to cyber-attacks, show how existing legal structures can effectively regulate state action in the realm of cyber strikes, and discuss the difficulties associated with such application. These difficulties include those arising from the predominance of dual-use systems, including: (a) the potential impact of cyber-attacks on civilian infrastructure; and (b) the complications associated with distinguishing between military and civilian systems and the difficulties of predicting reverberating effects. In Part V, I provide tangible solutions to ease the challenges associated with applying a proportionality analysis to cyber-attacks. Finally, in Part VI, I conclude by proposing the creation of a proportionality standard embodied within a unified international cyberwarfare agreement.

I. PROPORTIONALITY – A BASIC DEFINITION

With the growing effectiveness and use of cyber-attacks[2] as a mechanism of war, it is crucial to determine when cyber-attacks are likely to have a disproportionate impact on civilians.[3] Consequently, proportionality must play a crucial role in the future of cyberwar.[4]

Proportionality, in its basic form, exists as a limit on lethal force, which ensures that such force is only appropriately employed in a way that is commensurate with the military goal to be achieved.[5] Proportionality restricts the force employed within warfare through reference to a rather fixed standard: "[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

2. Throughout this article, I will use the terms "cyber-attack" and "cyber-strike" interchangeably.

3. *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 817 (2012) ("Cyber-attacks have become increasingly common in recent years. Capable of shutting down nuclear centrifuges, air defense systems, and electrical grids, cyber-attacks pose a serious threat to national security.").

4. Proportionality within the context of the law of international armed conflict is comprised of two principal components: the right to engage in war (*jus ad bellum*), and the limitation on conduct during war (*jus in bello*). *See generally* Enzo Cannizzaro, *Contextualizing Proportionality:* Jus Ad Bellum *and* Jus In Bello *in Lebanese War*, 88 INT'L REV. OF THE RED CROSS 779, 781–85 (2006). However, this paper will exclusively discuss *jus in bello* proportionality.

5. MICHAEL NEWTON & LARRY MAY, PROPORTIONALITY IN INTERNATIONAL LAW 2 (2014).

objectives of the use of force."[6] In other words, the "loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained."[7]

The *jus in bello* proportionality requirement prohibits "[any] attack 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."[8] Under the law of armed conflict, states may use aggressive force to destroy any legitimate enemy target(s). The law of armed conflict, however, places meaningful restrictions on states in their use of force against civilians and civilian objects.[9] Although states possess substantial discretion in targeting and destroying enemy combatants, *jus in bello* proportionality requires that states balance those legitimate military objectives against the likelihood of incidental harms to civilians.[10]

The *jus in bello* proportionality requirement is codified in the Geneva Conventions of 1949.[11] While the Conventions originally failed to address *jus in bello* proportionality,[12] Amendment Protocol I (API) to the Geneva Conventions explicitly required states to conduct proportionality analyses during armed conflict.[13] In particular, API prohibits "[any] attack 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."[14]

Accordingly, the principle of proportionality requires a military commander to balance the concrete and direct military advantage he is likely to obtain against any incidental harm the attack is likely to cause to civilians

---

6. *Id*. at 3.

7. U.S. DEP'T OF ARMY, FIELD MANUAL 27-10, THE LAW ON LAND WARFARE para. 41 (July 18, 1956).

8. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 57(2)(a)(iii), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

9. *See* Matthew L. Beran, *The Proportionality Balancing Test Revisited: How Counterinsurgency Changes "Military Advantage,"* THE ARMY LAW., Aug. 2010, at 4, 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.").

10. *See generally* Protocol I, *supra* note 8, art. 51 (laying out rules to help guarantee "general protection against dangers arising from military operations" to civilians).

11. Protocol I art. 51(5).

12. *See generally* Protocol I, *supra* note 8.

13. *See id.* art. 51.

14. *Id*. art. 51(5)(b) (emphasis added).

or civilian objects.[15] If the expected collateral damage to civilians or civilian property is excessive in relation to those concrete military objectives, the use of force would be disproportionate and therefore illegal.[16]

II. WHAT IS A CYBER-ATTACK? – VARYING DEFINITIONS

Cyber-attacks pose endless threats to an evolving technological world. Such threats range from viruses and worms capable of destroying financial records,[17] disrupting stock markets,[18] manipulating cryptocurrency,[19] shutting off nuclear reactors,[20] opening dams,[21] and even causing blackouts of air traffic control systems that could cause airplanes to crash.[22] Despite the omnipresent nature of these threats, there is not a settled method for identifying such threats as cyber-attacks.

This lack of a definition may lead to situations where *jus in bello* proportionality fails to be applied to certain cyber incidences that should be deemed as attacks under international law. Thus, risking the creation of a

15. There is some disagreement on the scope of the "military advantage" language in API. *Id*. Several States have argued that the expression "military advantage" refers to the advantage anticipated from the military attack considered as a whole and not only from isolated or particular parts of that attack. *See* INT'L COMM. OF THE RED CROSS [ICRC], *Distinction Between Civilian Objects and Military Objectives*, *in* CUSTOMARY INTERNATIONAL HUMANITARIAN LAW VOL. II 183–84 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) (comparing definitions of "military advantage" in different countries' military manuals). This represents a significant broadening of the concept of proportionality, as states would be permitted to consider abstract long-term advantages that might result from discrete military action, even if the short-term harm to civilians is disproportionate.

16. Protocol I provides that "[a]n attack 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" shall be considered an indiscriminate attack. Protocol I, *supra* note 8, at art. 51(5)(b). Additionally, it defines three types of indiscriminate attacks: (1) attacks that "are not directed at a specific military objective," (2) attacks that "employ a method or means of combat which cannot be directed at a specific military objective," and (3) attacks that "employ a method or means of combat the effects of which cannot be limited as required by this Protocol." *Id.* art. 51(4). Under Protocol I, it is a grave breach to launch an attack knowing it will cause excessive collateral damage in relation to the military advantage gained.

17. Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1031 n.37 (2007).

18. *See id.* at 1042.

19. *See, e.g.,* Charlie Dunlap, *Is Bitcoin Targetable?*, LAWFIRE (Mar. 10, 2018), https://sites.duke.edu/lawfire/2018/03/10/is-bitcoin-targetable-2/.

20. Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 140 (2005).

21. Barton Gellman, *Cyber Attacks by al Qaeda Feared: Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say*, WASH. POST, (June 27, 2002), https://www.washingtonpost.com/archive/politics/2002/06/27/cyber-attacks-by-al-qaeda-feared/5d9d6b05-fe79-432f-8245-7c8e9bb45813/?noredirect=on&utm_term=.31a1acbb782a.

