2017

# Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution

CDR Peter Pascucci

## Article

# Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution

**CDR Peter Pascucci, JAGC, U.S. Navy***

## Executive Summary

Cyberwar raises unique issues in the application of international humanitarian law ("IHL"). Numerous commentators and States have concluded that IHL applies to cyberwar, but the only detailed description of how IHL may be applied is in the Tallinn Manual.[1] However, the Tallinn Manual was written by an international group of experts, not States. Even under the Tallinn Manual application, the principles of distinction and proportionality fail to adequately protect civilians and civilian objects. Specifically, IHL is deficient in protecting civilians and civilian objects because: (1) the application and scope of the definition of what constitutes a civilian object versus military objective in cyberwar is unclear, particularly with respect to data and the functionality of cyber systems; (2) the definition of what constitutes an attack fails to adequately account for non-kinetic effects; (3) the definition of damage and the guidance for calculating damage in cyberwar is

---

* The author is an active duty judge advocate with the U.S. Navy and is a National Security Crisis Law fellow with the Center on National Security and the Law at Georgetown University Law Center. A previous version of this Article was submitted in partial fulfillment of the requirements of the award of the degree of Master of Laws from the Georgetown University Law Center. This Article was selected as the runner up for the 106 Lieber Society Richard R. Baxter Writing prize. The views expressed herein are solely those of the author and do not reflect the views or opinions of the Department of the Navy, the Department of Defense, or Georgetown University Law Center.

1. While the United States Department of Defense has published a Law of War manual that includes a cyberspace operations chapter, discussed further *infra*, the manual fails to offer the level of detail and certainty in opinion that is necessary to afford benefit to practitioners and comprehensive understanding to the international community. That being said, it is a significant step further than any other country has taken in detailing the analysis of the application of the law of armed conflict to cyberspace operations.

vague; and (4) there is a lack of guidance for assessing the extent to which indirect effects must be accounted in a proportionality analysis.

The principle of distinction requires a party to the conflict to target only other parties to the conflict—a party may not target a civilian or civilian object. Specifically, Article 48 of Additional Protocol I ("AP I") establishes this basic rule.[2] This foundational principle is further emphasized in Articles 51 and 52 of AP I to protect civilians and civilian objects.[3] Applying AP I to cyberwar yields results that simply do not provide adequate protection for civilians and civilian objects. This is a direct result of the unique and ubiquitous nature of cyber systems and the reliance on and use of civilian cyber systems by military forces. Additionally, the lack of identifiable standards or thresholds, such as the degree of fidelity required for future use of infrastructure for it to be targetable, further adds to the confusion. Moreover, data is not traditionally considered an "object."[4] Therefore, so long as an attack does not impair the underlying functionality of a system, but merely corrupts data, IHL offers inadequate protection. Finally, the definition of "attack" for purposes of IHL, as applied in cyberspace, is less than clear. Similar problems occur under the existing proportionality analysis.

Article 51 of AP I prohibits an 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 anticipated.[5] In cyberwar, the overarching question as to the success of the principle of proportionality in protecting the civilian population will largely turn on what the specific terms mean within the principle of proportionality, and how they are applied to cyber attacks. Thus, the definitional issues

2. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

3. *Id.* arts. 51, 52.

4. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 437 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL]. Of note, in February 2017, the authors of the Tallinn Manual published the second edition. The second edition focused on the application of international law to cyber activities during peacetime (i.e., those activities that fall short of the jus ad bellum threshold). In addition, there were some changes made to the rules and commentary from the original Tallinn manual.

5. Protocol I, *supra* note 2, art. 51.

associated with what constitutes a military object, as discussed with respect to distinction, pertain in the proportionality analysis as well. Additionally, there is no established collateral effect (damage) estimation methodology, causing all assessments to be subjective and largely inconsistent. Furthermore, it remains unclear to what degree knock-on or indirect effects must be considered.

The solution to these problems is Additional Protocol IV. While a new, comprehensive cyberspace treaty is neither necessary nor politically likely, a limited-in-scope additional protocol that seeks to clarify the definitions and application of key terms with respect to cyberwar is necessary, appropriate, and politically feasible. Specifically, Additional Protocol IV should clearly delineate what constitutes a civilian object versus a military objective in cyberspace, including how to calculate damage in cyberwar, and determine the scope and extent to which indirect or knock-on effects must be considered.[6] Additional Protocol IV will provide clarity and precision in terms that are vital to the success and consistent application of the IHL principles of distinction and proportionality.

## I. INTRODUCTION

"[S]upreme excellence consists in breaking the enemy's resistance without fighting."[7] Cyberwar offers the ability to subdue the enemy without engaging in traditional kinetic battles.[8] However, whether a cyber attack constitutes a *jus in bello* 'attack'[9] under IHL is one of the many aspects of international law that remains murky in the age of digital warfare. "Many difficult questions arise when trying to fit cyberspace within a warfare regime constructed long before even the most visionary policy makers imagined cyber weapons."[10] This Article will address the *jus in bello* principles of distinction

6. Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287 [hereinafter Protocol IV].

7. SUN TZU, THE ART OF WAR 11 (Lionel Giles trans., 2010).

8. *See generally* Matthew Borton, Samuel Liles & Sydney Liles, *Cyberwar Policy*, 27 J. MARSHALL J. COMPUTER & INFO. L. 303, 305 (2010) (defining cyberwarfare from an extrapolation of other terms as "any military operation designed to attack, deceive, degrade, disrupt, deny, exploit, and/or defend through the information infrastructure with a desired kinetic effect").

9. As distinguished from an 'attack' in the *jus ad bellum* construct.

10. Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 579 (2012).

and proportionality, as applied to cyberwar, and will demonstrate that the present structure of IHL and current interpretation fails to fulfill the spirit of adequately protecting civilians from the harms of war.

Part II of this Article will explore the current technology and its ubiquity, and the uncertain nature of law and policy in cyberspace. Part III analyzes cyberwar in the context of IHL, focusing on the principles of distinction and proportionality. After analyzing the shortcomings of the principles of distinction and proportionality in cyberwar in Part III, Part IV addresses possible solutions that establish clarity in applying the principles of IHL while upholding the spirit of protecting civilians from the harms of war. While some commentators have focused on when a State may resort to armed force, including in cyberspace, (i.e., *jus ad bellum*),[11] this Article focuses on the application of two key principles of IHL—distinction and proportionality—in an armed conflict where the methodology of attack is cyberwar. Therefore, the Article will not discuss the *jus ad bellum* analysis nor draw a distinction between an international armed conflict ("IAC") and a non-international armed conflict ("NIAC"), unless otherwise referenced. Finally, the principal use of cyberwar is against objects and, as such, this Article will not focus on the specific targeting of people. However, the impact of cyberwar on the civilian population will be addressed in the application of the principles of distinction and proportionality.

## II. CYBERSPACE: UBIQUITOUS AND UNCERTAIN

Any analysis of the application of the principles of IHL to a technology-based style of warfare must begin with a basic understanding of the technology at issue. "The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities."[12] Originally

11. *See, e.g.*, HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 118 (2012); William Banks, *The Role of Counterterrorism Law in Shaping* ad Bellum *Norms for Cyber Warfare*, 89 INT'L L. STUD. 157 (2013) (analyzing when cyberwar is justified in response to cyber terrorist attacks); Reese Nguyen, *Navigating* Jus Ad Bellum *in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079 (2013) (arguing a new framework to analyze whether the use of force is justified by shifting from an object-based definition of cyberwar).

12. BARRY M. LEINER ET AL., INTERNET SOC'Y, BRIEF HISTORY OF THE INTERNET 1 (2012) [hereinafter LEINER ET AL.], http://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf.

conceived as a way for academic researchers to share information, the internet, and by extension internets and networks, have transformed significantly over the past thirty years.[13] In an overly simplistic fashion, a network is comprised of computers, switches, routers, servers, printers, smart phones, and/or other devices that allow users to transmit, receive, and/or store information.[14] The Internet refers to the world-wide web and is the combination of all interconnected networks.[15] The transmission and receipt of information (i.e., data) across diverse platforms (i.e., computers, smart phones, etc.) relies upon the Transmission Control Protocol/Internet Protocol ("TCP/IP").[16] The TCP/IP protocol is what allows your Apple iPhone to talk seamlessly with your Samsung laptop, and to obtain information from a Cisco server.[17] This basic explanation of networking and technology, though oversimplified for a computer scientist, demonstrates the man-made nature of cyberspace, and the ease of interconnectedness. However, one need not possess a computer science degree to intelligently discuss the applicable principles of international humanitarian law to this technology. The technology is relevant to the discussion because of what it does: transmits, stores, and controls information. The nature of the technology and its integration into military systems leads to the likelihood of cyberwar.[18] "[V]irtually the U.S.'s entire infrastructure including dams, nuclear power plants, air-traffic control, communications, and financial institutions" rely on cyberspace.[19] But technology alone does not cause a commander to want to target something—it is what may be done with that technology, or what information resides on it, that leads to targeting.

---

13. *See id.* at 8.

14. *See What is a Network?*, FLA. CTR. FOR INSTRUCTIONAL TECH., http://fcit.usf.edu/network/chap1/chap1 (last visited Feb. 5, 2017).

15. *See What is the Internet?*, GOV'T AUSTL. DEP'T COMM., http://webarchive.nla.gov.au/gov/20150227175730/http://www.internetbasics.gov.au/getting_started_on_the_internet/what_is_the_internet# (last visited Feb. 19, 2017).

16. LEINER ET AL., *supra* note 12, at 4.

17. *See* Robert Sanchez, *What is TCP/IP and How Does it Make the Internet Work?*, HOSTINGADVICE.COM (Nov. 17, 2015), http://www.hostingadvice.com/blog/tcpip-make-internet-work/.

18. *See* DAVID S. ALBERTS, JOHN J. GARSTKA & FREDERICK P. STEIN, NETWORK CENTRIC WARFARE: DEVELOPING AND LEVERAGING INFORMATION SUPERIORITY (2d ed. 2000).

19. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 200 (2009).

