Michigan Telecommunications and Technology Law Review

Volume 23 | Issue 1

2016

Virtual Violence - Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law

Ido Kilovaty
Yale Law School

VIRTUAL VIOLENCE – DISRUPTIVE CYBERSPACE OPERATIONS AS "ATTACKS" UNDER INTERNATIONAL HUMANITARIAN LAW

*Ido Kilovaty**

Cite as: Ido Kilovaty, *Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under Humanitarian Law,*
23 MICH. TELECOM. & TECH. L. REV. 113 (2016).
This manuscript may be accessed online at repository.law.umich.edu.

Power outages, manipulations of data, and interruptions of Internet access are all possible effects of cyber operations. Unfortunately, recent efforts to address and regulate cyberspace operations under international law often emphasize the uncommon, though severe, cyber-attacks that cause deaths, injuries, or physical destruction. This paper deals with cyber operations during armed conflicts that cause major disruption or interruption effects – as opposed to deaths, injuries, or physical destruction.

The purpose of this paper is to explore the consequences of these cyber operations that cause major disruption or interruption effects, and to argue that they might still constitute "acts of violence," as the term "attacks" is defined under international humanitarian law. Cyber operations that qualify as "attacks" will have to comply with the principles of distinction and proportionality, thus requiring the initiator to design his or her cyber weapon humanely. Therefore, labeling these cyber operations as "attacks" will promote the (1) the protection of civilians and objects; (2) critical infrastructure, such as energy, transportation and emergency services, and (3) strengthen fundamental human rights.

* Cyber Fellow at the Center for Global Legal Challenges, Yale Law School; Resident Fellow Information Society Project, Yale Law School; S.J.D. Candidate, Georgetown University Law Center. I would like to gratefully acknowledge the generous support of the Minerva Center for the Rule of Law under Extreme Conditions at the Faculty of Law and Department of Geography and Environmental Studies, University of Haifa, Israel and of the Israeli Ministry of Science, Technology and Space, who made this project possible. I am thankful for the comments and support of Prof. Amnon Reichman, Prof. Rosa Brooks, Prof. Alexa Freeman, Prof. Mary DeRosa, Adv. Ido Rosenzweig.

I. Introduction

On December 23, 2015, Ukraine experienced a major power outage, affecting hundreds of thousands of people.[1] This time, however, it was not an occasional blackout caused by technical failure, high demand, or weather-related reasons. Rather, it was a blackout caused by a cyber-attack targeting the supervisory control and data acquisition ("SCADA") systems of the Ukrainian power grid.[2] Although cyber operations are already used frequently during armed conflicts,[3] and diplomatic and political tensions, this was the first time that cyber operations were successfully used to cause a power outage.[4]

---

1. Alex Hern, *Ukrainian Blackout Caused by Hackers that Attacked Media Company, Researchers Say*, The Guardian (Jan. 7, 2016, 8:20 AM), www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company.

2. Vangie Beal, *SCADA - Supervisory Control and Data Acquisition*, Webopedia, http://www.webopedia.com/TERM/S/SCADA.html (last visited Nov. 1, 2016) (defining SCADA as an "[a]cronym for supervisory control and data acquisition, a computer system for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.").

3. *See* Catherine Lotrionte, *Cyberwar: Building a Normative and Legal-Based Approach for Cyberdeterrence*, *in* Law and Disciplinarity: Thinking Beyond Borders (Robert Beck ed., 2013) 67, 69.

4. Andrea Peterson, *Hackers Caused a Blackout for the First Time, Researchers Say*, Washington Post (Jan. 5, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/.

A prolonged power outage such as this could certainly result in an enormous humanitarian crisis, which would most likely be in violation of international humanitarian law (IHL), and even international criminal law.[5] The question explored by this paper, however, is whether cyber operations that do not result in *direct* kinetic effects such as death, injury, or physical destruction,[6] can still qualify as an "attack" under IHL and, thus, be limited by its principles of distinction and proportionality in armed conflict. To this subset of cyber operations, I will refer to as "disruptive cyber operations".

Until now all recent efforts to address the threat of cyber warfare have focused on the effects of cyberspace activities. For example, efforts have questioned whether the effects were physical or non-physical, severe or less severe, violent or non-violent. While it is clear existing international law norms will cover severe forms of cyber operations, it is not clear what norms apply to non-destructive cyber operations – i.e. those that do not result in death, injury, or physical destruction.

While destructive cyber operations have little trouble being governed by IHL principles of distinction and proportionality, disruptive cyber operations are not necessarily governed by these principles. This is because there is no official or widely accepted definition of disruptive cyber operations. Generally, however, disruptive cyber operations are cyber operations that "*interrupt the flow of information or the function of information systems without causing physical damage or injury*".[7] An example could be a cyber operation that interrupts the access to the Internet or other information systems, which does not result in *direct* death, injury, or physical destruction.

IHL has yet to be adapted to this increasingly ubiquitous part of contemporary armed conflict despite the indirect effects of disruptive cyber operations potentially having devastating consequences. The massive manipulation and interruption of systems and information flow was previously unattainable through traditional means of warfare. But today, these manipulations and interruptions are not only possible through traditional means of warfare, but modern societies have also become much more depen-

---

5. *See, e.g.*, Rome Statute of the International Criminal Court, art. 8(2)(a)(iv), July 17, 1998, *reprinted in* 8 J. INT'L L. & PRAC. 227, 232 (1999) (defining as a war crime, and prohibiting, "Extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly."); *id.* at art. 8(2)(b)(ii), *reprinted in* 8 J. INT'L L. & PRAC. 227, 233 (1999) (prohibiting "Intentionally directing attacks against civilian objects, that is, objects which are not military objectives.") *id.* at art. 8(2)(b)(v), *reprinted in* 8 J. INT'L L. & PRAC. 227, 233 (1999) (prohibiting "Attacking or bombarding, by whatever means, towns, villages, dwellings or buildings which are undefended and which are not military objectives.").

6. *See* NILS MELZER, CYBERWARFARE AND INTERNATIONAL LAW 26 (United Nations Inst. for Disarmament Research ed., 2011), *available at* http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

7. Gary Brown & Owen Tullos, *On the Spectrum of Cyberspace Operations*, SMALL WARS JOURNAL (Dec. 11, 2012, 5:30 AM), www.smallwarsjournal.com/print/13595.

dent on these information systems. This explains why these disruptive cyber operations have become an integral part of nearly every recent armed conflict, and why the legal questions of these operations must be answered.[8]

This paper will argue that cyberspace has allowed for a new form of violence to emerge – violence that is enabled by the digital era, and that causes major disruptive effects to modern societies. To combat this new form of violence, disruptive cyber-attacks must be incorporated in the ambit of IHL in order to protect civilians and civilian objects. Once incorporated into IHL, if a disruptive cyber operation is deemed "violent" enough to be considered an "attack," the operation would be constrained by the principles of distinction and proportionality. The result would be that the cyber initiator of such attacks will be required to design the cyber operation *humanely.* This would mean that the code and target of the operation must be sophisticated enough to distinguish between civilians and combatants, military and civilian objectives, and cause only proportionate collateral damage. As the reliance on cyberspace, the internet of things, and data is becoming essential in nearly every society, limiting the instances in which disruptive cyber operations can be used is necessary to promote the proper functioning of society and to provide guidance to adversaries who wish to use disruptive cyber operations in armed conflict.