22. *See generally* U.S. GEN. ACCOUNTING OFFICE, GAO/AIM-98-155, AIR TRAFFIC CONTROL: WEAK COMPUTER SECURITY PRACTICES JEOPARDIZE FLIGHT SAFETY 9 (May 1998).

pathway for nations to engage in unlimited cyberwarfare without accounting for civilian casualties or the destruction of civilian infrastructure.

The absence of a clear definition of cyber-attack creates uncertainties for military commanders who seek to properly execute pre-strike proportionality analyses and for governments who seek to generate uniformity with the creation of an international cyberwar treaty.[23] Consequently, defining cyber-attack is an important first step towards addressing the applicability of the law of proportionality within the context of cyber-attacks. Although multiple definitions of "cyber-attack" exist, this paper will discuss the most widely cited and reliable definitions currently available, and thereafter propose a definition that incorporates the most aggressive cyber activities. This definition will definitively place such cyber actions within the purview of the law of armed conflict, and thus strengthen proportionality's applicability to cyber-attacks.

A. State Efforts

In a movement to recognize the legal and national security implications of cyber-attacks, a few states have led efforts to determine the scope of the threats posed by cyber-attacks.[24] The most prominent of these efforts are the Joint Chiefs of Staff Lexicon, the Shanghai Cooperation Agreement and the Tallinn Manual.[25]

---

23. *See* Hathaway, *supra* note 3, at 821.

24. *See id.* at 824. Scholars have also provided their own definitions of cyber-attack. Former National Coordinator for Security, Infrastructure Protection and Counter-terrorism, Richard A. Clarke provides one of the most widely cited definitions of a cyber-attack. Clarke defines cyber-attack as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010). Although Clarke's definition is commonly cited, by limiting his definition to attacks carried out by nation-states, Clarke excludes attacks committed by non-state actors. Michael Hayden, former NSA and CIA director, defines cyber-attack as "[the] deliberate attempt to disable or destroy another country's computer networks." Tom Gjelten, *Extending the Law of War to Cyberspace*, NPR (Sept. 22, 2010), https://www.npr.org/templates/story /story.php?storyId=130023318. Although these definitions are commonly used, they are too broad and fail to properly differentiate cyber-attacks from other cyber activities like cyber-crimes. *See* Hathaway, *supra* note 3, at 824. Consequently, Hayden's definition is vulnerable to dangerously broad applications of the law of armed conflict. Martin Libicki, the Chair of cybersecurity studies at the U.S. Naval Academy, provides another definition of cyber-war which limits cyber-war to semantic attacks. Libicki's definition is also limited, because it fails to incorporate potential cyber threats which do not meet the narrowed semantic attack classification. *See* Hathaway, *supra* note 3, at 824 ("This approach excludes the broad range of potential threats to a country's national security that target cyber-infrastructure but do not meet the requirements of a semantic attack. These threats have the same capacity to inflict harm on computer systems or network."). The potential threats, which Libicki excludes from his definition, possess the same capacity to inflict harm on computer systems as those threats included in his definition. Consequently, it is pertinent that any definition of cyber-attack also includes those threats. *See id*.

25. *See* Hathaway, *supra* note 3, at 824 (defining the Shanghai Cooperation Organization as "a security cooperation group composed of China, Russia, and most of the former Soviet Central Asian

B. US Efforts

In 2011, the Joint Chiefs of Staff published a lexicon for military use in cyber-operations. This lexicon included the first official military definition of cyber-attack. The Joint Chiefs defined a cyber-attack as:

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. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber-attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber-attack may be widely separated temporally and geographically from the delivery.[26]

This definition is limited because it defines cyber-attacks as only those attacks which seek to harm critical cyber systems.[27] The publication's approach is predominately focused on the objective of the particular attack, and thus the definition excludes attacks which lack a prerequisite intent.[28] Furthermore, it creates unnecessary ambiguity regarding the issue of what is and what is not a critical cyber system.[29]

C. The Shanghai Cooperation Organization's Approach

Comparatively, the Shanghai Cooperation Organization adopted a broader means-based approach in its definition of cyber-attack. The organization is concerned with the "threats posed by possible uses of [new information and communication] technologies and means for the purposes [sic] incompatible with ensuring international security and stability in both

republics, as well as observers including Iran, India, and Pakistan."). *See* MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE? 77 (1995) (defining "semantic attacks" as digital assaults that cause systems to seem to operate normally, when in fact they "generate answers at variance with reality"). *See generally* TALLINN MANUAL 2.0, *supra* note 1.

26. GEN. JAMES E. CARTWRIGHT, MEMORANDUM FOR CHIEFS OF THE MILITARY SERVS., COMMANDERS OF THE COMBATANT COMMANDS, DIRSECTORS OF THE JOINT STAFF DIRECTORIES ON JOINT TERMINOLOGY FOR CYBERSPACE OPERATIONS 5 (Nov. 2011).

27. *See* Hathaway, *supra* note 3, at 824.

28. *See id.*

29. Alternative views of cyber-attack came before this lexicon. For example, the U.S. National Research Council defined cyber-attack as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks." WILLIAM A. OWENS ET AL., NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT].

civil and military spheres."[30] Furthermore, the organization defines the term "information war" as "mass psychologic[al] brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party."[31] With this definition of "information war" the Shanghai Cooperation Organization primarily seeks to combat information that is harmful to "social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other states."[32]

The Shanghai Cooperation Organization's view of cyber-attacks includes the use of cyber-technologies in the creation of political instability. Such an expansive definition of cyber-attack seems to be focused more so on the censorship of political free speech, than protecting cyber-infrastructure.[33] Such attempts to suppress free-speech in the name of cyber security are antithetical to many concepts of human rights.[34] Consequently, the Shanghai Cooperation Organization's broad view of cyber-attacks is misguided, because of its failure to include many cyber-threats.[35]

D. Tallinn Manual

At the request of the NATO Cooperative Cyber Defense Centre of Excellence, nineteen international law experts created the Tallinn Manual on the International Law Applicable to Cyber Warfare (the "Tallinn Manual"). The Tallinn Manual is the most comprehensive analysis of how existing laws of armed conflict apply to cyber warfare.[36] The Tallinn Manual 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 to objects."[37]

The lack of uniformity existing within the aforementioned definitions of cyber-attacks demonstrates the need to create a clearer definition of the term itself in order to avoid unnecessary ambiguities within the cyberwar

---

30. AGREEMENT BETWEEN THE GOVERNMENTS OF THE MEMBER STATES OF THE SHANGHAI COOPERATION ORGANIZATION ON COOPERATION IN THE FIELD OF INTERNATIONAL INFORMATION SECURITY, 61ST PLENARY MEETING (Dec. 2, 2008) [hereinafter SHANGHAI COOPERATION AGREEMENT].