The technological transformation and integration of capabilities has significantly increased the speed at which information is transferred and the ease of access to vast quantities of data.[20] "Across a broad range of activities and operations, the time required by individuals to access or collect the information relevant to a decision or action has been reduced by orders of magnitude . . . ."[21] This makes information warfare ever more likely because "[t]he increasing availability and affordability of information, information technologies, and Information Age weapons increases the potential for creating formidable foes from impotent adversaries."[22] This is evident in the pervasive nature of interconnectedness among military and civilian systems, and the reliance of the military on civilian infrastructure.[23] Critical national security and public safety systems are connected, including air traffic control, oil and gas pipelines, electrical generating and transmission systems, hospital systems, emergency services, transportation systems, GPS satellites, financial systems, agricultural systems, and other critical infrastructure.[24] The ubiquitous nature of cyberspace has branched out into consumer goods including refrigerators, microwaves, thermostats, watches, and other traditionally non-internet connected items—the "Internet of Things."[25] Thus everyday items, from appliances to vehicles to commercial systems, are networked and connected to the internet.[26] "As more and more information becomes digitised [sic] and bandwidth expands, societies have become increasingly reliant on networked and electronic information,"[27] thus significantly increasing the quantity of potential military objectives and the ease with which States and non-State actors may achieve objectives by cyber means. As a result, "cyberspace

20. *See* ALBERTS, GARSTKA & STEIN, *supra* note 18, at 15.

21. *Id.* at 16.

22. *Id.* at 19.

23. *Id.* at 59.

24. DINNISS, *supra* note 11, at 12–13; *see also* Exec. Order No. 13636, 3 C.F.R. § 217 (2014) (taking action to improve cybersecurity on critical infrastructure).

25. *See The Internet of Things (IoT) Starts with Intel Inside*, INTEL, http://www.intel.com/content/www/us/en/internet-of-things/overview.html ?cid=sem132p41961g-c&gclid=Cj0KEQjwlYqoBRDajuaTvsyq1PQBEiQ AEhSjnLm_Ziki856GKchA07tUq-cecD2SqtmIMhOvE56NGLQaAqZI8P8HAQ (last visited Feb. 5, 2017); *see also* INTERNET THINGS COUNCIL, http://www.the internetofthings.eu/ (last visited Feb. 5, 2017).

26. DINNISS, *supra* note 11, at 12.

27. *Id.*

has gone from being an ornament of interest to forming a real pillar in national security efforts."[28] It is these pillars that States will consider as potential military targets in the event of armed conflict. "Over 120 countries have developed information operations systems" (cyber attack capabilities).[29]

The explosion of technology and the dramatic increase in States developing cyberwarfare capabilities is not merely for future use. States have already engaged in warfare by cyber means. On a strategic level there are examples: Stuxnet[30] and the Russian-Georgian cyber conflict.[31] However, cyberwar has also been used on a more tactical level. The United States used tactical cyber operations in the war against ISIL and in Afghanistan. [32] According to Lt. General Richard Mills of the United States Marine Corps, in 2010 the United States used cyber operations to "get inside [the enemy's] nets, infect [the enemy's] command-and-control, and in fact defend [United States forces] against [the enemy's] almost constant incursions . . . " inside United States forces' networks, to affect United States' operations.[33] Thus, cyberwar may be used from the strategic level to the tactical level of warfare, all based upon desired effect and target selection.

---

28. PAUL ROSENZWEIG, AM. BAR ASS'N STANDING COMM. ON LAW AND NAT'L SEC. & NAT'L STRATEGY FORUM, NATIONAL SECURITY THREATS IN CYBERSPACE 10 (2009), http://www.americanbar.org/content/dam/aba/migrated/2011_build/law_national_security/threats_in_cyberspace_report.authcheckdam.pdf.

29. Jeremy Richmond, Note, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842, 846 (2012).

30. *See, e.g.*, David E. Sanger, *Obama Order Sped Up Wave of Cyber Attacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (describing the attacks on Iran's nuclear enrichment facilities).

31. *See, e.g.*, Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 LOY. L.A. INT'L & COMP. L. REV. 303, 305 (2010) (detailing the Russian-Georgian cyber conflict).

32. *See* Press Release, Ash Carter, Sec'y of Defense, Department of Defense Press Briefing (Feb. 29, 2016) (transcript available at https://www.defense.gov/News/Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the); Tom Fox-Brewster, *Cyber-Warfare: Who's Afraid of the Big Red Button?*, INFOSECURITY MAG. (Oct. 31, 2014), http://www.infosecurity-magazine.com/magazine-features/cyber warfare-whos-afraid-of-the/.

33. Fox-Brewster, *supra* note 32 (quoting Lieutenant General Richard Mills of the United States Marine Corps).

Despite the prevalence and importance of cyberspace in national security affairs, the applicable international law, and more importantly, the precise application of the relevant provisions of international law, remain unclear.[34] Existing international treaties relating to or impacted by cyber operations do not specify how they apply in the event of an armed conflict.[35] Publicly, the United States declared that the same principles of law and policy that govern kinetic operations govern cyber operations.[36] However, when asked specifically how they apply, Admiral Michael Rogers, now Commander of United States Cyber Command, provided a generalized answer that did not directly answer the question. Specifically, Admiral Rogers was asked by the Senate Armed Services Committee,

> Has the Department of Defense determined how the laws of armed conflict (including the principles of military necessity in choosing targets, proportionality with respect to collateral damage and unintended consequences, and distinguishing between combatants and non-combatants) apply to cyber warfare, with respect to both nation-states and non-state entities (terrorists, criminals), and both when the source of an attack is known and unknown?[37]

Admiral Rogers responded, "[p]er [Department of Defense] guidance, all military operations must be in compliance with the

---

34. *See* Borton, Liles & Liles, *supra* note 8, at 304–05 (stating that experts disagree on the range and scope of cyberwarfare and that there are calls for policy as well as conflicting views of existing policy); *see also* Swanson, *supra* note 31, at 305 (stating that existing principles of international law need to be applied in new ways and old tenets reconsidered).

35. *See* Shackelford, *supra* note 19, at 198–99 (discussing how a cyber attack could implicate provisions of, inter alia, the International Telecommunications Union, matters of copyright infringement, and UNCLOS articles 19 and 113, and how these provisions do not specify the way they apply to armed conflict or lack enforcement mechanisms).

36. OFFICE OF GEN. COUNSEL, U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 16.2 (2015) [hereinafter DOD LAW OF WAR MANUAL]; Harold Hongju Koh, Legal Advisor, U.S. Dep't of State, International Law in Cyberspace 3 (Sept. 18, 2012) (transcript available at http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf).

37. U. S. SENATE COMM. ON ARMED SERVS., ADVANCE QUESTIONS FOR VICE ADMIRAL MICHAEL S. ROGERS, USN NOMINEE FOR COMMANDER, UNITED STATES CYBER COMMAND 14 (2014), http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf [hereinafter ADVANCE QUESTIONS].

laws of armed conflict-this includes cyber operations. The law of war principles of military necessity, proportionality and distinction will apply when conducting cyber operations."[38] The reason for the lack of a precise response to the foregoing question is unclear. In 2015, the United States Department of Defense ("DOD") published a manual on the Law of War that includes a chapter dedicated to cyber operations.[39] Even though an important first step for the United States DOD, the manual dedicates only six pages to the application of *jus in bello* principles to cyberspace operations.[40] Although indicative of DOD's intent, the content on these six pages does not definitively clarify the application of these principles to be of practical use to practitioners. Nor do these six pages provide any degree of certainty to the international community as to how, precisely, the United States will interpret its international obligations. Nevertheless, there are no internationally agreed-upon set of rules for cyberwar.[41] Even the framework for discussing the application of international law to cyberwar remains elusive. As recently as 2014, representatives at the United Nations were still calling for States to agree on "specific transparency and confidence-building measures."[42] Additionally, in 2014, the European Union referred to the lack of precise definitions and policy pertaining to cyberwar as a "black hole."[43] Most recently, in November 2016 at University of California Berkeley, Brian Egan, Legal Advisor at the United States State Department, built upon the 2012 Harold Koh speech regarding the application of the Laws of Armed Combat ("LOAC") in cyberwar. Egan's speech, too, failed to provide any meaningful clarification or insight of specific positions of the United States on the application of specific *jus in bello* principles.[44]

---

38. *Id.*; *see also* DOD LAW OF WAR MANUAL, *supra* note 36, § 16.2.

39. *Id.* at 994–1006.

40. *Id.* at 1003–08.

41. Fox-Brewster, *supra* note 32.

42. Press Release, General Assembly, Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment, U.N. Press Release GA/DIS/3512 (Oct. 28, 2014).

43. CARMEN-CRISTINA CIRLIG, CYBER DEFENCE IN THE EU: PREPARING FOR CYBER WARFARE? 3 (Oct. 2014), http://www.europarl.europa.eu/RegData/etudes/BRIE/2014/542143/EPRS_BRI(2014)542143_REV1_EN.pdf.

44. *See* Brian Egan, Legal Adviser, U.S. Dep't of State, Remarks on International Law and Stability in Cyberspace 3–5, (Nov. 10, 2016) (transcript available at https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf);

Despite the uncertainty of the precise application of existing international law, the number of countries engaged in or preparing to engage in cyberwar has increased dramatically to 100 countries developing cyber military commands.[45] These countries include "about 20 that are serious players, and a smaller number could carry out a whole cyberwar campaign."[46] Seemingly, the only progress in defining precise terms and exacting an explanation of the application of IHL in cyberwar comes from the Tallinn Manual.[47] However, the Tallinn Manual reflects the work of an international group of experts—not the efforts of States that are the principal architects of international law and would be the primary actors in cyberwar.[48] Additionally, in numerous topics within the Tallinn Manual, even the experts could not reach a consensus or agreement on precise tactical applications of IHL principles.[49]

The lack of clear and well-defined international law is particularly troubling as more State and non-State actors engage in conduct through cyberspace.[50] This is a direct result of the low costs associated with the entry and ability to reach world-wide without leaving the safety and security of one's territory.[51] Finally, the technology allows a State or non-State group to obfuscate—to varying degrees depending upon whom you believe—its actual identity when engaging in cyber operations, thus furnishing anonymity of the actor.[52]

---

*see also* Michael Schmitt, *U.S. Transparency Regarding International Law in Cyberspace*, JUST SECURITY (Nov. 15, 2016, 9:11 AM), https://www.justsecurity.org/34465/transparency-international-law-cyberspace/ (providing additional analysis on Brian Egan's remarks).

45. Steve Ranger, *Inside the Secret Digital Arms Race: Facing the Threat of a Global Cyberwar*, TECHREPUBLIC (Apr. 25, 2014), http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/.

46. *Id.*

47. *See* TALLINN MANUAL, *supra* note 4.

48. *Id.* at 2.

49. *See* Kristen E. Eichensehr, Book Review, 108 AM. J. INT'L L. 585, 586 (2014) (reviewing TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013)).

50. Ranger, *supra* note 45; Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, 89 INT'L L. STUD. 406, 407 (2013).

51. *See* Swanson, *supra* note 31, at 304; Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 897 (1999).