Section II will introduce the relevant norms and principles within IHL, and discuss the current debates on the nuances of these principles. Section III will (1) introduce the concept of disruptive cyber operations; (2) argue that these operations are in fact a new form of violence; and (3) apply accepted methods of treaty interpretation to establish a new norm to governing what qualifies as an "attack" under IHL. Section IV will discuss the normative and practical implications of allowing certain disruptive cyber operations to be included in the definition of "attack" under IHL. This section will (1) introduce the "duty to code humanely;" (2) offer a different perspective of the proportionality analysis; (3) discuss the targeting of data in these cyber operations; and (4) discuss current international and domestic legal frameworks, that have addressed the challenges of disruptive cyber operations.

II. "Attacks" Under International Humanitarian Law

IHL is a body of international law that applies during armed conflicts.[9] It is often synonymously referred to in Latin as "*Jus in Bello*" or "law in

8. *See* Marco Roscini, Cyber Operations and the Use of Force 165 (2014).

9. *See* Geneva Convention Relative to the Treatment of Prisoners of War, arts. 2-3, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

war." IHL, therefore, is the set of norms and principles that regulates the conduct of parties to an armed conflict.[10]

Armed conflicts can be either international armed conflicts ("IACs"),[11] between two or more states, or non-international armed conflicts ("NIACs"), between states and armed groups or between armed groups within a state.[12] The principles of distinction and proportionality, which are part of customary international law, and which apply to both IACs and NIACs, are only applicable to activities that qualify as "attacks." Thus, only a subset of military activities will be constrained by the principles of distinction and proportionality.

"Attacks" are defined as "acts of violence against the adversary, whether in offense or in defense" by Article 49(1) of Additional Protocol I of the Geneva Conventions.[13] The existence of an "armed conflict"" is a prerequisite for applying the principles of distinction and proportionality to "attacks." Thus, it is critical to understand when an act can be considered an "attack."

The term "attack" has received several definitions from countries and bodies around the world. For example, the International Committee of the Red Cross ("ICRC") commentary to Additional Protocol I and the International Criminal Tribunal for the Former Yugoslavia ("ICTY") have found that the term "attack" means combat action.[14] Meanwhile, Heather Dinniss' highly cited commentary argues "attacks" do not include the dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare since Article 49's definition of attacks as "acts of violence" denotes physical force.[15]

Cyber operations exacerbate the difficulty in defining the precise scope of "attacks" under IHL.[16] This is primarily because the debate focuses on

---

10. Int'l Comm. of the Red Cross, *What are Jus ad Bellum and Jus in Bello?*(Jan. 22, 2015), https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0.

11. *See* Int'l Comm. of the Red Cross, How is the Term "Armed Conflict" Defined in International Humanitarian Law 1 (2009), *available at* https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf (defining IACs as "those which oppose "High Contracting Parties" meaning states.").

12. *Id.* at 3.

13. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 49(1), June 8, 1977, U.N. Doc. A/32/144, *available at* https://www.icrc.org/eng/assets/files/other/icrc_002_0321.pdf [hereinafter AP I].

14. Int'l Comm. of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 para. 1880 (Yves Sandoz et al. eds., 1987), *available at* https://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_Protocols.pdf [hereinafter The Commentary]; *See* Prosecutor v. Strugar, Case No. IT-01-42-T, Judgment (Int'l Crim. Trib. for the Former Yugoslavia Jan. 31, 2005).

15. Michael Bothe et al., New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949 289 (1982).

16. *See* Heather Dinniss, Cyber Warfare and the Laws of War 197 (2012).

whether non-destructive cyber operations can even be considered "attacks" under IHL. There is, however, some precedent for IHL limiting certain actions due to their violent *consequences* even without a conventional manifestation of physical force – for example, IHL limited the use of chemical and biological weapons even though the deployment of these weapons does not release violent kinetic forces.[17] Given how the battlefield has changed dramatically since the language of Additional Protocol I was adopted back in 1977, IHL has at times adapted to meet the needs of the international community.

IHL experts have debated whether disruptive cyber operations can be deemed "attacks" and whether the principles of distinction and proportionality should only be applied to "attack" operations. For example, Yoram Dinstein argues that cyber operations are to be considered as "attacks" only "if they engender violence through their effects".[18] He believes that a simple firewall breach or virus dissemination is not enough,[19] while "shutting down a life-sustaining software programme or bring[ing] about serious damage to property" would qualify the cyber operation as an attack.[20] A contrary view held by Nils Melzer, Legal Adviser of the ICRC, believes that the substantive principles of distinction and proportionality should apply to the broader hostilities, rather than the narrow form of operations that qualify as "attacks,"[21] arguing that "the applicability of the restraints imposed by IHL on the conduct of hostilities to cyber operations depends not on whether the operations in question qualify as "attacks" . . . but on whether they constitute part of 'hostilities' within the meaning of IHL."[22]

Additionally, ICRC Deputy Head of Legal Division, Knut Dörmann, holds a different view,[23] arguing that "neutralization" should be part of the scope of "attack" due to its inclusion in Article 52(2) of Additional Protocol I, which provides that –

> "Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effec-

17. *See* MICHAEL SCHMITT, "ATTACK" AS A TERM OF ART IN INTERNATIONAL LAW: THE CYBER OPERATIONS CONTEXT 290 (C. Czosseck et al. eds., 2012), *available at* https://ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf, (referencing Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65.

18. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES IN AN INTERNATIONAL ARMED CONFLICT 2 (3d ed. 2016).

19. *Id.*

20. *Id.*

21. *See* MELZER, *supra* note 6, at 26.

22. *See* MELZER, *supra* note 6, at 26.

23. KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS 6 (2001), *available at* https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.