31. *Id.* at 209.

32. *Id*. at 203; *See also* Hathaway, *supra* note 3, at 825.

33. *See, e.g.*, Tom Gjelten, *Seeing the Internet as an "Information Weapon"*, NPR (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

34. *See* Hathaway, *supra* note 3, at 825 ("As the Internet is increasingly utilized as a forum for exchange of ideas and political organization, [Internet] suppression threatens human rights.").

35. *See id*.

36. *See generally* TALLINN MANUAL 2.0, *supra* note 1.

37. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 106 (Michael Schmitt ed. 2013) [hereinafter TALLINN MANUAL]. *See* Eric Boylan, *Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners*, 50 VAND. J. TRANSNAT'L L. 217, 223 (2017).

context. The subsequent section will provide the needed clarity, and resolve the ambiguities that exist in the search for an all-encompassing definition of a cyber-attack.

III. RECOMMENDED DEFINITION

This paper develops a limited definition of cyber-attack[38] which seeks to focus attention on the unique threats posed by cyber-technologies, and create a standard that is workable within existing international laws of armed conflict.[39] It defines cyber-attack as *any action taken, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage or destruction to objects, through the undermining of the functions of a computer network, for a political or national security purpose.*

This Section discusses the most pertinent aspects of this definition, clarifies the reasoning behind the specified language, and explains which activities it encompasses.

(1) "*Any action taken*"

To be a cyber-attack the goal of the action (hacking, bombing, cutting, infecting, etc.) must be to undermine or disrupt the function of a computer network. This part of the definition is an adoption of the U.S. objective-based approach rather than the means-based approach presented in the Shanghai Cooperation Organization.[40] Objective in this sense means the direct target, rather than the long-range purpose of the action. Defining cyber-attack based on its objective instead of its means is more efficient for two reasons.

i. An objective-based definition is better suited to protect civilian cyber infrastructure due to its inclusion of a multitude of cyber aggressions that a means-based approach fails to encompass. For example, using a computer network to operate a predator drone for a kinetic attack is not a cyber-attack; rather, it is technologically advanced conventional warfare. However, using kinetic capabilities to sever an undersea network cable that carries information between continents is a cyber-attack.[41]

Furthermore, means-based approaches allow for any objective, and only seek to control the means employed; objective-based approaches allow for any means, and only control the objective. In other words, under an objective-based approach, it does not matter what means the

38. This definition builds upon previous attempts to define cyber-attack.

39. The law of armed conflict applies when such attack is a "use of force." Thus, the term cyber-attack should be limited to only encompass actions which are deemed to be uses of force.

40. *See* Hathaway, *supra* note 3, at 826–27 (characterizing the U.S. approach as "objective-based").

41. *See* Antolin-Jenkins, *supra* note 20, at 138 ("[K]inetic weapons are certainly part of the cyberwar arsenal.").

attacker uses to accomplish the attack, as long as the objective is met. This view is in line with the U.S. Department of Defense's understanding of a cyber offensive. For example, the Department of Defense has identified kinetic attacks as a legitimate strategy in cyber-offensive operations.[42]

ii. An objective-based approach avoids any unnecessary limitation on free speech, thus avoiding the serious risks posed by a means-based definition.[43] Moreover, by encompassing any activity that uses cyber-technology and jeopardizes stability, a means-based understanding of cyber-warfare will likely preclude many cyber-attacks from pre-strike proportionality test requirements due to their failure to fall within the purview of the law of armed conflict.

(2) "*whether offensive or defensive*"

It is necessary to assert that an attack can be either an offensive or defensive action as this specificity prevents any ambiguity for states interpreting the definition. Asserting that both offensive and defensive cyber-attacks are encompassed by the meaning shows that the action can be either offensive or active defense. The goal of an "offensive" attack is to "alter, disrupt, deceive, degrade, or destroy adversary computer systems,"[44] the goal of a passive defense refers to actions taken to "reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative," and the goal of an active defense refers to the "employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[45] Therefore, the definition of an offensive or defensive action encompasses both offensive and defensive cyber-attacks.

(3) "*that is reasonably expected to cause injury or death to persons, or damage or destruction to objects*"

It is necessary to include this reasonable expectation prong within the definition (a) due to its ability to circumvent ambiguities existing within the *Nicaragua* "effects test," and (b) to be consistent with underlying

42. CHAIRMAN OF THE JOINT CHIEFS OF STAFF, U.S. DEP'T OF DEFENSE, NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS 15 (2006). A National Research Council report on "cyber offensive operations" excluded kinetic attacks on computer networks for the purposes of the report but acknowledged that such attacks were realistic forms of cyber-attack. NRC REPORT, *supra* note 29, at 1–2.

43. *See, e.g.*, Gjelten, *supra* note 33 (discussing the United States' opposition to efforts to limit Internet communications that are disguised as cyber security operations).

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

45. C. Robert Kehler, Herbert Lin and Michael Sulmeyer, *Rule of engagement for cyberspace operations: a view from the USA*, 3 JOURNAL OF CYBERSECURITY 69, 70 (2017).

humanitarian purposes of the law of armed conflict.[46] Unlike the effects test which restricts the application of international law to only cyber-attacks that produce conditions similar to that of kinetic weapons, this definitional requirement encompasses all reasonably foreseeable consequential damage, injury, or death. Since cyber-attacks often fail to generate physically identifiable effects, any definition that does not include attacks which do not produce physical effects, fails to include a majority of cyber-attacks. Furthermore, this portion of the definition includes injuries that incorporate the underlying humanitarian purposes of the law of armed conflict, by extending the definition to *serious* illnesses and *severe* mental sufferings that are indispensable from injuries caused by such attacks.

(4) "*to undermine the function*"

The objective of a cyber-attack must be to undermine the functioning of a computer network. Compromising a computer network can occur in a variety of ways.[47] A syntactic attack can compromise a computer network with the use of worms, viruses, [and] Trojan horses that target the network infrastructure.[48] Semantic attacks on the other hand, undermine the functions of computer networks by targeting the decision process of the system. Semantic attacks preserve the operating system but compromise the accuracy of the information it processes and to which it reacts.[49] As a result, "[a] system under semantic attack operates and will be perceived as operating correctly . . . but it will generate answers at variance with reality."[50]

However, neither cyber-espionage nor cyber-exploitation are considered cyber-attacks due to their failure to undermine computer networks in a way that affects current or future functionalities.[51] In 2003 for

46. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. Rep. 14, ¶ 195 (June 27) (theorizing that actions which result in damage, casualties, or other consequences typical of a "use of force" should be considered force themselves); *see also* Hathaway, *supra* note 3, at 841 ("The best test of when a cyber-attack is properly considered [a use of force] is whether the attack results in . . . a 'kinetic effect'—comparable to a conventional attack."); *see also* Stephen Petkis, Note, *Rethinking Proportionality in the Cyber Context*, 47 GEO. J. INT'L. L. 1431, 1447 (2016).