52. *See* Shackelford, *supra* note 19, at 200–01 (discussing the practical and fundamental problem of attribution); Koh, *supra* note 36, at 6. *But see* ADVANCE QUESTIONS, *supra* note 37, at 19 (stating attribution is improved but is not timely in many circumstances).

Despite the advancing technology and uncertainty with the precise application of international law, there is consensus among States and experts that principles of international law, including IHL in situations of armed conflict, apply to actions in cyberspace.[53] However, there is little consensus on how international law, and IHL in particular, will apply to cyberwar in practice.[54]

## III. CYBERWAR AND INTERNATIONAL HUMANITARIAN LAW

### A. OVERVIEW OF IHL

"The laws of armed conflict apply to all situations of armed conflict, whether or not war is declared, and regardless of whether the parties involved recognise [sic] the state of armed conflict or, indeed, the opposing force."[55] Although the preceding statement seems unambiguous, as with many aspects of law applied to cyberwar, the determination that IHL applies to cyberwar is not without question.[56] This is, in part, due to the fact that no specific provision in IHL expressly applies to cyberwar.[57] Presently, the International Committee of the Red Cross ("ICRC"), a majority of international experts, and a growing number of States have concluded that, when engaged in an armed conflict, IHL applies to cyber attacks.[58] However,

53. *See* TALLINN MANUAL, *supra* note 4, at 2, 375; U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Section VI. ¶ 28(d), U.N. Doc. A/70/174 (July 22, 2015) (stating that as a matter of international law, principles of humanity, necessity, proportionality, and distinction apply to information and communications technology, i.e., cyberwar); Koh, *supra* note 36, at 2–3.

54. *See generally* TALLINN MANUAL, *supra* note 4, at 2–6 (describing generally the process by which the international group of experts drew conclusions as to exact applications or scope of a treaty and its applicability to cyber space); U.N. Secretary-General, *supra* note 53, at Sec. III ¶ 9 ("The ICT environment offers . . . challenges to the international community in determining how norms, rules and principles can apply to State conduct of ICT-related activities.").

55. DINNISS, *supra* note 11, at 117.

56. *Id*. at 126.

57. Richmond, *supra* note 29, at 847.

58. *See* DINNISS, *supra* note 11, at 126, 128, 137; DOD LAW OF WAR MANUAL, *supra* note 36, § 16.2; TALLINN MANUAL, *supra* note 4, at 375; Jody M. Prescott, *The Law of Armed Conflict and the Responsible Cyber Commander*, 38 VT. L. REV. 103, 109–11 (2013) (describing that in addition to the United

conspicuously absent from any of the pronouncements (except for the Tallinn Manual), is a detailed description of how IHL shall apply. Therefore, before analyzing specific IHL principles in the cyberwar paradigm, one must first look at the key IHL principles and the underlying purpose of IHL.

### B. DISTINCTION IN CYBERWAR

Although the premise remains that all principles of IHL are applicable in cyberwar, the application of the principle of distinction raises unique issues. This section explores the principle of distinction, the application of distinction in cyberwar, and the specific attributes of the principle of distinction that, as applied, fail to adequately protect civilians.

#### 1. General Description of Distinction

Distinction is a seminal principle in international humanitarian law.[59] The International Court of Justice ("ICJ") has characterized the principle of distinction as "intransgressible."[60] Additionally, the principle of distinction is considered customary international law and applicable in both international and non-international armed conflicts.[61] The principle of distinction requires a party to the conflict to only target other parties to the conflict—a party may not target a civilian or civilian object.[62] Specifically, Article 48 of AP I

States, the United Kingdom and the Netherlands apply the Law of Armed Conflict (i.e. IHL) in cyberwar but China is reluctant to state that IHL applies); Adam Segal, *China, International Law, and Cyberspace*, COUNCIL ON FOREIGN REL. (Oct. 2, 2012), http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/ (explaining the United Kingdom, as well as the United States, applies existing international humanitarian law, but China, Russia, Tajikistan, and Uzbekistan believe a new treaty is required); Cordula Droege, *No Legal Vacuum in Cyber Space*, INT'L COMM. RED CROSS (Aug. 16, 2011), https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm; Koh, *supra* note 36, at 2–3 (stating that the Law of Armed Conflict (i.e. IHL) applies to cyber attacks).

59. Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, HARV. NAT'L SECURITY J. (Feb. 5, 2013, 2:07 PM), http://harvardnsj.org/2013/02/autonomous-weapon-systems-and-international-humanitarian-law-a-reply-to-the-critics/.

60. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 226, ¶¶ 78, 79 (July 8).

61. JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW VOLUME I: RULES 3 (2009).

62. Laurie Blank & Amos Guiora, *Teaching an Old Dog New Tricks:*

establishes the general rule: "[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[63] Article 48 sets a foundational rule upon which the protection of civilians from the harms of hostilities is based. This foundational principle is further emphasized in Article 52(1) which is designed to protect civilian objects.[64]

Civilian objects are those that are not military objects.[65] Article 52 defines military objects as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[66] Thus, Article 52 espouses a two-part test for determining the lawfulness of an object as a military object: (1) objectively, the nature, location, purpose, or use must make an effective military contribution; and (2) the destruction, capture, or neutralization, under the circumstances at the time, must offer a definite military advantage.[67]

2. Application of Distinction to Cyber Warfare

*a. Military Objectives vs. Civilian Objects*

While the principle of distinction appears straight-forward, its application to cyberwar is ambiguous. In cyberwar, increased reliance on civilian and commercial facilities and equipment blurs the distinction between civilian objects and military

*Operationalizing the Law of Armed Conflict in New Warfare*, 1 HARV. NAT'L SECURITY J. 45, 54 (2010).

63. Protocol I, *supra* note 2, art. 48.

64. *Id.* art. 52(1). While Article 51(2) of AP I further details the rule espoused in Article 48 with respect to the civilian population, because the specific targeting of civilians (i.e., individuals, as opposed to objects) by cyberwar is not a focus of this Article, the analysis of the principle of distinction will not significantly rely upon Article 51.

65. *See id.* art. 52(1).

66. *Id.* art. 52(2).

67. *See id.* art. 52; *see also* Robin Geiß & Henning Lahmann, *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space*, 45 ISR. L. REV. 381, 387 (2012).

objectives, and thus the initial determination of lawfulness.[68] In this regard, the key is the nexus between the military objective and the object a commander seeks to attack. This is where the nature of cyberspace—the interconnectedness, built-in resiliency of the communications pathways, and the reliance on civilian systems and off-the-shelf hardware and software—complicates the analysis.[69]

Further complicating the distinction analysis is the nature of data. Whether data, per se and regardless of nature, location, purpose, or use, may be considered an object—let alone characterized as either a military objective or civilian object—remains in controversy.[70] While the literature fails to identify any State's position with respect to data as a potential "object," a majority of experts involved in the creation of the Tallinn Manual concluded that for the purposes of IHL data should not, in most cases, be considered an object.[71] The Tallinn Manual reaches this conclusion by viewing data as "intangible," and therefore outside the "ordinary meaning of the term object."[72] The experts further opined that inclusion of data as an object would not comport with the ICRC Commentary on the Additional Protocols.[73] Thus, a cyber operation directed at manipulating, destroying, or corrupting data resident on a computer or cyber system that does not affect functionality of the computer or system itself does not constitute an attack on an object. [74] This seemingly expansive gap in what constitutes an object is minimally limited by the experts' conclusion that a cyber operation targeting data that affects the functionality of computers or cyber systems may "sometimes" qualify as an attack.[75] In an information-driven society, such as the United States, this gap could have a profound effect, especially if it means that an action that results in corruption or destruction of

68. *See* Richmond, *supra* note 29, at 875.

69. *See* Geiß & Lahmann, *supra* note 67, at 388.

70. Michael N. Schmitt & Eric W. Widmar, *"On Target": Precision and Balance in the Contemporary Law of Targeting*, 7 J. NAT'L SECURITY L. & POL'Y 379, 395 (2014); *see also* Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, 89 INT'L L. STUD. 252, 268–269 (2013).

71. TALLINN MANUAL, *supra* note 4, at 437.

72. *See id*. (citing the Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, reprinted in 8 I.L.M. 679 (entered into force Jan. 27, 1980)).

73. *See id.*

74. *See generally infra* Part III C.2a for additional discussion on functionality.

75. *See* TALLINN MANUAL, *supra* note 4, at 437.

all the data on a civilian computer or cyber system, except for the operating system and functionality supporting software, is outside the scope of the principle of distinction.

There is little doubt that "[m]ilitary objectives in cyberspace can include computers, computer networks, and other tangible components of cyber infrastructure . . . ."[76] In fact, "[m]ilitary use of a computer has to be understood in its widest possible meaning, running the whole gamut from the plotting of attacks—through the crunching or storage of military data and the encryption or deciphering of codes—to plain administrative military tasks."[77]

*b. Contribution to Military Action*

Applying the principle of distinction to cyberwar, one must distinguish between civilian objects and military objectives. In other words, a proposed attack must target an object that has an "inherent characteristic or attribute which contributes to military action."[78] Focusing on the second aspect of the definition of a military objective, the "effective contribution" of the object "need not be critical, or even significant" so long as it contributes to military action.[79] While this is generally accepted as a matter of customary international law, the scope of the "contribution to military action" standard varies.[80] War-fighting objects are objects used for combat that are usually military in nature.[81] In the cyber context, a war-fighting object would include the computer guidance system in a weapon or the classified network on which military operations are planned and executed. "War-supporting objects are those used to directly buttress the war effort . . . ."[82] This would include the factory that makes the computer guidance system for a weapon or the proprietary software for a classified network. "There is universal agreement that war-fighting and war-supporting objects can qualify as military objectives on [the bases of nature, location, purpose, or

76. *See* Schmitt & Widmar, *supra* note 70, at 395.

77. Yoram Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, 17 J. CONFLICT & SECURITY L. 261, 263 (2012).

78. Schmitt & Widmar, *supra* note 70, at 392.

79. *Id.* at 391.

80. *See* DINNISS, *supra* note 11, at 188.

81. *See* Schmitt & Widmar, *supra* note 70, at 393.

82. *Id.* at 394.

use]."[83] However, and of particular relevance in the cyberwar context, the United States includes war-sustaining objects as lawful military objectives.[84] The U.S. Commander's Handbook on the Law of Naval Operations defines war-sustaining objects as "economic objects of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability . . . ."[85] This bears a significant impact with respect to cyberwar.[86] By dramatically increasing the number of potentially valid military targets that comport with the principle of distinction, the United States and those States that may adopt the war-sustaining interpretation undercut the protection offered by IHL to the civilian population. While the interpretation of war-sustaining objects as potential military objectives in cyberwar was rejected in the Tallinn Manual,[87] it remains the practice of the United States in the kinetic context and would reasonably continue to be so in the cyberwar context as well.