> tive 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".[24]

Dörmann also argues that "In literature it is sometimes claimed that the use of CNA expands the range of legitimate targets because it enables attacks with reversible effects against otherwise prohibited objects. If this claim implies that an attack against a civilian object may be considered lawful if the attack does not result in destruction or if its effects are reversible, this claim is unfounded under existing law".[25] While Dörmann's intention of protection of civilians and civilian objects from neutralizing cyber operations is desirable, it does not necessarily follow given the language of Article 52(2), which only deals with military objectives.[26]

In 2011, the ICRC released a statement at the U.N. General Assembly, reaffirming the importance of IHL compliance with regards to cyber warfare:

> [T]he ICRC draws the attention of States to the potential humanitarian consequences of cyber warfare, that is the resort to computer network attacks during armed conflict situations. Such consequences may include disastrous scenarios such as air traffic control systems being interfered with and causing airplanes to collide or crash, disruption of the electricity or water supplies for the civilian population, or damage to chemical or nuclear facilities. The ICRC therefore recalls the obligation of all parties to conflicts to respect the rules of international humanitarian law if they resort to means and methods of cyber warfare, including the principles of distinction, proportionality and precaution.[27]

This quote illustrates the ICRC's serious concern about the potential humanitarian consequences of cyber operations and makes an argument for how, regardless of the medium used for executing an action, any type of operation should still require compliance with distinction, proportionality, and precaution. To better understand the restrictions imposed on "attacks", the next sections will discuss distinction, indiscriminate attacks, and proportionality.

---

24. AP I, *supra* note 13, at art. 52(2).

25. Dörmann, *supra* note 24, at 5.

26. *See* Dinniss, *supra* note 16, at 198 (providing a counterargument to Dörmann's assertions).

27. U.N. Gen. Assembly, General Debate on All Disarmament and International Security Agenda Items, 66th Sess., First Committee, items 87 & 106 of the agenda, statement by the Int'l Comm. of the Red Cross, New York (October 11, 2011), *available at* https://www.icrc.org/eng/resources/documents/statement/united-nations-weapons-statement-2011-10-11.htm.

A. *Distinction*

IHL seeks to protect civilians from "the calamities of war" by creating a distinction between civilians and combatants, military objectives, and civilian objects.[28] The basic rule of distinction in Article 48 of Additional Protocol I provides that: "[p]arties 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."[29] The Commentary to Additional Protocol I explains that "operations" in the context of Article 48 includes "all movements and acts related to hostilities that are undertaken by armed forces."[30]

Distinction is a bedrock principle for the conduct of hostilities. Distinction obligates parties to direct their attacks to military targets and to spare civilians and civilian objects. This principle also reinforces both humanitarian and strategic considerations due to direct attacks being permissible only against military objectives. This is illustrated by Article 52(2) of Additional Protocol I, which states that "*[a]ttacks* shall be limited strictly to military objectives."[31] This means that "the civilian population as such, as well as individual civilians, shall not be the object of *attack*"[32] and that "civilian objects shall not be the object of *attack*."[33]

Any intentional violation of this principle of distinction is considered a war crime under customary international law.[34] It would therefore be illegal to initiate a cyber operation *directly* targeting civilians, if the operation were considered an "*attack.*"

While the case of *destructive* cyber operations as *attacks* is quite straightforward, it does not extend to *disruptive* cyber operations. As noted by Heather Dinniss –

> it is common ground that computer network attacks which result in physical damage to civilian property, injury or death to civilians constitute attacks under international humanitarian law and are thus prohibited. However, the status of computer network attacks directed at civilian objects that do *not* result in such deleterious effects remains the subject of debate.[35]

Excluding disruptive cyber operations from the scope of "attack" would mean that civilians and civilian objects could legitimately become a *direct*

---

28. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Dec. 11, 1868, *reprinted in* 1 AM. J. INT'L L. 95, 95-96 (Supp. 1907).
29. AP I, *supra* note 13, at art. 48.
30. The Commentary, *supra* note 14, at para. 1875.
31. AP I, *supra* note 13, at art. 52(2) (emphasis added).
32. AP I, *supra* note 13, at art. 51(2) (emphasis added).
33. AP I, *supra* note 13, at art. 52(1) (emphasis added).
34. Rome Statute, *supra* note 5, at arts. 8(2)(b)(i) & 8(2)(b)(ii).
35. DINNISS, *supra* note 17, at 197.

target of disruptive cyber operations. This would be a strange outcome because the ICTY has explained there are no exceptions to the prohibition of direct attacks against civilians and civilian objects, even if military necessity required such attack to be made.[36]

B. *Indiscriminate Attacks and Proportionality*

In addition to protection from direct attacks, IHL also prohibits "indiscriminate *attacks*"[37] Indiscriminate attacks are "those which are not directed at a specific military objective,"[38] "employ a method or means of combat which cannot be directed at a specific military objective,"[39] or employ methods and means of combat the effects of which cannot distinguish between protected and military targets.[40]

The prohibition against indiscriminate attacks is essential because it allows attacks to be prohibited if they fall under the definition of "indiscriminate attacks," even if the attack is not directed at civilians or civilian objects.[41] This is of particular concern for cyber operations, which include poorly designed viruses and worms that do not distinguish between identities of their targets,[42] as well as distributed denial of service (DDoS) attacks, which can affect untargeted civilians.[43]

The indiscriminate attack prohibition only applies to operations that are considered "attacks" under IHL. Therefore it is important to establish disruptive cyber operations as "attacks.".

C. *Proportionality*

IHL adds another layer of protection to civilians and civilian objects, even if an attack was not directed at a civilian or civilian object, and even if the employed methods were capable of discriminating between protected and unprotected targets. IHL assumes that even if these attacks do not target a civilian or civilian object and discriminate between protected and unprotected targets, incidental damage to civilians and civilian objects is still pos-

36. *See* Prosecutor v. Galiæ, Case No. IT-98-29-A, Judgment, ¶ 130 (Int'l Crim. Trib. For the Former Yugoslavia Nov. 30, 1996).

37. AP I, *supra* note 13, at art. 51(4) (emphasis added).

38. AP I, *supra* note 13, at art. 51(4)(a).

39. AP I, *supra* note 13, at art. 51(4)(b).

40. AP I, *supra* note 13, at art. 51(4)(c).

41. *See* DINSETIN, *supra* note 19, at 127.

42. *See* Yoran Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, 17 J. CONF. & SEC. L. 261, 267 (2012).

43. Vangie Beal, *DDoS Attack: Distributed Denial of Service*, WEBOPEDIA, http://www.webopedia.com/TERM/D/DDoS_attack.html (last visited Nov. 1, 2016) ("[I]n a DDoS attack, the incoming traffic flooding the victim originates from many different sources — potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a simple IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.").

sible. Therefore, for additional protection, Article 51(5)(b) provides that "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" is indiscriminate, and therefore, illegal.[44] This principle is commonly referred to as "proportionality", and along with distinction represents the fundamental principles of modern IHL.[45]

Article 51(5)(b) notably uses *damage* as opposed to *destruction*, which broadens the scope of its applicability as damage means "harm . . . impairing the value or usefulness of something"[46] and therefore inclusive of an act or acts "disrupting the functioning of certain systems by interfering with their underlying computer systems can amount to damage insofar as it impairs their usefulness".[47]

Yet even after determining the principle of proportionality ought to apply to cyber operations, cyber operations still pose a great challenge to the principle of proportionality. Military advantage is often complicated to calculate, and might be either biased or arbitrary, but assessing collateral damage after a conventional military operation is relatively straightforward. The same cannot be said for cyber operations. After all, once a malicious tool is released, there is little to no control over the eventual exposure,[48] and the subsequent physical, economic and societal effects that such malicious tool is capable of causing.[49] Moreover, cyber operations blur the line between collateral damage and inconveniences that are excluded from the scope of collateral damage. Cyber operations can cause new types of harms, including, but not limited to, disruption harms. However, the traditional rubric for damage assessment does not properly weight the new types of harm produced by cyber attacks.