47. *See* Antolin-Jenkins, *supra* note 20, at 139–41 (giving examples of syntactic, semantic, and mixed attacks); *see also* Hathaway, *supra* note 3, at 828 (discussing syntactic and semantic attacks).

48. *See* Antolin-Jenkins, *supra* note 20, at 139; *see also* Hathaway, *supra* note 3, at 828 ("Syntactic attacks disrupt a computer's operating system, causing the network to malfunction.").

49. *See* Antolin-Jenkins, *supra* note 20, at 140.

50. MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE? 77 (1995).

51. This paper adopts the following definition of cyber-espionage: "the science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence." Seymour M. Hersh, *The Online Threat: Should We Be Worried About a Cyber War?* NEW YORKER (Nov. 1, 2010) http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?. The former director of the Central Intelligence Agency (CIA) emphasizes that cyber-espionage does not fall under the umbrella of

example, sensitive information was leaked from U.S. Department of Defense computers.[52] The Department has acknowledged that this incident of cyber-espionage was carried out by the Chinese.[53] Another example of a similar cyber-espionage incident occurred when Chinese hackers copied data from Google and other major Internet technology companies in 2010. This act of cyber-espionage led to the theft of intellectual property and the unlawful surveillance of human rights activists.[54] Moreover, the Chinese government sought to monitor the emails of U.S. government officials. More recently, the Department of Defense revealed that it suffered one of its worst cyber-espionage leaks in March 2011 when foreign hackers gained access to over 24,000 Pentagon files. [55]

(5) "*of a computer network*"

It is necessary for the target of a cyber-attack to be a computer network. For the purposes of this definition, a computer network is defined as any system of computers and devices linked by varying channels of communication.[56] When employing this portion of the definition, necessity also lies in one's ability to conceptualize the evolving reality that computer networks do not solely include commonplace laptops and desktops. Computer networks control standard appliances and devices that play an essential role in our everyday lives. These networks include devices that control elevators, traffic lights, city water systems, and the power grids that distribute electricity.[57] Due to the ubiquitous nature of computer systems, the potential for a cyber-attack to produce extensive destruction will continue to

---

cyber-warfare, likely because the U.S. government—like many other governments—routinely engages in espionage over communications networks. Gjelten, *supra* note 33. Notably, the National Research Council distinguishes what it calls cyber-exploitation from cyber-attack because "[t]he [law of armed conflict] presumes that a clear distinction can be drawn between the use of force and espionage, where espionage is avowedly not a use of force." NRC REPORT, *supra* note 29, at 22, § 1.6.

52. CLAY WILSON, CONG. RESEARCH SERV., RL 32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 14 (2008).

53. *Id.*

54. *See* James Glanz & John Markoff, *State's Secrets Day 7; Vast Hacking by a China Fearful of the Web*, N.Y. TIMES (Dec. 4, 2010) https://archive.nytimes.com/www .nytimes.com/2010/12/05/world/asia/05wikileaks-china.html.

55. *See, e.g.*, Amir Efrati & Siobhan Gorman, *Google Mail Hack Is Blamed on China*, WALL ST. J., June 2, 2011, at A1; Wyatt Andrews, *China Google Hacker's Goal: Spying on U.S. Govt*, CBS NEWS (June 2, 2011), http://m.cbsnews.com/fullstory.rbml?catid=20068474&feed_id=0& videofeed=36; Thom Shanker & Elisabeth Bumiller, *After Suffering Damaging Cyberattack, the Pentagon Takes Defenive Action*, N.Y. TIMES, July 15, 2011, at A6; Jack Goldsmith, *What Is the Government's Strategy Damaging Cyber Exploitation Threat?* LAWFARE BLOG (Aug. 10, 2011, 10:58 PM), https://www.lawfareblog.com/what-governments-strategy-cyber-exploitation-threat.

56. *See* Hathaway, *supra* note 3, at 830.

57. *See id.*

grow as the world continues to become ever more dependent on computer networks.

(6) "*for a political or national security purpose.*"

It is necessary to also include this prong within any definition of a cyber-attack due to its ability to distinguish a cyber-attack from other cyber-crimes. Any aggressive cyber action by a state against another state necessarily implicates national security and is thus a cyber-attack so long as all other prongs of this definition are met. But although this distinguishing purpose is not necessary in the context of state actions, it serves a pivotal role in defining cyber-attack when the action is taken by a non-state actor. If a non-state actor engages in any cyber action which is made with a political or national security purpose, such action shall be deemed a cyber-attack under this definition.[58] Conversely, a cyber action taken by a non-state actor which lacks political or national security scienter will be treated as a cyber-crime (i.e. cyber actions that are not carried out for political or national security purposes) and will not trigger an application of the laws of armed conflict.[59]

It is pertinent to exclude cyber-crimes for two primary reasons. First, such actions are likely not in breach of public international law, and thus they do not raise the same grave legal concerns that cyber-attacks do.[60] Moreover, unlike cyber-attacks, the actions of private criminal hackers often fail to trigger legal doctrines within the context of state responsibility and terrorism.[61] Secondly, a clear distinction between cyber-attacks and cyber-crimes is necessary to create efficiencies within cyber security cooperative efforts. That is to say, state cyber security cooperative efforts will operate more smoothly if there is a distinction between what is an act of war and what is solely a crime. This will ensure that state resources are allocated appropriately in cooperative attempts to combat cyber threats.[62]

Additionally, this definitional prong highlights the public nature of cyber-attacks without restricting the definition to state actors. Because

58. The actions of Kremlin Kids, private hackers who shut down the Internet in Georgia in coordination with the Russian invasion of the country, would be an example of a private cyber action that meets the political or national security purpose prong of this definition. *See* Noah Shachtman, *Kremlin Kids: We Launched the Estonian Cyber War*, WIRED (Mar. 11, 2009, 12:45 PM), http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/.

59. *See* Hathaway, *supra* note 3, at 830–31 (asserting that internet fraud, identity theft, and intellectual property piracy are not cyber-attacks).

60. *See id.* (stating that cyber-crimes do not "raise the same legal questions as activities that might breach public international law").

61. *See id.* (comparing the differences between the actions of the Kremlin Kids, which "invoked the legal doctrines surrounding state responsibility and terrorism," and those of a student infecting tens of millions of computers with a "love bug virus").