However, use of the Internet and cyber systems by military personnel does not ipso facto make them a proper object of attack. Military use of computers and cyber systems may be for non-hostilities related purposes.[88] These uses may include email and phone services to communicate with family members or pay bills.[89] The experts drafting the Tallinn Manual did not reach consensus on whether such use of civilian systems subjected the systems to attack.[90] The debate focused on whether morale of the troops constitutes a military advantage, with the majority of

---

83. *Id.*

84. *See id.*

85. THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 8-3 (July 2007), http://www.jag.navy.mil/documents/NWP_1-14M_Commanders_Handbook.pdf; *see also*, 10 U.S.C. § 950p(a)(1) (2015) (defining a military objective for military commissions as including war-sustaining capabilities). *But see* Yoram Dinstein, *Legitimate Military Objectives Under the Current* Jus In Bello, 78 INT'L L. STUD. 139, 145–46 (stating that war sustaining objects do not qualify as military objectives).

86. *See, e.g.*, DINNISS, *supra* note 11, at 189 ("[T]he US targeting of war-sustaining capabilities moves the target of military operations away from military effort of the enemy and onto the political command and control system and its resource base . . . .").

87. *See generally* TALLINN MANUAL, *supra* note 4, at 441 (rejecting the notion that war-sustaining objects are military objectives when applied to the cyberwar arena).

88. *See id.* at 444.

89. *Id.*

90. *See id.*

experts concluding it does not constitute an advantage that would subject the otherwise civilian cyber systems to targeting.[91]

*c. Nature, Location, Purpose, and Use*

The second portion of the first prong looks at the characterization of the object. In the cyber context, "[t]he key words here are 'nature, location, purpose, or use.'"[92] In cyberwar, distinguishing between nature, location, use, and purpose may be particularly difficult given the nature of cyberspace.

"The 'nature' of a military objective refers to its 'inherent characteristic or attribute which contributes to military action.'"[93] Military networks, long-haul communication systems used by the military, and the computer systems in weapons are all, by their nature, valid military objects in the context of cyberwar.

"Location" refers to geography that is of special importance to the military action.[94] While one may think of cyberspace in the abstract, the servers, routers, switches, and computers that comprise networks all physically reside somewhere. Therefore, location may be achieved by noting that a particular router or switch connects to a military air defense radar, or that the likely communications pathway for a certain piece of data is to transit a particular network, based upon the particular software and services used to transmit the data. Additionally, "there may be circumstances where it is important to deny a network or other object to the enemy where its location does play a role in computer network attacks"[95] (e.g., a civilian wireless network upon which the military is piggy-backing). Similarly, an attack on a SCADA system that results in water being released from a dam and denying an area to the adversary may qualify as a military objective under the location test because, while the land area is the actual object of attack, the SCADA system is merely the means to deny the location to the adversary.[96]

"'[U]se' pertains to how an object is currently being employed."[97] "The criterion applies in the case of civilian objects

91. *See id.*
92. Dinstein, *supra* note 77, at 263.
93. Schmitt & Widmar, *supra* note 70, at 392.
94. *Id.*
95. DINNISS, *supra* note 11, at 185–86.
96. *See, e.g.*, TALLINN MANUAL, *supra* note 4, at 438.
97. Schmitt & Widmar, *supra* note 70, at 393.

that are being used for military purposes, but only during the period of use."[98] In cyberwar, it is rare that the use of a cyber objective or infrastructure would transition exclusively from civilian to military. This is a direct result of the architecture of networks and cyber systems, as discussed in Part II. Rather, the more likely, and arguably harder determination, is whether the targeting of a dual-use cyber object, one that serves both a civilian and a military purpose, complies with the principle of distinction. Of note, the dual-use may occur simultaneously, as in the case of a server hosting both a civilian website and a military propaganda website. This is particularly complicated because "most Internet infrastructure can serve as a dual-use object because military systems are so often interwoven with civilian infrastructure."[99]

By way of example, "the US military's global communications backbone consists of seven million computing devices on thousands of networks across hundreds of installations" spread around the world.[100] As stated in Part II, cyberspace is man-made. The majority of the infrastructure that comprises it was funded through private investment and its use is predominantly private.[101] Additionally, the nature of the TCP/IP algorithm causes even military communications to be separated into data packets, "all of which may travel via different (civilian) channels and typically traverse various civilian systems . . . ."[102] That is not to say that an attack against dual-use infrastructure is unlawful. It is widely accepted in IHL that a dual-use object is a lawful military objective for the purpose of targeting regardless of the extent of the military use.[103] This interpretation of dual-use objects was affirmed in the cyberwar context by the international group of experts that drafted the Tallinn Manual and is implicitly recognized in the United States DOD Law of War manual.[104] Thus in cyberwar, significant components of the Internet and cyber systems qualify as a dual-use objects.

---

98. *Id.*

99. Gervais, *supra* note 10, at 568.

100. *Id.*

101. *See id.* at 568.

102. Geiß & Lahmann, *supra* note 67, at 385.

103. *See* Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 298 (2014).

104. *See* DOD LAW OF WAR MANUAL, *supra* note 36; TALLINN MANUAL, *supra* note 4, at 435–48.

Also complicating the 'use' standard is the widespread production of computers and cyber systems that are not specifically intended for the military but which are frequently used by military forces.[105] In analyzing the 'use' standard, the experts drafting the Tallinn Manual agreed that "whether such a factory [i.e., computer production facility] qualifies as a military objective by use depends on the scale, scope, and importance of the military acquisitions . . . ."[106] However, the drafting experts were unable to determine any precise thresholds, leaving little clarity to the standard to apply.[107]

"'Purpose' denotes the intended future use of the object."[108] There is no requirement to wait for cyber infrastructure to actually be used before it may be a lawful military object.[109] So long as a State has reason to believe its adversary intends to use the cyber infrastructure for military purposes, even at a later date, the purpose criterion is satisfied.[110] Therefore, if a State has intelligence that the adversary is about to purchase specific computer hardware or software that will make a military contribution, or use a particular civilian satellite provider for such a purpose, those objects are then legitimate military objectives.[111]

The issues surrounding 'purpose' are highlighted by the recent use (e.g., command and control, propaganda, inciting violence) of social media (e.g., Facebook, Twitter, etc.) by parties to a conflict.[112] Therefore, one may reasonably conclude that Facebook and Twitter may be properly classified as military objectives subject to cyber attack. [113] In addressing the potential targeting of social media, the experts drafting the Tallinn Manual concluded that only those portions of Facebook and

105. TALLINN MANUAL, *supra* note 4, at 439.

106. *Id*. at 439.

107. *See id*.

108. Schmitt & Widmar, *supra* note 70, at 393.

109. *See* Geiß & Lahmann, *supra* note 67, at 385; *see also* TALLINN MANUAL, *supra* note 4, at 439–40.

110. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 99–100 (2d ed. 2010); *see also* Schmitt & Widmar, *supra* note 70, at 392 (discussing the ability to deduce intended use based upon intelligence collection).

111. *See* TALLINN MANUAL, *supra* note 4, at 439.

112. *Id*. at 446.

113. However, as will be discussed *infra*, one must first consider whether an operation against Facebook or Twitter would even rise to the level of an 'attack' under IHL. *Id.*

Twitter used for military purposes may be attacked.[114] Nevertheless, at least significant portions of popular social media sites may lawfully be subject to cyber attack for the purpose of disrupting enemy command and control and for countering propaganda.

IHL does not, however, provide any standards of reliability of information or likelihood of use.[115] Therefore, considering the nature of the technology, as discussed in Part II, and the application of the 'purpose' analysis from IHL—reason to believe there is intended future military use—there are a significantly greater number of civilian objects that may lawfully be attacked as military objectives in cyberwar. Furthermore, because there is no threshold of reliability of intelligence or certainty standard for future use, this leaves open a large number of civilian objects to the subjective decision-making of military commanders.

*d. Military Advantage from Destruction, Capture, or Neutralization*

The second prong of the definition of a military objective states that the destruction, capture, or neutralization of the object, under the circumstances at the time, must offer a definite military advantage.[116] While there is no specific significance associated with the use of the word "definite," some commentators have concluded that it requires the military advantage to be "concrete and perceptible" as opposed to "hypothetical and speculative."[117] Potential or indeterminate advantages are insufficient to meet the standard.[118] Additionally, the advantage gained must be military in nature and is assessed by reference to the advantage gained from the attack as a whole, not just from parts or portions of an attack.[119] For example, an attack on one transmission tower that is part of a broader attack on command and control networks would be viewed as a single, all-encompassing attack on command and

114. *Id.*

115. *Id.* at 439.

116. Geiß & Lahmann, *supra* note 67, at 387.

117. DINNISS, *supra* note 11, at 190; DINSTEIN, *supra* note 110, at 106.

118. CLAUDE PILLOUD ET AL., INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 636 (Yves Sandoz et al. eds., 1987) [hereinafter AP I COMMENTARY].

119. DINNISS, *supra* note 11, at 191; *see also* TALLINN MANUAL, *supra* note 4, at 131.

control for the purpose of determining the military advantage.[120] Furthermore, the military advantage analysis focuses on the "commander's intent in determining whether or not an object constitutes a military objective rather than actual effect as determined subsequently."[121] In other words, the attack cannot be designed purely to achieve a political advantage, although the attack may provide a political benefit in addition to military advantage.[122] As Dinniss notes, in the age of cyberwar, "the individual targeting of small parts of an integrated system will accumulate to contribute to a military advantage that would not necessarily eventuate from neutralising [sic] a single part of the system."[123]

Targeting a military computer system that will only disable or destroy the system or otherwise impact only the system, and not otherwise affect civilians or civilian objects (including civilian systems), will not violate the principle of distinction. Similarly, targeting a civilian academic research computer system that has no current or future military use and is not otherwise part of any war-fighting or war-supporting effort will clearly violate the principle of distinction. Unfortunately, modern computer systems and the interconnected nature of networks, as discussed in Part II, rarely yield such bright-line distinctions.

3. General Precautions and Discrimination

In addition to, but separate from, the technical distinction analysis are the requirements of general precautions and discrimination. Under Article 57 of AP I, when there is a choice between several military objectives for obtaining a similar military advantage, the attacker must select the objective which "may be expected to cause the least danger to civilian lives and to civilian objects."[124] More specifically, Article 57 requires those who plan and authorize attacks to: (1) do everything feasible to

120. *See* ICTY, *Final Report of to the Prosecutor of the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia*, ICTY (2000) ¶¶ 72, 78, http://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal.