Another critical difficulty is determining the temporal scope of the collateral damage anticipated. Since the effects of cyber operations can often materialize when certain time has elapsed, the exact proximity of the effects to the initial operation is highly ambiguous,[50] and this gap might be used by

---

44. AP I, *supra* note 13, at art. 51(5)(b) (emphasis added).

45. ROSCINI, *supra* note 8, at 219.

46. Cordula Droege, *Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT'L REV. OF THE RED CROSS 533, 559 (2012).

47. *Id.*

48. *See* DINNISS, *supra* note 17, at 203 ("Viruses and worms are two methods of computer network attack which are particularly likely to fall into this category [of indiscriminate attacks] as their effects are often not limited by their creators.").

49. *See* Karine Bannelier-Christakis, *Is the Principle of Distinction Still Relevant in Cyberwarfare?*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 343, 349-350 (Nicholas Tsagourias & Russell Buchan, eds., 2015) (comparing states with varying degrees of reliance upon cyberspace as a factor affecting the expected collateral damage).

50. *Id.* at 350.

some actors to claim that certain harms are too distant to be linked to the initial operation.

III. Disruptive Cyber Operations as a New Form of Violence

On May 2009, President Obama made a speech regarding the U.S. Cyber-Security Plan. During that speech he stated that cyber tools such as spyware, malware, spoofing, phishing, and botnets are all "weapons of mass disruption."[51] Weapons have always been considered to be destructive in nature. With his play on the more familiar term "weapons of mass destruction, Obama highlighted the different character of cyber threats while simultaneously underscoring the potential for certain cyber tools to cause wholesale destruction.

Modern weapons are now used for strategic and coercive purposes, may support ongoing military operations, or may have a sole purpose of causing harm, fear, and panic by terrorist organizations. There is now a new form of violence, not necessarily kinetic but more than a mere inconvenience.

So, what are "disruptive cyber operations?"

A. *Scope of "Disruptive"*

The scope of "disruptive" is best described by its contrast to "destructive." Disruptive cyber operations *do not* directly cause kinetic effects. Kinetic effects are either absent or cannot be causally linked to the initial cyber operation. Destructive cyber operations, however, directly cause kinetic effects.

While there is no widely recognized or otherwise authoritative definition of "disruptive cyber operations" there are some proposed definitions that are helpful in understanding the effects of "disruption." For example, the National Initiative for Cybersecurity Careers and Studies (NICCS) defines "disruption" in its glossary as "[a]n event which causes unplanned interruption in operations or functions for an unacceptable length of time."[52] The Michigan Cyber Disruption Response Strategy describes it as "an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability, of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the state economy, or diminish the security posture of the state."[53] Another definition, advanced by Brown and Tullos, simply provides

---

51. David Sanger & John Markoff, *Obama Outlines Coordinated Cyber-Security Plan*, N.Y. Times (May 29, 2009), http://www.nytimes.com/2009/05/30/us/politics/30cyber.html?_r=0.

52. *Explore Terms: A Glossary of Common Cybersecurity Terminology*, NICCS https://definedterm.com/a/download/document/11128 (last updated Feb. 10, 2015).

53. State of Michigan Executive Office, Michigan Cyber Disruption Response Strategy: Protecting Michigan's Critical Infrastructure and Systems 1 (2013),

that a "cyber disruption" is an action to "interrupt the flow of information or the function of information systems without causing physical damage or injury."[54]

There are several key factors to these definitions of disruptive cyber operations. First, there needs to be a certain event or incident beginning in cyberspace. That means that either the operation is initiated with the use of computer systems transmitting data packets, or a certain malicious tool is created separately, and is then distributed physically.

Second, the harm needs to be of an interruptive nature. It must make certain services, activities or functions unavailable as a result of the incident. There can be a wide variety of functions affected including access to critical information systems, access to the internet, access to certain computer networks, operating system malfunction. These effects, which are directly caused by the cyber operation, can result in second-order and even third-order effects.

Thirdly, the interruptive effects need to be of *violent* nature. Naturally, certain disruptions are more severe than others.[55] For example, taking down critical governmental websites is far more serious than taking down an online shopping website. Whether the disruption is *violent* will be determined contextually and on a case-by-case basis. That determination, however, should take into account three criteria: (1) the *essentiality* of the disrupted target to the day-to-day civilian lives; (2) the *scope* of disruption, the amount of individuals and organizations affected by the disruption; and (3) the *duration* of the operation, the presumption being that long-lasting effects are more likely to be *violent*.

1. Interruption in internet access and other services

Disruption may include interruptions to the Internet or to other online services. Access to the Internet and online services is essential to the proper functioning of societies throughout the world and IHL should protect their availability.

---

available at https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf.

54. Brown & Tullos, *supra* note 8.

55. *See* Droege, *supra* note 47, at 559 ("Yet, an overly broad interpretation of the term 'attack' would mean that all interferences with civilian computer systems would amount to attacks: the interruption of email or social network communications, of online booking or shopping systems, etc. To equate such disruptions of what are essentially communication systems with attacks would probably go beyond the scope of what was envisaged by the rules on the conduct of hostilities. These rules have traditionally sought to prevent damage to civilian infrastructure that manifests itself in the physical world, not interference with propaganda, communication, or economic life. In today's world, the reliance of civilian life on communication systems blurs these lines, and it is not easy to distinguish between what is 'mere' communication and what goes beyond.").

Consider a DDoS attack targeting the Rutgers University network that caused massive interruptions to Rutgers' Internet services.[56] University tools used both by students and faculty were unavailable due to that cyber-attack.[57] This type of cyber operation that interrupts Internet access in a major educational institution is disruptive and such disruption endangers the interest of the proper functioning of an academic institution.

If such a disruptive cyber operation took place in an armed conflict context, the consequences could be far-reaching. Therefore, it is vital to for IHL to protect civilians and civilian objects from these types of operations, even if there is no apparent destruction.

2. Functionality of computer systems

Disruptive cyber operations may also impair the functionality of computer systems and networks. Cyber operations that affect functionality of computers, computer systems, and networks may be causing effects very briefly, temporarily, or permanently. If the loss of functionality requires the replacement of hardware, then such cyber operation would be of destructive nature, because it caused physical damage to the components of the targeted computer system. If, however, such loss of functionality is due to a DDoS attack that floods the targeted system with requests, making it inoperable, the loss of functionality is either very brief, or temporary. Other types of attacks can cause loss of functionality for longer periods of time, say, if the tool used is a very sophisticated virus that interferes with proper functioning of the target system.