62. *See id.* (stating that such a distinction would clarify ownership of cyber-security needs).

cyber-attacks are relatively inexpensive in comparison to many kinetic weapons that produce similar results, and since non-state actors are relatively invulnerable to in kind retribution, cyber-attacks seem to be a perfect tool for terrorist groups.[63] Consequently, any definition of cyber-attack must encompass the cyber actions of non-state actors when they rise to the level of a cyber-attack.

IV. THE APPLICABILITY OF PROPORTIONALITY AND THE LAW OF ARMED CONFLICT TO CYBER ATTACKS

Although it is settled law that a physical "attack" would be governed by the law of armed conflict, and thus subject to a proportionality standard, some contemplate whether hostilities in the realm of cyber warfare constitute attacks governed by the law of armed conflict.[64] Nevertheless, this paper accepts the assertion of the Tallinn Manual that the law of armed conflict applies to cyber operations "[d]espite the novelty of cyber operations" and the absence of specific rules in the law of armed conflict that discuss cyber-attacks.[65]

Though it is assumed that the law of armed conflict applies to cyber-attacks, applying a proportionality analysis to cyber warfare is a difficult task. Such an application requires one to determine what systems are "dual use" (i.e. systems employed by the military and civilians) and to distinguish within such systems, what is civilian from what is military. Additionally, the existence of dual-use systems heightens the likelihood of collateral damage.[66] Furthermore, the presence of knock-on effects (i.e. indirect effects that result from a given action but are not immediately discernable) and the requirement that they be included in a proportionality analysis present added complications.

63. *See* Mary Louise Kelly, *ISIS Uses Cyber Capabilities to Attack the U.S. Online*, NPR (Apr. 25, 2016), https://www.npr.org/2016/04/25/475631277/isis-uses-cyber-capabilities-to-attack-the-u-s-online (discussing the relatively inexpensive cyber-capabilities ISIS uses and how the spread of similar cyber capabilities "play into the larger expansion of cyber-strike and counter-strike throughout the Middle East.").

64. *See* Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INT'L. STUD. 198, 200–201 (2013) (discussing differing viewpoints); *see* Boylan, *supra* note 37, at 229–30 (stating that at least one commentator has argued that the term "attack" shall only be used for actions resulting in "death, damage, destruction, or injury," while another commentator argued that "any action aimed at civilians amounts to an 'attack'.").").

65. TALLINN MANUAL, *supra* note 37, at r. 20, para. 1.

66. *See* Boylan, *supra* note 37, at 230.

A. Dual-Use Systems

Dual-use systems are systems which serve both military and civilian purposes. Unlike conventional physical military installations—which are easily distinguishable and separate from civilian infrastructure—civilian and military cyber networks are commonly interwoven.[67] Such systems include power plants which supply power to both civilian and military areas, air traffic control systems which support both civilian airports and military bases, and other communication networks which provide platforms for both military and civilian communications.[68] Dual-use systems can be considered valid military targets; however, a number of unique challenges exist when one attempts to apply a proportionality test to dual-use systems.[69]

Though civilian usages of such systems may influence the proportionality analysis, civilian usage does not preclude a dual-use system from a legal cyber-attack.[70] However, two requirements must be met before a dual-use system can be legitimized as a valid military target: the target itself must create an operational contribution to the enemy's military action, and the destruction of the target must generate a tangible military advantage.[71] Additionally, an attack against a dual-use system must also pass a proportionality test.[72] However, unlike the case with purely civilian systems, once a dual-use system meets these prerequisites it may be lawfully targeted and attacked.[73]

Although dual-use systems are not precluded from cyber-attacks, their multifunctional purposes create two distinct problems within a proportionality analysis. First, attacking dual-use systems presents an increased likelihood that the presupposed collateral damage calculated in a proportionality test will be drastically insurmountable when balanced with the expected military advantage. Second, attacking a dual-use system

---

67. HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 194 (2012) ("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.").

68. *Id.*; *see also* Boylan, *supra* note 37, at 231.

69. The integration of military and civilian cyber networks, will make it harder for nations to distinguish between what is civilian and what is military—making it harder to apply a proportionality analysis. *See* DINNISS, *supra* note 67, at 194–95.

70. *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 . . . .").

71. *See* Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 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.").

72. *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."); *see also*, Boylan, *supra* note 37, at 232.

73. Boylan, *supra* note 37, at 232.

requires engaging with the difficult—and often impossible—task of distinguishing between what parts of a dual-use system are civilian and what parts are military.[74]

Due to the prevalent nature of dual-use systems within the world of cyber technology, cyber-attacks will have a more amplified impact on civilian infrastructure in comparison to kinetic attacks of an analogous form. Increased impacts on civilian infrastructure lessen the likelihood that the reasonably expected military advantage gained from such an attack will outweigh the reasonably foreseeable collateral damage. In other words, increased collateral damage caused by a prevalence of dual-use systems makes it more difficult for a proposed cyber-attack to overcome a proportionality test.[75]

The prevalence of dual-use systems will also inhibit the ability to distinguish between military and civilian cyber infrastructure.[76] Military commanders will likely encounter scenarios where they are unable to determine the difference between infrastructure that is civilian and that which is military.[77] Moreover, commanders will often be unable to conduct a complete proportionality calculation due to their inability to determine what impact their attack will have on civilian infrastructure.[78]

Distinguishing civilian from military infrastructure is necessary for a proper application of a proportionality test to a cyber-attack. In order to adequately apply a proportionality analysis, one must know the character and capabilities of the system under consideration for attack in order to reasonably predict the effects of such attack.[79] However, such analysis has become increasingly difficult in an intersecting technological environment where systems are simultaneously used by both civilians and the military.[80]

---

74. *Id.*

75. *Id.* at 232–33 ("However, if the impact on civilian infrastructure is increased to the point that it outweighs the military advantage to be gained, this would constitute an attack violative of the law of armed conflict."); *see also*, Boylan, *supra* note 37, at 232.

76. *Id.* at 231.

77. *Id.* at 231 ("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. 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.").

78. *Id.* at 233.

79. *Id.*

80. *See generally* DINNISS, *supra* note 67.