121. DINNISS, *supra* note 11, at 193.

122. DINSTEIN, *supra* note 110, at 107.

123. DINNISS, *supra* note 11, at 191–92.

124. Protocol I, *supra* note 2, art. 57(3).

ensure the object of the attack is a military objective and not otherwise protected under the Protocol; (2) take all feasible precautions in the choice of means and methods to avoid or at least minimize incidental loss of civilian life, injury to civilians, and damage to civilian objects; and (3) refrain from launching an 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."[125] In this regard, Article 57 "requires attackers to take 'constant care' and 'all reasonable precautions' to spare the civilian population and civilian objects."[126]

AP I further delineates indiscriminate attacks in Article 51(4). Specifically, attacks that: (1) "are not directed at a specific military objective," (2) "employ a method or means . . . which cannot be directed at a specific military objective," or (3) "employ a method or means . . . the effects of which cannot be limited as required by this Protocol" violate IHL.[127] The second prong of Article 51(4) requires States to employ cyber weapons that are capable of distinguishing between military objectives and civilian objects.[128] In this regard, the cyber weapon must be able to discriminate between the two types of objects—civilian and military. Therefore, a commander has complied with the rule so long as the commander and his or her subordinates have taken "reasonable precautions," employed a cyber weapon that is capable of "discrimination," and targeted a valid military objective, even if the cyber weapon unexpectedly malfunctions or goes awry and attacks civilian objects.[129] However, if the cyber weapon is unable to be limited in retransmission or otherwise limited in the scope as to which cyber systems it attacks, either through built-in code or additional intervention, then the weapon is indiscriminate and prohibited.[130]

Building upon the difficulties detailed above, as a general proposition, a cyber attack is often preferable to a kinetic strike in that it is assumed a cyber attack generally will cause less

125. *Id.* art. 57(2)(a)(i)–(iii).

126. Gervais, *supra* note 10, at 569.

127. Protocol I, *supra* note 2, art. 51(4).

128. *See id.*

129. *Id.* art. 57.

130. *See* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus In Bello,* 84 INT'L REV. RED CROSS 365, 389 (2002).

physical damage and fewer civilian deaths.[131] "When a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be [the one] . . . expected to cause the least damage to civilian lives and to civilian objects."[132] Therefore, on a macro scale, applying the third section of Article 57 and assuming a cyber attack is less likely to result in physical injury, destruction, or death, a cyber attack will almost always be preferable to a kinetic strike. But, on a micro scale, "[m]ilitary systems are usually more secure than civilian systems."[133] Therefore, recalling the technology discussion from Part II and the interconnected nature of military and civilian systems, it is easier to launch a cyber attack against civilian infrastructure the military relies on (i.e., dual-use systems or systems that meet the 'purpose' standard under the description of a military objective) than to launch a cyber attack against purely military cyber infrastructure.[134] This may have the unintended result of increasing the adverse impacts of war on the civilian population. This risk is recognized in the DOD Law of War manual in that it notes the "obligation to take feasible precautions may be of greater relevance in cyber operations . . . because this obligation applies to a broader set of activities than those to which other law of war rules apply."[135] While the requirement to take feasible precautions applies, the general requirement does not offer the same degree of protection for civilian objects as application of the principle of distinction.

### 4. What Constitutes an Attack Under International Humanitarian Law?

One must note that the term "attack" as used in IHL is fundamentally different from the traditional notion of a cyber attack. In a colloquial sense, the term "cyber attack" has a broad meaning and encompasses everything from cyber espionage and hacking, to a denial of service attack or a complicated cyber attack designed to destroy an object or cause it to be destroyed

131. *See* Gervais, *supra* note 10, at 570.
132. Protocol I, *supra* note 2, art. 57(3).
133. Gervais, *supra* note 10, at 570.
134. *Id*.
135. DOD LAW OF WAR MANUAL, *supra* note 36, § 16.5.3.

(e.g., Stuxnet).[136] Additional definitions of cyber attack can be found in academic literature.[137]

In IHL, the term "attack" has a specific meaning and is the subject of regulation under applicable treaties. Article 49 of Additional Protocol I defines attacks as "acts of violence against the adversary."[138] Of note, Article 49 applies to "all attacks in whatever territory conducted."[139] Additionally, Article 49 applies to air, sea, and land warfare which may affect individual civilians, the civilian population or civilian objects on land.[140] Further, Article 52 of Additional Protocol I states that civilian objects may not be the "object of attack."[141]

The Tallinn Manual concluded that, for a cyber operation to be subject to the targeting rules under IHL, the operation must constitute an attack.[142] Similarly, the DOD Law of War manual also concludes that cyberspace operations amounting to an attack are subject to the principles of IHL, including distinction and proportionality.[143] Therefore, cyber operations that fall short of the definition of an attack are not governed by the IHL principles of distinction and proportionality.[144] The Tallinn

136. *See* Blank, *supra* note 50*; see also* Bob Violino, *Unseen, All-Out Cyber War on the U.S. Has Begun*, INFOWORLD (January 28, 2013), http://www.infoworld.com/article/2612825/hacking/unseen--all-out-cyber-war-on-the-u-s--has-begun.html; Lubell, *supra* note 70, at 255.

137. *See, e.g.,* Gervais, *supra* note 10, at 533 ("The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political, or similar objectives. Or to intimidate any person in furtherance of such objectives.") (citing U.S. ARMY TRAINING & DOCTRINE COMMAND, DCSINT HANDBOOK NO. 102, CRITICAL INFRASTRUCTURE THREATS AND TERRORISM, VII-2 (2006)); Lubell, *supra* note 70, at 255; Gary D. Solis, *Cyber Warfare*, 219 MIL. L. REV. 1, 3 (2014); Jeffrey T.G. Kelsey, Note, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1443 (2008);. *Cf.* DOD LAW OF WAR MANUAL, *supra* note 36, § 16.5.2 (providing examples of what would NOT constitute an attack).

138. Protocol I, *supra* note 2, art. 49.

139. *Id.* art. 49(2).

140. *Id.* art. 49(3).

141. *Id.* art. 52.

142. TALLINN MANUAL, *supra* note 4, at 423.

143. DOD LAW OF WAR MANUAL, *supra* note 36, § 16.5.1.

144. However, as detailed in Article 52 of AP I, and as the Tallinn Manual recognizes in Rule 114, there are other generally applicable protections in effect during all cyber operations that are designed to spare the civilian population from unnecessarily suffering the effects of military operations. *See* TALLINN MANUAL, *supra* note 4, at 477; DOD LAW OF WAR MANUAL, *supra* note 36, § 16.5.1.

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."[145] The Tallinn Manual notes that the term "acts of violence" in the definition of attacks in Article 49(1) of AP I should not be read as limited to kinetic action; rather it is the nature of the effect caused by the action that determines if it is an attack.[146] In this regard, the determination of whether a cyber operation constitutes an attack is an effects-based analysis. The Manual states that the focus must be on the consequences of an operation rather than on its nature.[147] Therefore, cyber espionage, psychological operations, and other non–violent operations (i.e., operations that do not result in kinetic-like effects) do not constitute attacks.[148] That is not to say that all effects which cause damage or destruction amount to an attack under IHL. *De minimis* damage or destruction does not rise to the level of harm required.[149] Thus, the focus of the definition of a cyber attack, for the purposes of IHL and this Article, is whether the effect can reasonably be expected to cause more than *de minimis* damage to or destruction of objects.[150] Because determination of whether an action constitutes a cyber "attack" is an effects-based determination, an operation targeting data that "results in the . . . damage or destruction of physical objects . . . qualifies as an attack."[151] However, targeting that results in *de minimis* damage or no loss of functionality is not an attack and, therefore, all the protections afforded civilian objects subject to an attack by the principles of distinction and proportionality do not apply.[152]

Additional Protocol I uses the term "attack," as well as the term "operation," in describing actions taken against military

145. TALLINN MANUAL, *supra* note 4, at 415.

146. *Id*. at 415–16.

147. *Id*. at 415.

148. *Id*.. The Tallinn Manual relies on the International Court of Justice's decision in *Tadic*, which stated, inter alia, that chemical, biological, and radiological attacks do not usually have "kinetic effect" on their designated target but still constitute attacks as a matter of law. *See also* DOD LAW OF WAR MANUAL, *supra* note 36, § 16.5.2.

149. TALLINN MANUAL, *supra* note 4, at 416.

150. *Id*. (citing Protocol I, *supra* note 2, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b), 35(3), 55(1), and 56(1)).

151. *Id*. at 416.

152. However, as the Tallinn Manual notes, other relevant provisions of IHL (*e.g.*, constant care (Rule 114) and the prohibition on collective punishment (Rule 144)) apply. *Id*. at 418.

objectives.[153] Despite the use of both terms, the primary focus of AP I is on attacks. In other words, while the term "operation" is used to generally describe actions of the military, the focus is on protecting civilians and civilian objects from harms associated with attacks. Specifically, Article 48 of AP I states that parties must direct their "operations" only against military objectives.[154] In fact, throughout AP I there is an emphasis on "restricting military operations by reference to attacks."[155] Thus the reference in Article 48 to operations "must be interpreted as bearing on a particular type of operation, an attack."[156] Alternatively, one could argue that the principles of distinction and proportionality apply to both operations and attacks. However, this argument fails to account for the specific words found in the Articles and is not supported in the literature interpreting AP I.[157]

The practical implication of the interpretation of what constitutes an attack for purposes of IHL is that the principle of distinction offers little protection for civilian data in cyberwar.[158] "The principle of protection of the civilian population is inseparable from the principle of the distinction . . . between military and civilian persons. In view of the latter principle it is essential to have clear definitions of each of these categories."[159] Therefore, clarity in application of the principle of distinction and definitional clarity in the words comprising the principle are necessary to ensure protection of civilians, the civilian population, and civilian objects.

153. *See*, *e.g.*, Protocol I, *supra* note 2, art. 51.

154. *Id.* art. 48.

155. Michael N. Schmitt, *Cyber Operations and the Jus In Bello: Key Issues*, 87 NAVAL WAR COL. INT'L L. STUD. 89, 92 (2011).

156. *Id.*

157. *See*, *e.g.*, TALLINN MANUAL, *supra* note 4; Schmitt, *supra* note 155, at 92.

158. *See* Schmitt, *supra* note 103, at 298*; see also*, TALLINN MANUAL, *supra* note 4, at 416–19, 423 (stating that depending on the circumstances, an attack that causes significant damage to civilian objects might violate the principle of proportionality (Rule 113)—not the principle of distinction).