The discussion on whether functionality of computer systems qualifies as "attack" was debated by the International Group of Experts (IGE) of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. The *Manual* states –

> [T]here was [an] extensive discussion about whether interference by cyber means with the functionality of an object constitutes damage or destruction for the purposes of this Rule. Although some Experts were of the opinion that it does not, the majority of them were of the view that interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components. Consider a cyber operation that is directed against the computer-based control system of an electrical distribution grid. The operation causes the grid to cease operating. In order to restore distribution, either the control system or vital components thereof must be replaced. The cyber operation is an attack. Those experts

56. *See* Vernal Coleman, *Cyber Attack Causes Rutgers Internet Service Interruptions*, NJ.COM (Apr. 28, 2015, 10:23 AM), http://www.nj.com/middlesex/index.ssf/2015/04/cyber_attack_against_rutgers_causes_internet_servi.html.

57. *Id.*

> taking this position were split over the issue of whether the 'damage' requirement is met in situations where functionality can be restored by reinstalling the operating system.[58]

According to the *Tallinn Manual* experts, the loss of functionality can only be an "attack" if it is linked physical damage. This assertion, however, misses the point of functionality of computer systems as a standalone value. That is, we want to protect computer systems from functionality loss, regardless of physical damage that may or may not be linked to it.

3. Data manipulation, alteration, or deletion

Certain disruptive cyber operations might target data, whether the data resides in certain computer systems, online or in classified networks. As UK Cyber Security Strategy points out, "a growing number of adversaries are looking to use cyberspace to steal, compromise or destroy critical data. The scale of our dependence means that our prosperity, our key infrastructure, our places of work and our homes can all be affected."[59] Data is becoming central in nearly every society, and if compromised, it can pose a greater threat to national security and the wellbeing of civilians in general.

The *Tallinn Manual* dealt with the scenario of data being the target of an attack, presenting the opinion of few IGE members:

> "A few Experts went as far as to suggest that interference with functionality that necessitates data restoration, while not requiring physical replacement of components or reinstallation of the operating system, qualifies as an attack. For these Experts, *it is immaterial how an object is disabled; the object's loss of usability constitutes the requisite damage*".

This, however, represents the minority view. The majority believes that cyber operations that alter or destroy civilian data without generating these consequences are not attacks under the current state of law, and are, in fact, lawful.[60]

---

58. INTERNATIONAL GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 108 (Michael N. Schmitt ed. 2013).

59. UNITED KINGDOM CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN THE DIGITAL WORLD 15 (2011), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

60. *See* Michael Schmitt, *The State of Humanitarian Law in Cyber Conflict*, JUST SECURITY (Jan. 6, 2015, 2:50 PM), https://www.justsecurity.org/18891/state-humanitarian-law-cyber-conflict/.

Assuming data is an *object*, operations against civilian data would be prohibited. The question of whether data can qualify as "civilian object," however, is subject to extensive debates.[61]

B. *Modern Reinterpretation of Violence*

The key to incorporate disruptive cyber operations within the scope of "attack" under IHL is to interpret "acts of violence" as including cyber operations with disruptive effects. This is easily achieved because of society's dependence on information systems.[62] Any tempering with the functionality of these systems should be regarded as violence because it can be just as harmful as the use of physical force.

The argument that "violence" is sufficiently broad to incorporate disruptive activities and effects should be substantiated by contemporary international law on treaty interpretation. The Vienna Convention on the Law of Treaties ("VCLT") provides the framework for interpreting treaties, as well as the conclusion, observance, and application of treaties. Therefore, in order to understand the term "violence," to aid in the understanding of "attack" and the inclusion of disruptive cyber operations in IHL, one must interpret it within the VCLT framework.

1. General Rule of Interpretation

The "general rule of interpretation" according to the VCLT is textual.[63] Article 31(1) of the VCLT reads as follows: "a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and purpose."[64] The International Court of Justice reaffirmed that if the ordinary meaning of a term is clear, that should suffice for interpretational purposes.[65] When the

---

61. For more on this debate, *see, e.g.*, Michael Schmitt, *The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision*, 48 ISR. L. REV. 81 (2015) (arguing that data should not be characterized as an object in itself); Kubo Macak, *Military Objectives 2.0: The Case for Interpretive Computer Data as Objects under International Humanitarian Law*, 48 ISR. L. REV. 55 (2015) (arguing that data out to be an 'object'); Heather Harisson Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives,* 48 ISR. L. REV. 39 (2015) (arguing that data should be recognized as object to better protect civilians).

62. *See* NAT'L RES. COUNCIL OF THE NAT'L ACADEMIES, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 253-54 (William A. Owens et al. eds., 2009).

63. *See* BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 379 (James Crawford ed., 8th ed. 2012).

64. Vienna Concention on the Law of Treaties, art. 31(1), Jan. 27, 1980, 1155 U.N.T.S. 331, 8 I.L.M. 679 [hereinafter VCLT].

65. *See, e.g.*, Competence of the General Assembly for the Admission of a State to the United Nations, 1950 I.C.J. 5, 8 (May 30) ("if the relevant words in their natural and ordinary meaning make sense in their context, that is an end of the matter.").

ordinary meaning is unclear, however, Article 31(2) of the VCLT provides sources that may be used to aid the interpretation.[66]

a. Violence Generally

The basic premise of the law of treaties is that natural and ordinary meaning of terms is the first step in the process of interpreting treaties. The Oxford Dictionary defines "violence" as a "the deliberate exercise of physical force against a person, property, etc.; physically violent [behavior] or treatment; (Law) the unlawful exercise of physical force, *intimidation* by the exhibition of such force."[67] The French definition of 'violence', which is equally authoritative as the English one,[68] is defined *inter alia* as physical or *moral coercion*, exerted on a person with the purpose of inducing him to perform a certain action.[69] As evidenced by these definitions includes actions that are not necessarily physically forceful.

The ordinary meaning of treaty terms is often insufficient to establish authoritative interpretation. Therefore, interpretation sometimes requires an examination of the context, including relevant treaty text, preambles, and annexes. The argument that "violence" should be interpreted broadly is supported by Article 51(1) of Additional Protocol I, which provides that "the civilian population and individual civilians shall enjoy general protection against *dangers* arising from military operations."[70] The Commentary defines *military operations* as "all the movements and activities carried out by

---

66.

> *2. The context for the purpose of the interpretation of a treaty shall comprise, in addition to the text, including its preamble and annexes:*
>
> (a) Any agreement relating to the treaty which was made between all the parties in connection with the conclusion of the treaty;
>
> (b) Any instrument which was made by one or more parties in connection with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty.
>
> 3. There shall be taken into account, together with the context:
>
> (a) Any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions;
>
> (b) Any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation;
>
> (c) Any relevant rules of international law applicable in the relations between the parties.
>
> 4. A special meaning shall be given to a term if it is established that the parties so intended. VCLT, supra note 65, at art. 31(2).