B. Knock-on Effects

Knock-on effects are "the indirect consequences that flow from the direct results of a given action."[81] Although these effects are difficult to predict in the cyber realm, one must consider such effects when conducting a proportionality analysis. The interconnectedness of cyber systems creates complications in estimating the effects of a cyber-attack, and due to this interconnectedness, information is able to travel between networks at distances that make it difficult to ascertain the ripple effects of an attack with any accuracy.[82] This problem is further exacerbated by international applications of cyber languages. The multi-national and multi-linguistic nature of cyber systems make understanding the reach of a given system increasingly difficult.[83] Such an expansive and complex cyber space makes it challenging to estimate the ways in which a cyber-attack can affect those outside of the initial sphere of attack.[84]

Moreover, the rapid operating nature of computer systems also stands as an obstacle in the adequate estimation of knock-on effects. Computer operating speeds have increased exponentially over the past few years, and Central Processing Units that once only occupied two-thousand transistors, now hold nearly two billion.[85] This increased processing capability has made the predictability of knock-on effects inscrutable.

The inability for militaries to thoroughly predict the consequences of cyber-attacks was shown in the Stuxnet case. The Stuxnet malware virus was released by a U.S.-Israeli joint operation, into the Natanz nuclear facility in Iran.[86] Stuxnet was created to target centrifuges used in the production of the

81. Boylan, *supra* note 37, at 235; *see* Ian Henderson & Kate Reece, *Proportionality Under International Humanitarian Law: The "Reasonable Military Commander" Standard and Reverberating Effects*, 51 VAND. J. TRANSNAT'L L. 1, 12–13 (2018); *see also* Eric Talbot Jensen, *Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1176 (2003).

82. *See* MARK GRAHAM & STEFANO DE SABATA, *INTERNET TUBE: An Abstraction of the Global Submarine Fiber-Optic Cable Network*, OXFORD INTERNET INST. (Apr. 2, 2014), https://geography.oii.ox.ac.uk/internet-tube/ ("Today, an entire network of fiber-optic cables connects almost every corner of the world, enabling the hyper-connected world that many of us take for granted.").

83. *See* Daniel Sorid, *Writing the Web's Future in Numerous Languages*, N.Y. TIMES (Dec. 30, 2008), www.nytimes.com/2008/12/31/technology/internet/31hindi.html ("The next chapter of the World Wide Web will not be written in English alone.").

84. *Id*.

85. *See* Dean Takahashi, *Forty Years of Moore's Law*, SEATTLE TIMES (Apr. 18, 2005), http://www.seattletimes.com/business/forty-years-of-moores-law.

86. Ellen Nakashima and Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say,* WASH. POST (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?noredirect=on&utm_term=.7fd2ef4bee5f.

enriched uranium powering Iranian nuclear weapons and reactors.[87] The worm was intended to be a tool to derail, or at least delay, the Iranian program to develop nuclear weapons.[88] The malware caused the centrifuges to operate erratically – forcing the centrifuges to speed up and slow down at uncontrollable rates, which caused them to self-destruct. Simultaneously, the virus sent signals to the facility's computers which told operators that the centrifuges were operating regularly.[89]

Stuxnet was never intended, nor expected to spread beyond the nuclear facility at Natanz. Nevertheless, the malware infected an internet-connected computer and began to spread uncontrollably outside the facility. Although the leak of the malware to outside systems did not cause collateral damage, the case is illustrative of the difficulties in predicting the impact of a cyber strike even when implementing a well thought out and prepared attack such as Stuxnet.[90]

These difficulties in applying the proportionality standard to cyber-attacks must be eased. The next section lays out two possible solutions.

V. SOLUTIONS TO DEAL WITH CYBER COMPLEXITIES

With a growing reliance on cyber strikes, it is necessary for military leaders to work through the complexities that arise from the application of a proportionality analysis to cyber-attacks. Cyber-attacks can provide nations with a myriad of benefits and flexibilities. Cyber-attacks allow militaries to impair enemy capabilities in a fashion analogous to, but more efficient than, kinetic attacks. This greater efficiency stems from: (1) the capacity for cyber-attacks to produce the same military advantage without the heightened probability of inflicting civilian casualties; (2) the lower cost of cyber-attacks; (3) the possibility that cyber-attacks can produce the same military advantage without the amount of physical destruction associated with kinetic attacks;[91] and (4) the capacity for cyber operations to provide nations with

87. Josh Fruhlinger, *What is Stuxnet, Who Created It and How Does It Work?*, CSO (Aug. 22, 2017), https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

88. *See id.*

89. 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).

90. *See* Boylan, *supra* note 37, at 237 ("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 operations.").

91. *See* Schaap, *supra* note 71, 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.").

the ability to circumvent belligerents' uses of lawfare[92] in an attempt to garner animosity against an opposing military operation.[93]

These benefits have catalyzed a growing reliance on militarized cyber operations. Although such benefits tend to create a presumption of operational legitimacy, militaries must still structure these attacks within the confines of a proportionality analysis, despite the confusions that may arise from it. Consequently, the two recommendations provided in the following section should ameliorate the friction caused by the application of a proportionality analysis to a cyber-attack.

A. Apply a Comprehensive Analysis Prior to All Attacks

Due to the relative ease and efficiency of initiating a cyber strike, militaries may minimize the need to forego a thorough proportionality analysis. In other words, since military commanders are likely to view cyber strikes as less dangerous, due to the reduced possibility of civilian deaths associated with their use, commanders may become more aggressive and conduct a lackluster pre-strike analysis in lieu of a complete proportionality analysis.[94]

This diminished need to conduct a proper pre-strike analysis is not only negligent but amounts to a dereliction of duty by the commander conducting the operation. With the unpredictable nature of cyber operations, even the most planned and thought out cyber-attacks lead to knock-on effects that were not predicted prior to the strike. It is this unpredictability that makes it essential for militaries to conduct a thorough proportionality review prior to conducting a cyber strike.

Not only do militaries need to conduct a proportionality analysis prior to any cyber-attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, but Protocol I[95] requires that militaries also "exert caution as to civilians and

92. Maj. Gen. Charles J. Dunlap, Jr., *Lawfare Today: A Perspective*, 3 YALE J. INT'L AFF. 146, 146 (2008) (defining "lawfare" as "the strategy of using – or misusing – law as a substitute for traditional military means to achieve an operational objective").

93. *Id.* at 148 ("[B]elligerents have long sought to use the perception or fact of wrongdoing by their opponents as a means of catalyzing support among their own people, and eroding it among their foes."). With a cyber-attack, militaries can efficiently impair enemy capabilities without risking the potential public delegitimation associated with kinetic attacks that cause massive civilian casualties.

94. *See* Boylan, *supra* note 37, at 238 ("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.").