159. AP I COMMENTARY, *supra* note 118, at 610.

### C. PROPORTIONALITY IN CYBERWAR

#### 1. Proportionality Generally

Distinction is not the only relevant IHL principle when discussing protection of civilians and civilian objects from the harms of cyberwar. Proportionality plays a large role in targeting decisions but, due to the narrow interpretation of the scope of attacks regulated by IHL, proportionality also falls short of the goal of protecting the civilian population. The principle of proportionality underpins the prohibition on indiscriminate attacks,[160] and is designed to overcome the otherwise "inadequate" protection offered to the civilian population, civilians and civilian property by the principle of distinction.[161] The principle is codified in Article 51(5)(b) of AP I and prohibits "an 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."[162] Underscoring the importance of the proportionality analysis, Article 57(2)(a)(iii) repeats the standard and precludes those planning, launching or executing attacks from proceeding with the attack if it becomes apparent that the attack would violate the principle.[163]

The principle of proportionality is considered a principle of customary international law and applies in both international and non–international armed conflicts.[164] "Proportionality governs the degree and kind of force used to achieve a military objective by comparing the expected military advantage gained to the expected incidental damage caused to civilians and civilian objects."[165] In this regard, it is a balancing test of suffering and damage versus military advantage.[166] Although a commander only need engage in a proportionality analysis if, after reviewing a target, he concludes there are civilians or civilian objects in the area and, therefore, there could be

160. DINNISS, *supra* note 11, at 205.
161. Richmond, *supra* note 29, at 879.
162. Protocol I, *supra* note 2, art. 51(5)(b).
163. *Id.* art. 57(2)(a)(iii).
164. *See* GEOFFREY S. CORN ET AL., THE WAR ON TERROR AND THE LAWS OF WAR 83–84 (2d ed. 2015).
165. Gervais, *supra* note 10, at 571.
166. Schmitt, *supra* note 130, at 391–92.

collateral damage,[167] the nature of computers and cyber systems—the interconnectedness and reliance on civilian infrastructure—will almost always necessitate a proportionality analysis.[168] Proportionality seeks to preclude "reckless" attacks but does not limit commanders to a single course of action.[169] Additionally, the principle requires consideration of both direct and knock-on or indirect effects of attacks.[170]

In applying the principle of proportionality, the applicable standard is that of a reasonable commander based upon the circumstances known at the time she/he launched the attack.[171] Furthermore, the principle of proportionality is "among the most complex and misunderstood in [IHL] with respect to both interpretation and application."[172] This is a direct result of counter-intuitive application of the rule. The principle of proportionality is an *ex ante* analysis, rendering the *ex post facto* consequences irrelevant for determining whether or not the principle of proportionality has been violated.[173] In other words, if a cyber attack is reasonably expected to cause a temporary disruption to a public-facing website but actually results in an unanticipated destruction of a server hosting medical records and leading to patient deaths, the principle of proportionality is met so long as the expected temporary disruption to the public-facing website would not be excessive in light of the concrete and direct military advantage anticipated from the attack.[174] Recognizing the difficulty of this analysis, the commentary accompanying AP I recognizes a need for "complete good faith on the part of the belligerents, as well as the desire to conform to the general principle of respect for the civilian population."[175]

---

167. CORN ET AL., *supra* note 164, at 84.

168. Presumably, it is possible for a military objective to be so remote and disconnected from all civilian objects yet still susceptible to a cyber attack that it is conceivable, but unlikely, that a proportionality analysis would not be required. An example would be an air-gapped military system accessed directly by a team of special operations forces at a remote location that is not otherwise connected to any civilian cyber systems, and where no civilians or civilian objects are present.

169. *See* Gervais, *supra* note 10, at 572.

170. *Id.*

171. Blank & Guiora, *supra* note 62, at 57.

172. Schmitt, *supra* note 59, at 18.

173. *Id.* at 18 n.59.

174. *See* DOD LAW OF WAR MANUAL, *supra* note 36, §16.5.2 (stating that temporary disruption does not amount to an attack under IHL and, therefore, is not subject to the principle of proportionality).

175. AP I COMMENTARY, *supra* note 118, at 625.

Finally, the principle of proportionality exists to protect civilians and civilian objects, but not combatants or military objectives.[176]

Although the focus of IHL is to protect civilians and civilian objects from the harms of war, "not every inconvenience to civilians ought to be considered relevant to . . . the principle of proportionality."[177] According to Dinstein, "[o]nly loss of life, injury to human beings and (more than nominal) damage to property count."[178]

2. Proportionality in the Context of Cyber Attacks

In cyberwar, the overarching question as to the principle of proportionality's success in protecting a civilian population will largely turn on what the specific terms mean within the principle and how they are applied to cyber attacks. For example, the term "object" for the purpose of a proportionality analysis has the same meaning as an "object" in the distinction analysis.[179] Thus, the principle of proportionality, again, has a large gap with respect to data. This is especially the case because "the importance of data usually exceeds that of [its] physical manifestation."[180] Presently, a reasonable interpretation of IHL would cause a commander to select a cyber attack that may result in collateral damage destroying terabytes of data including medical records and other key pieces of civilian data, over a kinetic strike that is expected to result in, for example, three civilian casualties. Similarly, determining what constitutes "damage" in cyberspace will be key to ascertaining adequate protections. For example, a cyber attack may result in a range of effects from those that result in temporary, reversible loss of use, to those that cause physical damage and destruction. Determining which of these effects constitutes "damage" for the purpose of IHL is a necessary predicate to ascertaining whether the injury or damage is excessive in relation to the direct and concrete military advantage anticipated. Furthermore, because the principle is "couched in language of expectation and anticipation,"[181] the ability to assess expected collateral damage

176. Dinstein, *supra* note 77, at 269–70.

177. *Id.* at 270; *see also* DOD LAW OF WAR MANUAL, *supra* note 36, § 16.5.1.1.

178. *See* Dinstein, *supra* note 77, at 270.

179. Schmitt, *supra* note 103, at 297.

180. *Id.*

181. Dinstein, *supra* note 77, at 270.

from a cyber attack is of paramount importance. The experts drafting the Tallinn Manual recognized the unique nature of the proportionality analysis in cyberwar. In the commentary to rule 113 (Proportionality), the experts noted that "a cyber attack can cause collateral damage during transit and because of the cyber attack itself."[182] In the traditional kinetic attack, there is a mechanism to ascertain the likely collateral damage—the collateral damage estimate methodology ("CDEM").[183] However, to date, no such system exists for cyberwar.

*a. Loss of Functionality*

The experts contributing to the Tallinn Manual noted that, in some circumstances, the loss of functionality, as previously discussed in connection with attacks, may constitute damage to civilian objects.[184] For example, the majority of experts agreed an impairment of functionality that requires replacement of physical components constitutes an attack[185] and, in the context of proportionality, would constitute collateral damage if it occurred to a civilian object. However, the same experts were split as to whether reinstallation of an operating system was a sufficient impairment of functionality as to constitute "damage" in determining whether an operation is an attack.[186] Incorporating this interpretation into the proportionality analysis demonstrates that it remains unclear whether a functional impairment that requires significant software reinstallation would constitute "damage" for the purpose of a collateral damage assessment. Therefore, the precise scope of impairment of functionality and its corresponding application in the proportionality analysis remain unclear under the principles of IHL as espoused in the rules of the Tallinn Manual.

*b. What is Excessive?*

Given the relevant infancy of cyberwar, the Tallinn Manual commentary to Rule 113 (Proportionality) notes that extensive and excessive are not synonymous, yet it offers little by way of

182. TALLINN MANUAL, *supra* note 4, at 471.
183. Schmitt, *supra* note 59, at 19.
184. TALLINN MANUAL, *supra* note 4, at 472.
185. *Id.* at 416.
186. *Id.* at 417.

guidance and clarification.[187] "The term 'excessive' is not defined in international law."[188] The Tallinn Manual, citing the Air Warfare Manual, notes that determining excessiveness is not a purely mathematical comparison of civilian casualties and enemy combatants.[189] The experts, adopting a position that is against the ICRC Commentary,[190] go on to state that, "extensive collateral damage may be legal if the anticipated concrete and direct military advantage is sufficiently great."[191] In other words, under the Tallinn Manual model, there may be a significant amount (extensive) collateral damage that is lawful (not excessive) under a proportionality analysis so long as the concrete and direct military advantage is sufficiently great. Whether that is what the contributors to the Tallinn Manual intended is unclear because in developing Rule 113, the experts failed to articulate in any significant detail exactly how the rule will apply. However, this may, in part, be a result of the subjective nature of the principle.

*c. Knock-On Effects*

Complicating the proportionality analysis in cyberwar are knock-on effects. A knock-on effect is an indirect or reverberating effect of a military attack.[192] "[T]here is a qualitative difference between attacks designed to gain direct control of a physical object and cause it to act in a specific planned way, and attacks targeting the networks and data themselves, aiming for more generalized knock-on [or indirect] effects."[193] Attacks generating collateral knock-on effects are possible in cyberwar given the interconnected nature of computers and cyber systems.[194] Recognizing this risk, the Tallinn Manual states that "indirect effects of a cyber attack comprise 'the delayed and/or displaced second-, third- and

187. *See id*. at 473.

188. *Id*. at 473.

189. *Id*.

190. *See generally* AP I COMMENTARY, *supra* note 118, at 626 (discussing how Article 48 and paragraphs 1 and 2 of Article 51 of Additional Protocol I state that there is no "justification for attacks which cause extensive civilian losses and damages. Incidental losses and damages should never be extensive").

191. TALLINN MANUAL, *supra* note 4, at 473.

192. *See* Schmitt, *supra* note 130, at 392.

193. Lubell, *supra* note 70, at 256.

194. DINNISS, *supra* note 11, at 207–08; *see also* Schmitt, *supra* note 130, at 393.

higher-order consequences of action, created through intermediate events or mechanisms.'"[195] Nevertheless, what remains unclear is "how many levels of these cascading effects will need to be taken into account."[196] For example, Michael Schmitt argues that all reasonably foreseeable effects must be considered, regardless of what tier they may be.[197] Schmitt's position, not surprisingly, is reflected in the Tallinn Manual in the commentary to Rule 113, which states that any expected indirect effects must be factored into the proportionality analysis.[198] However, the literature does not indicate that any State has expressed with fidelity or precision to what extent indirect or knock-on effects will be considered in cyberwar.[199] Additionally, and as previously noted, what level of detail is sufficient for a commander to reasonably rely upon in making the collateral damage determination remains unclear. This is where a detailed understanding and mapping of networks and infrastructure is of paramount importance in cyberwar.[200]

What the traditional proportionality analysis fails to address is that, as a man-made system, computers and cyber systems can, and often do, change dramatically in short amounts of time. In other words, what is saved on a server now and what is saved on that server in 15 minutes may be vastly different. This poses a unique problem in that the rapidly evolving nature of cyber systems, coupled with an *ex ante* analysis, means that the principle of proportionality may be complied with despite the massive collateral effect associated with unexpected or unanticipated data resident on a system that is subject to attack.