67. Oxford English Dictionary (2d ed. 1989).

68. *See* VCLT, *supra* note 65, art. 33(1) ("When a treaty has been authenticated in two or more languages, the text is equally authoritative in each language, unless the treaty provides or the parties agree that, in case ofdivergence, a particular text shall prevail.").

69. Dictionnaire de Français, LaRousse, *available at* http://www.larousse.fr/dictionnaires/francais/violence/82071?q=violence#81105 ("Contrainte, physique ou morale, exercée sur une personne en vue de l'inciter à réaliser un acte déterminé.").

70. AP I, *supra* note 13, at art. 51(1) (emphasis added).

armed forces related to hostilities," and explains that "there is no doubt that armed conflicts entail dangers for the civilian population, but these should be reduced to a minimum."[71] Additionally, Article 57(1) of Additional Protocol I states: "[i[n the conduct of *military operations*, constant care shall be taken to spare the civilian population, civilians and civilian objects."[72] Though in that case, several experts make the argument that "military operations" and "attacks" are synonyms, which signifies that "military operations" is not broader in scope compared to "attacks."[73] In both provisions, the term "attack" is not used, suggesting that civilians ought to be protected from a wide array of operations.

In a different context, "cyber violence" (also known as "online bullying") was recently compared by the U.N. to physical violence: "cyber violence is just as damaging . . . as physical violence."[74] That is an example of how cyberspace changes the traditional notion of violence, and given that violence can take a multitude of forms other than physical.

b. Violence in Cyberspace

So, what constitutes violence in cyberspace? Obviously, not all cyberspace operations or activities are "violent" by their nature. Certain cyber operations or activities may be violent, however, if they cause kinetic effects or if they cause disruptive effects. Therefore, in cyberspace, violence is any effect that is either kinetic or disruptive.[75]

Thomas Rid, leading cyber warfare scholar and author of "Cyber War Will Not Take Place" tackled this very question. Rid reached the conclusion that cyber operations are almost always non-violent.[76] Rid recognized that cyberspace might be changing the notion of violence, and that it depends on where the line is drawn between violence and non-violence.[77] Rid's narrow reading of violence is what leads him to the conclusion that cyber operations are non-violent in nature, as their violent effects are only materializing indirectly.[78] His conclusion, though contrary to the argument in this paper, is apt,

---

71. The Commentary, *supra* note 14, at paras. 1935–36.

72. AP I, *supra* note 13, at art. 57(1) (emphasis added).

73. Schmitt, *supra* note 61, at 93.

74. Charlotte Alter, *U.N. Says Cyber Violence is Equivalent to Physical Violence Against Women*, TIME (Sept. 24, 2015), http://time.com/4049106/un-cyber-violence-physical-violence/ ("The U.N. defines violence against women as "any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts." The report notes that cyber violence is an extension of that definition that includes acts like trolling, hacking, spamming, and harassment.").

75. *See* SCHMITT, *supra* note 61, at 290 ("A careful reading of Additional Protocol I's prohibitions and restrictions on attacks discloses that the concern was not so much with acts which were violent, but rather with those that have harmful consequences (or risk them), in other words, violent consequences.").

76. Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD. 5, 11 (2012).

77. *Id.*

78. *Id.*

due to him drawing the line between violence and non-violence based on direct physical effects. Rid's assertion that most cyber operations are not violent (i.e., lacking physical effects) is correct. However, that should lead to the conclusion that IHL should address these operations when directed against civilians. Therefore, the inclusion of these operations within the scope of "attack" is necessary in order to avoid a scenario where these operations are used widely against civilians, with no restriction on IHL's behalf.

Nils Melzer illustrated the difficulty in drawing a line between violence and non-violence. He stated that "it would hardly be convincing to exclude the non-destructive incapacitation of a state's air defense system or other critical military infrastructure from the notion of attack simply because it does not directly cause death, injury or destruction." As persuasive as Melzer's perspective is, it does not solve the disruptive cyber operations question.[79]

i. Diffusion of Power in Cyberspace

There are two broader phenomena that should be noted with regard to the changing notion of violence in cyberspace: (1) diffusion of power in cyberspace; and (2) cyberspace allows for a broader spectrum of violence. The first is the diffusion of power in cyberspace. States no longer have a monopoly over power when it comes to cyberspace and more non-state entities are becoming involved in cyberspace activities on a large-scale. Joseph Nye eloquently summarized it by saying that "[a]nyone from a teenage hacker to a major modern government can do damage in cyber space",[80] While states will remain the dominant actor on the world stage, they will find the stage far more crowded and difficult to control.[81]

This phenomenon could imply that states should be in favor of broadening the scope of "acts of violence." States should support this because a variety of non-state actors may exploit this lacuna by carrying out disruptive cyber operations against civilians and escaping any accountability that IHL could have imposed.[82] International law, which is based mostly on the cen-

79. Droege, *supra* note 47, at 555 ("Melzer's argument is attractive in that it gives effect to the very object and purpose of the rules on the conduct of hostilities, which is that 'innocent civilians must be kept outside hostilities as far as possible and enjoy general protection against danger arising from hostilities'. However, it leaves open the most critical question, namely whether operations that disrupt civilian infrastructure without destroying it fall under the concept of hostilities.").

80. JOSEPH S. NYE, JR., CYBER POWER 11 (Harv. Kennedy Sch., Belfer Center for Sci. and Int'l Aff. ed., 2010), *available at* http://belfercenter.hks.harvard.edu/files/cyber-power.pdf.

81. *Id.* at 1.

82. Even when the direct participation in hostilities framework is concerned (the framework that deals with civilians who engage in hostilities, and whether their acts can result in forfeiture of their protected status, thus making them targetable with lethal force), these non-state actors who use disruptive cyber operations will not be targetable because disruptive cyber operations against civilians will not reach the threshold of harm provided by the framework due to its focus on physical effects (death, injury, and physical destruction) on civilians. *See*

trality of state sovereignty and the state monopoly on physical force,[83] should keep up with the diffusion of power in cyberspace.

The second phenomenon provides that cyberspace allows for a broader spectrum of violence to emerge. As a result, certain longstanding categories are beginning to erode: "violence is no longer solely physical, distinctions between violence inflicted by state and non-state actors is less clear, and physical territory is less fundamental."[84] Some even claim that Internet itself is a new form of violence.[85] International law must change as violence in cyberspace evolves.

2. Panama's Proposal

On January 4, 1999, the U.N. General Assembly adopted a resolution on "[d]evelopments in the field of information and telecommunications in the context of international security."[86] This resolution invited U.N. Member States to submit responses to the Secretary General, informing their views.