95. Article 57 of Additional Protocol I is titled "Precaution in the Attacks." This Article states "[i]n the conduct of military operations . . . all reasonable precautions [shall be taken] to avoid losses of civilian lives and damage to civilian objects." Protocol I, *supra* note 8, art. 57.

civilian objects, even when not in the throes of battle."[96] This Additional Protocol I requirement, known as the "constant care standard," reveals the high standard of care that militaries must impose when conducting cyber operations that touch civilians or civilian infrastructure—even if such operations are not attacks.[97] Since "virtually every cyber operation will traverse, affect, employ or damage civilian cyber infrastructure of some kind,"[98] the constant care standard seems to require militaries to maintain constant situational awareness, and a high level of vigilance in all militarized cyber operations.[99] Consequently, if such a heightened sense of vigilance is required for operations that are not attacks, it is intuitive that militaries must impose an especially stringent set of precautionary pre-strike measures when such operations are attacks (i.e. a proportionality test).[100]

Despite the complications associated with conducting a proportionality test within a cyber context, the unpredictability of cyber-attacks as well as the symbiotic nature of dual-use systems require militaries to conduct a proportionality analysis prior to initiating any cyber-attack.[101] As mentioned previously, when a cyber operation rises to the level of an attack, it must be subjected to a proportionality analysis. Notwithstanding the complications that modern computer networks present to militaries in their attempts to conduct proportionality analyses, militaries must take the necessary steps to assess the likely civilian repercussions of any cyber-attack they engage in.

B. Hire Cyber Specialists

With the complexities existing in an ever-evolving cyber world, it is not feasible for military commanders to conduct proportionality reviews related to cyber operations without the consultation of a cyber specialist.[102] It would be ill-advised and reckless for military officers well versed in kinetic proportionality analyses to be charged with understanding the convoluted

---

96. *See* Jensen, *supra* note 64, 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."); *see also* Boylan, *supra* note 37, at 238.

97. *See* Boylan, *supra* note 37, at 238.

98. *See* Jensen, *supra* note 64, at 203.

99. *See id*. at 203 ("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."); *see also* Boylan, *supra* note 37, at 238.

100. Boylan, *supra* note 37, at 239.

101. *See id*.

102. There is some question on whether or not military commanders are required to consult network specialist in the application of proportionality. *See* DINNISS, *supra* note 67, 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.").

cyber systems, which these cyber-attacks attempt to disrupt. Consequently, militaries must hire individuals who are experts in cyber systems and who are aware of the possible impacts cyber operations may have on said systems.

Customarily, military leaders are obligated to obtain optimal intelligence and act in good faith on that said intelligence.[103] These obligations are often easily attainable within the confines of customary kinetic warfare.[104] Proficiency in the use of traditional weapons systems is a skill found throughout most developed militaries. Consequently, it is relatively easy for military officers to obtain expertized collateral damage estimates when an attack is kinetic in form.[105] However, when militaries engage in cyber-attacks, an analogous level of expertise may likely be absent.

In order to properly carry out their duties, military leaders must hire outside specialists or train military specialists to determine if a cyber-attack is reasonably expected to inflict incidental loss of civilian life, injury to civilians, damage to civilian objects,[106] or a combination of all three.[107] Although any military that is capable of waging a complex cyber operation likely possesses the monetary resources essential for retaining a suitable cyber specialist, hiring or training such specialist will still likely be an expensive undertaking. The added expense associated with retaining a cyber specialist could cause militaries to reevaluate their newfound reliance on cyber operations.[108] As mentioned previously, one major advantage of cyber operations is their ability to create results similar to that of their kinetic alternative, without the additional cost. This benefit, however, may vanish if

103. *See id.* at 207 ("[Commanders] are also under an obligation to obtain the best possible intelligence . . . ."); *see also* Boylan, *supra* note 37, at 239.

104. *See* DINNISS, *supra* note 67, 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 systems involved and its effects . . . .").

105. *See id*.

106. *See* TALLINN MANUAL, *supra* note 37, at 103–4 (discussing the principle of distinction).

107. These seem to be the only viable options for military commanders in this situation. Commanders are responsible for obtaining all reasonably optimal intelligence prior to initiating any attack. If a commander fails to determine if a cyber-attack will inflict collateral damage solely due to a lack of subject matter expertise, that commander will be failing in his or her duty. *See* Boylan, *supra* note 37, at 240 ("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.").

108. Boylan, *supra* note 37, at 240 (asserting that using a cyber-specialist "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.").

the cost of retaining a specialist makes the cost of the cyber-attack exponentially higher than the cost of a kinetic attack.[109]

Moreover, militaries may be dissuaded from hiring cyber specialists due to the possibility that their services may never actually be needed. In other words, even if a commander does not wish to engage in a specific cyber-attack, a specialist must still continually be retained for the moment(s) a commander does wish to engage.[110] Admittedly, the other advantages of cyber strikes (the absence of civilian deaths, lessened destruction of civilian property, and circumvention of belligerent use of lawfare) on balance, likely make the additional cost of training and retaining specialist inconsequential.[111]

However, militaries whose cyber programs are relatively new may seek to retain the services of an outside cyber technology group as a means to circumvent this dead weight concern.[112] By hiring consultants on a contingency basis, militaries ensure that they are only paying for a specialist when their services are specifically needed, avoiding the dead weight issue of having a specialist on staff whose services are rarely needed. Although such a policy may prove to be monetarily expedient, these cyber operations may not meet the constant care standard without an on-staff specialist. A military cannot maintain constant situational awareness and a high level of vigilance within a cyber operation when it fails to maintain an individual on staff who is equipped to predict the effects of such operations. Thus, newly emerging cyber powers should utilize their hiring of outside specialists to the fullest extent. Newly emerging cyber powers should also require their consultants to train individuals within their militaries in the cyber services being provided in order to guarantee that there is a trained individual on staff who can aid in at least a bare minimal analysis to meet the constant care standard. Nevertheless, if employing a specialist for proportionality analyses generates an absence of civilian casualties and a lessened amount of civilian infrastructural devastation, the inconveniences and monetary cost of doing so are likely outweighed.

109. *Id.*

110. *Id.*

111. *See id* (asserting that monetary expense of employing a specialist is less consequential when advantages of a cyber attack are weighed in to consideration).

112. When I refer to dead weight, I am referring to the phenomena of hiring an individual for a particular job when that individual's services are rarely needed for that particular job.

VI. DEVELOPING A PROPORTIONALITY STANDARD WITHIN A UNIFIED INTERNATIONAL CYBERWARFARE AGREEMENT

With all of the aforementioned complexities and issues associated with the applicability of proportionality analyses within a cyber context, necessity lies in the development of an international cyberwarfare agreement which includes a detailed *jus in bello* proportionality standard and the unified definition of a cyber-attack provided in Part II.