---

195. TALLINN MANUAL, *supra* note 4, at 472 (referring to JOINT CHIEFS OF STAFF, JOINT PUB. 3-60: JOINT TARGETING I-10 (2007)); *see also* JOINT CHIEFS OF STAFF, JOINT PUB. 3-60: JOINT TARGETING (Jan. 2013) (instructing the utilization of the Department of Defense Collateral Damage Estimation Methodology to ascertain the scope and extent of expected collateral effect).

196. DINNISS, *supra* note 11, at 208.

197. *Id.*

198. TALLINN MANUAL, *supra* note 4, at 472–73.

199. While the Tallinn Manual notes the United States 2015 submission to the United Nations Group of Governmental Experts noted that in addition to the physical damage that a cyber activity may cause, parties must assess the potential effects of a cyber attack on civilian objects that are networked to military objectives, the submission fails to establish thresholds or otherwise articulate the scope of requirement in a manner that aids practitioners. Tallinn, *supra,* note 4 at 472 (citing United States Submission to the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, in Digest of United States Practice in International Law 2014 at 737.

200. *See* Schmitt, *supra* note 130, at 393.

While every environment is subject to change and while an *ex ante* analysis is the standard for a proportionality analysis in all types of warfare, the speed and magnitude with which changes occur in cyber systems, as discussed in Part II, further erode the protection afforded to civilians by the principle of proportionality.

Applying the principles of IHL to cyberwar is generally difficult, and particularly so with respect to the principle of proportionality. "[I]nternational humanitarian law governing the conduct of hostilities is premised on a paradigm in which most of the deleterious consequences that it seeks to temper are physically destructive or injurious. Cyber operations deviate from this underlying paradigm."[201] Therefore, potential solutions must be sought to ensure adequate protection of the civilian population, civilians and civilian objects. "The nature of combat in new warfare also demands a more nuanced understanding of the factors to include in a proportionality analysis and how to weigh those factors."[202]

## IV. SOLUTIONS TO THE CONUNDRUM

The debate regarding whether IHL applies to cyberspace is largely settled.[203] However, the adequacy of existing IHL rules when applied to cyberwar remains in question. Key deficiencies in the application of the principles of distinction and proportionality to cyberwar are the definition and scope of what constitutes a civilian object versus a military objective, determining what constitutes and how to calculate damage in cyberwar, and ascertaining the scope and extent of indirect or knock-on effects. "Scholars generally divide into two camps on whether current LOAC rules adequately regulate cyberwar: those that believe that current LOAC rules can adequately address cyber war and those that believe new treaties will be necessary to regulate it effectively."[204] While the debate remains among scholars, generally, governments believe existing law, including IHL, is sufficient.[205] However, as previously discussed,

---

201. Schmitt, *supra* note 103, at 289.

202. Blank & Guiora, *supra* note 62, at 66.

203. *See* TALLINN MANUAL, *supra* note 4; *see generally* Koh, *supra* note 36 (discussing how IHL applies across cyberspace).

204. Richmond, *supra* note 29, at 865.

205. *Id.* (citing Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 124 (2009)).

governments have failed to articulate in any appreciable detail how the principles of IHL apply in the case of operations that destroy data or temporarily interfere with functionality.[206]

Developing solutions to the applicability of IHL in cyberwar requires a review of the underlying paradigm. Specifically, IHL is "premised on a paradigm [where the adverse effects] . . . it seeks to temper are physically destructive or injurious."[207] Parts II and III of this Article detail many cyber effects that do not result in traditional injury or destruction. Additionally, the prevalence of dual-use infrastructure significantly affects the traditional targeting analysis because there is a greater number of civilian objects that may qualify as military objectives in cyberwar and the precise application of the IHL principles of distinction and proportionality is unclear.[208] Thus, the question remains: what actions may be taken to achieve the goal of IHL to protect civilians from the effects of hostilities?

There are a multitude of options to clarify application of IHL to cyberwar, each with associated benefits and risks. Solutions include a new treaty, a new additional protocol to an existing treaty, and refinement through State practice to establish customary norms. In order to assess the adequacy and risks with each of the potential solutions, the goals must be further clarified. The underlying goal of IHL is to protect civilians. This goal is achieved through, among other things, the application of the principles of distinction and proportionality. Further refinement of this goal should include the use of traditional targeting rules, but with a clearer articulation of how traditional rules (e.g., distinction and proportionality) apply in cyberwar in light of the unique and interconnected nature of data and cyber infrastructure.

In the cyberwar context, the principles of distinction and proportionality fail to adequately protect civilians not because of an inherent flaw, but rather because the application of the

206. *See, e.g.*, ADVANCE QUESTIONS, *supra* note 37; JOINT CHIEFS OF STAFF, JOINT PUB. 3-12: CYBERSPACE OPERATIONS (Feb. 5 2013); DOD LAW OF WAR MANUAL, *supra* note 36, § 16.1; Australian Permanent Representative to the UN Peter Woolcott, Statement to the UN General Assembly (Oct. 20, 2011) (transcript available at http://australia-unsc.gov.au/2011/10/disarmament-measures-and-international-security/); UK CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD17 (2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

207. Schmitt, *supra* note 103, at 289.

208. *Id.*; Prescott, *supra* note 58, at 126–27.

principles is unclear and suffers from a historical focus on effects generated from traditional kinetic warfare. As previously noted, the Tallinn Manual distinguishes between attacks that are subject to the distinction and proportionality analysis based upon effects, and operations that are not subject to the principles of distinction and proportionality but are covered by other aspects of IHL.[209] Therefore, one may successfully assert that in an effects-based analysis, the reliance on the traditional application of the principles of IHL is sufficient in cyberwar so long as the attack generates a kinetic-like effect. In other words, so long as the cyber attack yields death, injury to persons, or physical damage, then the principles of distinction and proportionality apply to protect the civilian population and civilian objects. However, where a cyber attack or operation does not result in physical damage but rather only creates a cyber effect (e.g., temporary inability to access a public facing website, corruption, manipulation, or loss of data with no corresponding impact on the functionality of a cyber system, etc.), further clarification of the application of the principles of IHL is necessary. The solutions proposed in this Article address when an operation would rise to the level of an attack under IHL but yields only a cyber effect (no kinetic-like damage). The paradigm to be applied to operations that do not rise to this level will not be addressed herein.

The solution is not merely a matter of interpretation of existing principles. Indeed, some experts believe that the existing interpretation of these principles is flawed: "[A]n interpretation that limits the notion of attacks to acts generating physical effects cannot possibly survive."[210] This interpretation creates risk that a broader definition of attacks may result in the future. Similarly, it is unrealistic to suggest that the civilian population may lawfully suffer significant disruption and mass data destruction from a cyber operation merely because a physical result does not occur.[211] Therefore, how the protective goals may be realized while recognizing that war is inherently disruptive towards civilians requires additional definitions and clarity.

Commentators have suggested that a new treaty for cyberspace is unrealistic and unlikely, due to the myriad issues

209. *See* TALLINN MANUAL, *supra* note 4, at 415, 421–22, 476.
210. Schmitt, *supra* note 103, at 295.
211. *Id*. at 295–96.

associated with cyberspace, war, and international relations.[212] Additionally, a new treaty is not necessary because IHL remains largely sufficient to protect civilians, even in a cyberwar where a cyber attack results in physical damage or destruction. Because an entire new protective structure is not required (existing IHL and its application addresses those cyberattacks that generate kinetic-like effects), nor is one likely to be agreed upon by States, a treaty is not the correct mechanism to resolve this issue. If sought, a new treaty is likely to be politically difficult as countries will seek to use this as a mechanism to shape their own domestic security authority, limit actions by other States to engage in espionage, and potentially even address international trade. Furthermore, given the interconnected nature of cyberspace, establishing even the issues and topics the treaty will cover would likely prove incredibly difficult. A second, more viable option is a new additional protocol—Additional Protocol IV ("AP IV"). While a new additional protocol is also a treaty, there is a greater likelihood of adoption of a protocol because a protocol supplements existing rules whereas a treaty would promulgate an entirely new rule set.[213] An additional alternative to a new protocol, advocated by at least one expert over a decade ago, is a restatement of applicable *jus in bello* principles as was done in the San Remo Manual.[214] While such a restatement could be valuable to shape State practice, it was for all intents and purposes accomplished in the Tallinn Manual. Assuming it would be similar in scope and development to the Tallinn Manual, it would not be binding or represent actual State practice. In these regards, a restatement will fail to ensure adequate protection for civilians and civilian objects.

The creation of a new additional protocol, AP IV, offers the most effective means to provide for the protection of civilians in a cyberwar that does not yield kinetic-like effects. AP IV should

---

212. *See id.* at 296; Marshall J. Breger & Marc D. Stern, *Symposium on Reexamining the Law of War: Introduction to the Symposium on Reexamining the Law of War*, 56 CATH. U. L. REV. 745 (2007); Gervais, *supra* note 10, at 579.

213. *See* U.N. Treaty Collection, Definitions of Key Terms Used in the UN Treaty Collection, 69 https://treaties.un.org/doc/source/publications/THB/English.pdf (last visited Mar. 25, 2017); *see also* UNICEF, INTRODUCTION TO THE CONVENTION ON THE RIGHTS OF THE CHILD: DEFINITIONS OF KEY TERMS, http://www.unicef.org/crc/files/Definitions.pdf (defining an optional protocol).

214. YORAM DINSTEIN, INTERNATIONAL EXPERT CONFERENCE ON COMPUTER NETWORK ATTACKS AND THE APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW: PROCEEDINGS OF THE CONFERENCE 18 (Karin Bystrom ed., 2005).

build off the work of the Tallinn Manual, however, reflecting the opinions and positions of States, and offer adequate protection for civilians while recognizing that the nature of warfare necessitates the use of the latest technology. With respect to distinction and proportionality, there are several aspects of IHL that should be addressed in AP IV.