(a) General appreciation of the issues of information security;

Ido Kilovaty, *ICRC, NATO AND THE U.S. – Direct Participation in Hacktivities – Targeting Private Contractors and Civilians in Cyberspace under International Humanitarian Law*, 15 DUKE L. & TECH. REV. 1 (2016).

83. *See* SAMULI HAATAJA, TECHNOLOGY, VIOLENCE AND LAW: CYBER ATTACKS AND UNCERTAINTY IN INTERNATIONAL LAW 319 (2013), *available at* http://www.academia.edu/6776442/Technology_Violence_and_Law_Cyber_Attacks_and_Uncertainty_in_International_Law ("Due to technological change, there has been a diffusion of power in cyberspace and states are no longer able to maintain a monopoly of violence in this realm. Thus power relationships are changing, though international law remains premised on a different technological environment in which state power is supreme. As the technological change reflected in the Estonia incident demonstrates, a new technological environment has been made apparent in which states are no longer the sole actors capable of engaging in an effective form of wide scale violence. Nor is it always clear when a state is involved in acts of violence as the current technological environment makes it easy to mask one's identity and thus blurs traditional legal distinctions of acts for which states may be responsible for. Consequently, there is not just uncertainty about how existing legal doctrine on state responsibility should apply or what legal regime cyber attacks should be categorised into. There is also uncertainty as to the ability of international law, structured around the centrality of sovereign states and based on the assumption that states are the only actors technologically capable of maintaining a monopoly of violence, to regulate behaviour in cyberspace where power is more diffused, violence is no longer solely physical, distinctions between violence inflicted by state and non-state actors is less clear, and physical territory is less fundamental. This raises questions about the significance of territoriality, physicality and violence to sovereignty and international law, and reinvigorates one of the central concerns of international law – its ability to control international violence.").

84. *Id.* at 320.

85. Merritt Baer, *Cyber Disarmament Treaties and the Failure to Consider Adequately Zero-Day Threats*, *in* PROCEEDINGS OF THE 8TH INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY 255, 257 (Doug Hart ed., 2013).

86. G.A. Res. 53/70, U.N. Doc. A/RES/53/70 (Jan. 4, 1999).

(b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;

(c) Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality.[87]

On June 24, 2002, Panama submitted its response to the Secretary General, which although brief, managed to present several highly persuasive propositions. First, Panama argued that the focus on kinetic effects of cyber operations is flawed, because today computers regulate many critical aspects such as emergency services, air traffic, and financial information, and therefore, "an attack in which new information and telecommunications technologies are employed may cause more damage than, for instance, a conventional bombardment."[88] Second, Panama argues that this threat "requires protection systems tailored to this *new form of violence.*" Panama is correct in the assumption that new types of attacks, using information and telecommunications technologies, can cause more harm than conventional attacks.

The core of Panama's proposal is to rethink violence. Violence in the modern, digital age is a different phenomenon entirely compared to traditional forms of violence. While Panama does not argue in the context of IHL, its argument is helpful in the sense that the "ordinary meaning" of violence is changing. This idea supports the notion that disruptive cyber operations should be included in the scope of "attack."

IV. Normative and Practical Implications of Disruption as "Attacks"

Including disruptive cyber operations within the ambit of "attack" has a variety of normative and practical implications. The most obvious is that they cannot be directed at civilians or civilian objects. But there are additional, less obvious implications, which must be acknowledged. First, it would make disruptive cyber operations subject to the *duty to code humanely*, to design all cyber operations, whether disruptive or destructive, in a way that discriminates between military and civilian targets. Second, it is essential to rethink the proportionality equation. Illegitimating civilian *disruption* harm under the auspices of IHL leads to its inclusion under the proportionality analysis, which typically seeks to limit collateral damage to

87. *Id.* at 2.

88. Panama's Response to Developments in the Field of Information and Telecommunications in the Context of International Security, G.A. Res. A/57/166/Add.1, at 5 (Aug. 29, 2002).

civilians, and; Third, the argument made by this paper should be compared and contrasted to existing frameworks dealing with similar issues, namely the U.S. Department of Defense Law of War Manual, The Tallinn Manual, and the UN Governmental Group of Experts Report.

A. *The Duty to Code Humanely*

The *duty to code humanely* implies that parties to a conflict are under obligation to design their cyber operations in accordance with the prohibition on *indiscriminate attacks*. As discussed above, the prohibition is concerned with attacks that are unable to discriminate between military and civilian targets. When attacks are unable to discern between military and civilian targets, it increases the likelihood of harming civilian targets. In order to distinguish between protected civilians and ilitary targets, adversaries will be required to take additional steps to ensure compliance. .[89]

If disruptive cyber operations are indeed "attacks," then the prohibition on *indiscriminate attacks* would apply to these cyber operations as well. Therefore, the duty to code humanely is applicable to a broader set of cyber operations. That is, not only destructive cyber operation, but also disruptive cyber operations. This broad inclusion is making the determination of IHL compliance easier, since coding humanely is to be a prerequisite of nearly all cyber operations. In addition, this may set the standard of due diligence in designing cyber operations, which is so desperately needed today.[90]

The U.S. Marine Corps Counterinsurgency Field Manual does not use "attack" when defining "discrimination," in the context of IHL, by providing that:

> Discrimination requires combatants to differentiate between enemy combatants, who represent a threat, and noncombatants, who do not. In conventional operations, this restriction means that combatants cannot intent to harm noncombatants, though proportionality permits them to act, knowing some noncombatants may be harmed.[91]

A "humane" cyber operation is one in which the operation is designed to only cause harm to specified computer systems and networks. For example,

---

89. *See* AP I, *supra* note 13, at art. 51(4).

90. *See* Michael Schmitt, *In Defense of Due Diligence in Cyberspace*, Yale Law Journal Forum (Jun. 22, 2015) – "Furthermore, although the precise threshold of harm at which the duty arises is unclear in law,37 there has been no suggestion from any quarter that the duty extends to mere irritation or inconvenience, such as defacement and temporary minor denials of service. Rather, harm must rise to such a level that it becomes a legitimate concern in interstate relations and, thus, an appropriate subject of international law rights and obligations.", quoting Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1911, 1963 (Arb. Trib. 1941), available at http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace."

91. Dep't of the Army, U.S. Army and Marine Corps Counterinsurgency Field Manual 7-7, para. 7-34 (2006), *available at* http://usacac.army.mil/cac2/Repository/Materials/COIN-FM3-24.pdf.

if it is known that a certain military objective uses computer systems of a particular manufacturer, having very specific software and properties, it will be easier to design a human cyber operation that will only cause effects to computer systems meeting these parameters, while others will be spared. That will give effect to the protection from indiscriminate attacks, and will enhance the discriminative aspect of cyber operations.[92] As summarized by Bill Boothby, leading IHL expert and Deputy Director of Legal Services at the British Royal Air Force:

> [T]he critical issue . . . is whether the cyber weapon limits its damaging effect reasonably to the intended target, that is, to the cyber node or to the part of the network that is the military objective. In this regard, for example, worms, viruses and other malware that spread their effects uncontrollably may cause damage to other, civilian computer systems, and if the consequence is that their nature is to strike military objectives and civilians or civilian objects without distinction, then the cyber weapon will be indiscriminate by nature and thus unlawful.[93]

Duncan Hollis, law professor at Temple University and IHL expert adds that "malware of various types can quickly be distributed world-wide. Without careful planning cyber operations may be indiscriminate or cause harms greater than expected or necessary to achieve their military objective."[94] That connects to a possible problem related to lack of careful planning of cyber operations, which can ultimately harm unintended targets, while also violating bedrock principles of IHL.