While cyber warfare is primarily governed by the existing codified laws of armed conflict, these laws were written prior to the advent of modern computing technology.[113] Consequently, the applicability of current international standards to cyberwarfare stems from a false notion of cyber-kinetic equivalency.[114] The absence of laws explicitly developed for tackling the nuances of cyber war, in addition to the predominant application of other fields that are loosely related, create unnecessary challenges in regulating cyber war.[115] The difficulty in applying laws that were written prior to the notion of computers let alone complex cyber warfare, hinders militaries that seek to utilize cyber-attacks as a means of war.[116]

Moreover, without an international standard governing cyber-attacks, nations will likely take advantage of the legal ambiguities existing within the current framework to initiate cyber-attacks without restraint. In other words, the lack of an international treaty governing cyberwar creates a void which will allow nations to employ lawfare as a means to circumvent restrictions on the use of cyber force.[117] The recent actions of China in the South China Sea[118] and Russia within the former Soviet bloc[119] reveal a willingness for

113. Boylan, *supra* note 37, at 220.

114. *See id*. at 242 ("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.").

115. *See* Antonia Chayes, *Rethinking Warfare: The Ambiguity of Cyber Attacks*, 6 HARV. NAT'L SEC. J. 474, 510 (2015) ("However, until international agreements alter the law, or the International Court of Justice rules on such issues, many of the novel legal questions that cyberattacks pose will be answered by creative, if contrived, adaption of historic doctrines.").

116. *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. . . ."); *see also* Boylan, *supra* note 37, at 221.

117. *See* Dunlap, *supra* note 92, at 146 (defining lawfare as "the strategy of using – or misusing – law as a substitute for traditional military means to achieve an operational objective.").

118. *See* Joel P. Trachtman, *Integrating Lawfare and Warfare*, 39 B. C. INT'L & COMP. L. REV. 267, 273 (2016) (discussing how China's recent creation of artificial islands "seem[s] to combine an assertion of regional power with the desire for mineral and other resources in the South China Sea. China's claim is based on certain alleged land features as the basis for marine entitlements under international law.").

119. *See id*. at 272–73 (revealing that Russia supported its invasion of Crimea by asserting that it was "engaging in the right of self-defense on behalf of the ethnic Russian minority in Crimea. . . . There was no factual support for this claim, the persons allegedly at risk were not Russian citizens, and there is probably no legal right to use force to protect citizens overseas.").

the world's cyber super powers to take advantage of legal uncertainties—or creating them if necessary—for the sole purpose of circumventing existing legal restraints on their efforts for global hegemonic supremacy. Such a void will act as a catalyst in the creation of a pathway for the conducting of lethal cyber aggressions that are unrestrained by the laws of war.

As mentioned previously, the most beneficial means for combating legal ambiguities within the cyberwarfare context is to create an international treaty or some version of a multi-lateral agreement, that would govern cyberwar. The treaty must not only seek to prohibit illegal uses of cyberwarfare and provide standards for pre-strike proportionality analyses, but it must also establish codified expectations, or norms of behavior, that solidify foreign and defense polices and guide international cooperation.[120]

It is important to note that none of these suggestions for an international treaty are meant to propose that the law of armed conflict is utterly incompatible with cyber-attacks, nor do these suggestions attempt to assert that historical legal doctrine can never evolve with an ever–changing world. In reality, the law of armed conflict must be at the foundation of any treaty that seeks to govern cyberwar. A codification of a new legal regime detached from the law of armed conflict may actually prove to be counterproductive to any efforts to constrain and regulate the use of cyber-attacks,[121] and such a legal regime risks solely encompassing the cyber threats of today and precluding the cyber threats of tomorrow.[122]

Accordingly, this article does not call for the creation of a state-of-the art cyber legal regime. This article merely calls for the creation of an international treaty that builds on existing international law and provides the international community with a more efficient and tangible means for

120. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011) (explaining that the U.S. currently is prepared to create a bilateral and multilateral partnership to work "with like-minded states to establish an environment of expectations, or norms of behavior, that ground foreign and defense polices and guide international partnerships.").

121. *See* Charlie Dunlap, *Autonomous Weapons and the Law: The Yale and Brookings Discussions*, LAWFIRE (Apr. 9, 2018), https://sites.duke.edu/lawfire/2018/04/09/autonomous-weapons-and-the-law-the-yale-and-brookings-discussions/ ("My long-standing view is that the best way to regulate any weapon (to include autonomous and other high-tech weapons) is by insisting that it strictly adhere to the *existing* law of war (as opposed to trying to create a specialized legal regime for every new technology that appears).").

122. *See id.* ("Any technologically-specific legal regime inevitably captures the technology at a specific 'snapshot' in time, and this can cause unintended and even counterproductive consequences as science advances.").

conducting cyberwar by resolving the current ambiguities and complexities existing today.[123]

CONCLUSION

Although cyber-attacks are governed by the law of armed conflict, the aforementioned ambiguities and complexities associated with its applicability within the context of cyber-attacks will leave civilian populations vulnerable to the aggressive cyber actions of the world's cyber powers. Without a unified international cyberwarfare agreement, which includes a detailed *jus in bello* proportionality standard and a unified definition of cyber-attack, aggressive militarized cyber actions will be unchecked by the law of armed conflict. The tolerance of such a world where nations can take advantage of legal ambiguities as a means to wreak havoc on vulnerable civilian populations is inexplicable and inconsistent with the underlying humanitarian purposes of the law of armed conflict.

123. There have been recent attempts to develop such a standard, however more must be done. *See* Chayes, *supra* note 115, at 500 ("[C]reative attempts have been made to bring cyber attacks under the umbrella of existing international and domestic legal doctrines."). For example NATO has created the Cyber Defense Management Board and the NATO Cooperative Cyber Defense Center of Excellence in Tallinn. Boylan, *supra* note 37, at 242–43. The Cyber Defense Center has created the leading treatise on the subject of cyber war: the Tallinn Manual on the International Law Applicable to Cyber Warfare. *See* TALLINN MANUAL, *supra* note 37, 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."). This effort has laid the foundation for the creation of an international cooperative structure that addresses the issues associated with applying the laws of armed conflict to cyberwar. *See* Chayes, *supra* note 115, at 511 ("There are conferences and membership training to defend against cyber attack, which has included NATO training Jordanian army to defend against ISIS cyber attacks."). The European Union (EU) has also taken steps to generate a cooperative effort to resolve inefficiencies in the methods States use to conduct cyberwar. *See* Boylan, *supra* note 37, at 243 ("The European Union has adopted a Union-wide directive to improve cooperation on cyber security."). EU member states are now required to meet a minimum threshold of cyber defenses, and member states are encouraged to cooperate and communicate with other member states on matters of cyber security. *See id.* Canada, the United Kingdom, and Russia have also followed suit with their own similar cooperative efforts. *See id*. ("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*.").