### A. SOLUTIONS FOR THE PRINCIPLE OF DISTINCTION

First, agreement as to the status of data as an object must be included. This does not require a blanket statement, although such a statement could be made. In the absence of a blanket statement regarding data's status as an object, an alternative would be the establishment of a test for data to determine if the data in question constitutes a military objective. To the extent it qualifies as a military objective, then it meets the standard for purposes of distinction and provides a piece of the balancing test for proportionality. Criteria for data to be considered a military objective should include the application of the nature, location, use, and purpose standard, modified for cyberwar. More specifically, the data itself should offer a definitive military advantage or demonstrable military purpose to qualify as a military objective. Data meeting this standard could include logistical data regarding shipping times and locations for military equipment and personnel; data containing personnel qualification standards; electronic copies of war or contingency plans; and data containing demographic, or other aspects of a targeted group for developing a military information support operation campaign. The corollary is that all data that is not a military objective should be treated as civilian objects for the purpose of distinction and collateral damage assessments. It is unrealistic in an information age for data to fall outside the scope of constituting an object, thus failing to receive IHL protection associated with the principles of distinction and proportionality. Additionally, by defining the parameters within which data constitutes a valid military objective, the corollary establishes the non-military objective data as a civilian object thus clarifying the scope of the protections afforded by IHL.

Second, additional clarification and limitation on what constitutes a lawful military objective should be included in AP IV. Specifically, the definition of dual-use objects must be clarified. Presently, a significant portion of the internet backbone and cyber systems may constitute a legitimate

military objective, afforded only the protection of the principle of proportionality. To ensure adequate protection of the civilian population and civilian objects, certain aspects of the internet's infrastructure should be designated as protected objects and the dual-use definition for cyber systems must be modified in a manner that tips in favor of protection for civilians as opposed to the military needs of the belligerents.[215] More specifically, under AP IV, action against dual-use infrastructure should be limited to the least disruptive action so as to minimize collateral effect against civilians and civilian objects. Additionally, AP IV should specifically preclude war-sustaining objects from being subject to cyber attack. The inclusion of war-sustaining objects as valid military objectives so dilutes the protection of the principle of distinction in cyberwar as to virtually eliminate the protection. Furthermore, AP IV must establish a threshold of likelihood of use to limit the extent to which the "purpose" test for determining what constitutes a military object under the principle of distinction. This test should set a high bar, thus affording civilians and civilian objects maximum protection. The specific nature of cyber systems relies on the resiliency of the networks and opening them to large-scale adverse impacts based upon a low threshold of likely future use fails to adequately protect the civilian population.

Third, AP IV must clarify whether loss of functionality or destruction of data constitutes an attack for purposes of IHL. Additionally, for operations short of attacks, AP IV should expand upon Rule 114 from the Tallinn Manual and provide specific guidelines on how commanders may avoid unnecessary effects on civilians.[216] Combining new rules on data with clarity as to the status of loss of functionality as an attack completes the circle with respect to the application of the principle of distinction in cyberwar.

### B. SOLUTIONS FOR THE PRINCIPLE OF PROPORTIONALITY

The principle of proportionally will also benefit from establishment of AP IV. AP IV must clarify what constitutes collateral damage in a cyberwar and establish a threshold for

215. Alternatively, though unrealistically, States could agree to build separate infrastructure for military networks. Because this is likely cost-prohibitive and unlikely to be done it should be discarded from consideration.

216. *See generally* TALLINN MANUAL, *supra* note 4, at 476–78 (discussing Rule 114).

certainty that must be achieved with respect to the characteristics of the cyber system before it is attacked. While a rigid burden of proof would be unworkable in the case of war and constantly evolving cyber systems, the delineation of more specific factors to consider when determining collateral damage and the establishment of a subjective test for certainty with respect to understanding the cyber systems to be attacked will yield greater protection for civilians. This is the only way for the "good faith" reliance on the judgment of the belligerent to actually benefit the civilian and civilian objects. Additionally, AP IV must consider how the overall proportionality analysis of any planned attack on a military objective is considered. While a mathematical formula is inappropriate, at a minimum, thresholds and guidance must be developed to aid the commander in combining the physical harm to civilians with the loss of functionality and data from cyber systems. To that end, further clarifying the impact of functionality, as described in Part IV A will benefit the proportionality analysis by shifting the balance more in favor of protecting civilians and civilian objects. In turn, establishing formal thresholds and guidance and incorporating changes in the interpretation with respect to functionality will aid in the development of formal collateral damage estimation methodologies for cyber attacks. This will yield a more consistent and universal application of the principle of proportionality.

Finally, AP IV should establish the extent to which knock-on effects must be considered. Specifically, it should establish a "one-tier beyond the attack level analysis" requirement plus those effects that are reasonably foreseeable at the time. It is reasonable to require a commander to gain insight into what will be indirectly affected by the loss of a particular cyber system. It is unreasonable to expect a commander to consider unforeseeable second- and third-tier effects that may occur down the road. Additionally, given the rapidly changing nature of cyber systems, AP IV should establish a time period of review for purposes of protecting commanders when they make good faith judgments. In other words, so long as a commander relied upon information that was no more than 48 hours old in making a targeting decision, that will be considered reasonable for purposes of a good faith judgment with respect to the application of IHL to the facts as presented. This is especially important given the rapidly changing nature of cyberspace, a man-made domain. While establishing a time period of review will require intelligence assets to continually update the target package, it

will furnish greater protection for civilians and civilian objects while preserving some decision-space for a commander to execute the targeting process.

### C. RISKS AND BENEFITS OF AP IV

The benefits of establishing an AP IV are numerous. A new additional protocol would be the result of discussions and agreement amongst States. Thus, the public position on each of these issues of each of the participants would be clear at the outset. Additionally, AP IV would reflect the consensus of the international community and would then be subject to ratification by States. This public debate and transparency of process allows the civilian population, whom the new protocol will protect, to be engaged in its development through each State's political process.[217] Finally, AP IV offers the best way to rapidly establish protection for civilians and civilian objectives or, in the alternative, put them on notice of the framework under which they may likely suffer the harms of cyberwar.

Despite many benefits, there are significant drawbacks and risks associated with AP IV as well. First, the difficulties associated with negotiating and bringing into force a new treaty for cyberspace largely exist with respect to establishing a new additional protocol. Yet, this is mitigated by the limited nature and scope of AP IV—supplementing existing rules. Second, a new additional protocol will likely reflect the consensus of the international community, that is, the lowest common agreement of States and thus the lowest level of protection for civilians. While a treaty would also reflect the consensus of the international community, the limited scope of AP IV and the fact that there is an existing body of law to build from will hopefully yield a level of protection for civilians that is greater than would otherwise be achievable with a full cyber treaty. Third, there is a significant chance that there will be no agreement or minimum ratification of AP IV. If that were to occur, the civilian population retains existing IHL protection and further protections would be the result of the negotiation process and other mechanisms, such as the normative process, contributing to customary international law.

---

217. While some States, e.g., China, may not seek or accept input from its citizens, this is also true with any other international law negotiation.

Alternatively, and what the United States seeks to do,[218] is to rely on the development of customary international law norms to clarify how IHL will apply in cyberwar. A significant benefit of this approach is reliance upon what States actually do out of a sense of legal obligation as opposed to what States say they will do. Second, this approach offers a slower development over time, allowing for a more thoughtful and reflective approach. Third, it allows the States who are actors in cyberspace to exercise greater influence over the development of IHL in cyberspace.

Cutting against the customary normative approach is the nature of cyberspace operations. It is often difficult to ascertain what States do for policy, political, or tactical reasons, and what States do out of a sense of legal obligation.[219] Additionally, the often classified nature of cyberspace operations shields them from the public and international community.[220] Therefore, distilling international norms from the practice of States will be difficult at best. Second, the customary normative approach is based upon practice over time, with time being the operative word. This approach offers little certainty for the civilian population and breeds uncertainty in the application of IHL by States. Thus in the interim, civilians may suffer more because States may engage in actions that adversely impact civilian data and the functionality of civilian cyber systems, and States may be hesitant to use cyberwar, thus resulting in continued reliance on kinetic attacks.[221] Finally, by allowing only those States that engage in cyberwar to establish the customary norms, it disproportionately places at risk the civilian population in States that do not actively engage in cyberwar. In other words, this process allows the rules to be formed by those who engage in cyberwar. This subjects those in States not engaging in cyberwar to watch from the sidelines and prepare to suffer adverse

---

218. *See* BARACK H. OBAMA, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

219. *See* John B. Bellinger III & William J. Haynes II, *A US Government Response to the International Committee of the Red Cross Study* Customary International Humanitarian Law, 89 INT'L REV. RED CROSS 443, 444–47 (2007).

220. *See* Zachary Fryer-Biggs, *US Begins to Define Military Cyber Ops*, DEFENSE NEWS (June 17, 2013), https://fortunascorner.wordpress.com/2013/06/17/u-s-begins-to-define-military-cyber-operations/.

221. *See supra* Section III B.3. Generally, cyberwar offers less risk of death to the civilian population and is therefore preferential under a macro view of IHL.

consequences. While this Article notes the increasing prevalence of cyber capabilities, it is safe to presume that only a small subset of those countries with the capabilities have or do use them in a fashion that may be cited to develop international norms.[222] On balance, while there are benefits to the customary normative approach, AP IV offers greater protection of civilians and is more in accord with the spirit of IHL.

## V. CONCLUSION

One of the key purposes of IHL today is to protect the civilian population from the harms of hostilities. Cyberwar is the warfare of the future—countries are dramatically increasing their capability in this area. In cyberwar, the application of the principles of distinction and proportionality fail to adequately provide protection of the civilian population because the definitions and current application are based upon the historical application to kinetic warfare. Despite the public statements of the international community that IHL applies in cyberspace, there has been a lack of transparency in how States will apply the principles of IHL to cyberwar. While the Tallinn Manual takes a big first step, it is the work of experts, not States, and does not necessarily reflect the position States will follow when they engage in cyberwar.

For reasons stated above, a cyberspace treaty is not needed and continued reliance on the customary normative process is inadequate. The best way to protect the civilian population, ensure equality in the establishment and development of the application of the IHL framework, and provide transparency for the civilian population and other States is to develop and ratify Additional Protocol IV. This Protocol would further distinguish what constitutes a civilian object from military objective in cyberspace, including with respect to data and the functionality of cyber systems, addressing what constitutes and how to calculate damage in cyberspace, and determining the scope and extent to which indirect or knock-on effects must be considered. This is the only way to ensure adequate protection for civilians and civilian objects in the midst of a cyberwar.

---

222. This is a direct result of the difficulty associated with attribution in cyberspace and the difficulty associated with ascertaining whether a particular action by a State was performed out of a sense of legal obligation.