Lack of careful planning can also lead to loss of control over the initial cyber operation, because once viruses or worms are unleashed, they "can quickly spiral out of control, infiltrating civilian systems and causing damage to property that far surpasses the intent of the cyber attacker."[95] Careful planning stems from a commander's obligation to make a decision based on

---

92. *See* Eric Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INT'L L. STUD. 198, 203 (2013) ("When employing a cyber tool or conducting cyber operations, the commander would need to maintain oversight of the tool and be ready to adjust operations if the tool or operation began to have effects that the commander determined would have an illegal impact on civilians. This might be especially difficult in the cyber domain since virtually every cyber operation will traverse, affect, employ or damage civilian cyber infrastructure of some kind.").

93. William H. Boothby, *Where do Cyber Hostilities Fit in the International Law Maze?*, *in* NEW TECHNOLOGIES AND THE LAW OF ARMED CONFLICT 59, 68 (Hitoshi Nasu & Robert McLaughlin eds., 2014).

94. Duncan B. Hollis, *Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, *in* CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 129, 170 (Jens David Ohlin et al. eds., 2015).

95. Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 570 (2012).

all available information, and to collect the best intelligence given the circumstances.[96] It is based on the precaution in attack principle, which obligates parties to an armed conflict to take feasible measures to ensure that civilian targets are sufficiently protected. The Additional Protocol I provides: "in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects"[97] and therefore, adversaries are requested to "take all *feasible precautions* in the choice of means and methods of attack with a view to *avoiding*, and in any event to *minimizing*, incidental loss of civilian life, injury to civilians and damage to civilian objects".[98]

The standard of the precaution principle is "feasibility," meaning that the required measures are "practicable or practically possible, taking into account all the circumstance ruling at the time, including humanitarian and military considerations."[99] In that regard, ICRC legal adviser Cordula Droege posited that the precautionary principle "will require verifying the nature of the systems that are being attacked and the possible damage that might ensue from an attack. It also means that when it becomes apparent that an attack will cause excessive incidental civilian damage or casualties, it must be cancelled."[100] Droege argues that "the use of a worm that replicates itself and cannot be controlled, and might therefore cause considerable damage to civilian infrastructure, would be a violation of IHL."[101]

Some experts claim that because disruptive cyber operations are non-lethal there is incentive not to comply with IHL. Jeff Kelsey argued that "the potentially non-lethal nature of cyber weapons may cloud the assessment of an attack's legality, leading to more frequent violations of the principle of distinction in this new form of warfare than in conventional warfare."[102] This illustrates that the duty to code humanely is critical to disruptive cyber oper-

96. *See* Dieter Fleck (ed.), The Handbook of International Humanitarian Law (2013), para. 443, comm. 7 (Stating that "Exact reconnaissance and the procurement of precise information by military intelligence services become key factors of lawful warfare. The technologically and institutionally highly developed military organizations of the industrial states could probably manage these requirements;338 military actors without efficient means of reconnaissance and intelligence, however, will encounter serious difficulties in meeting the requirements of Article 52, para. 2, AP I [requirement of attacks only against military objectives] Also, stating that "The command authorities responsible for planning and deciding upon an attack must employ all means of reconnaissance and intelligence available to them unless and until there is sufficient certainty of the military nature of the objective of an attack".)

97. AP I, *supra* note 13, at art. 57(1).

98. AP I, *supra* note 13, at art. 57(2)(a)(ii) (empahsis added).

99. Holis, *supra* note 95, at 160.

100. Cordula Droege, Legal Advisor, Int'l Comm. of the Red Cross, No Legal Vaccum in Cyber Space (Aug. 16, 2011), *available at* https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm.

101. *Id.*

102. Jeffrey T. G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 Mich. L. Rev. 1427, 1439 (2012).

ations, even though it applies equally to destructive cyber operations. To avoid this negative incentive to comply with IHL principles, disruptive effects need to be addressed and covered by IHL.

It must be noted, that even the best cyber operation designers may be prone to human error and unforeseen consequences.[103] This is, however, not specific to cyber operations as errors may occur in the non-cyber realm as well. If the cyber operation is designed humanely there is a reduced risk that such operation will be indiscriminate.[104] Additional challenge to the *duty to code humanely* is the dual-use reality, in which many cyber infrastructure targets are used both by civilians and the military. As eloquently described by prominent IHL scholars Robin Geiβ and Henning Lahmann –

> "Whereas it is technically possible to distinguish virtual targets in cyberspace – meaning that a hyper-distinctive attack against a military network is certainly realistic – the application of the accepted legal definition of military objectives in the interconnected cyber domain will render basically every cyber installation a legitimate military objective. In cyberspace, every component of the cyber infrastructure is a dual-use object".[105]

This challenge is not cyber-specific, as contemporary conflicts exacerbate the difficulty to distinguish between military and civilian objectives.

1. Case study – Stuxnet: Humane Cyber Operation

In 2010, the computer networks of the Iranian nuclear research facility in Natanz were infected by a malware, which caused unexpected detrimental physical destruction. The *Stuxnet* virus, which infected the Iranian nuclear plant, caused damage to the uranium-enriching infrastructure by making the centrifuges spin out of control up to the point that they become irreversibly damaged. This was achieved by a so-called "semantic cyber attack," which manipulates the output of the targeted system, by showing incorrect informa-

---

103. *See* Erki Kodar, *Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I*, 15 ENDC PROCEEDINGS 107, 121-22 (2012).

104. *Id.* at 121 ("The difficulty of cyber attacks is that, to be conducted legally, they have to be of high sophistication so as not to violate the requirements of LOAC. But a cyber attack can easily, either intentionally or through a human or technological mistake, transform into an indiscriminate attack. If a belligerent programs a virus the sole purpose of which is to replicate in IT systems, infect as many computers as possible and destroy all the data on infected machines, then it would be hard to argue that such a cyber attack is in accordance with LOAC. In this example, the cyber attack (virus) would be uncontrollable and spread through military and civilian systems alike, constituting an indiscriminate attack. Therefore, a cyber attack must be of high sophistication and adhere to the principle of distinction and to LOAC in general.").

105. Robin Geiβ & Henning Lahmann, *Cyber Warfare: Applying the Principles of Distinction in an Interconnected Space*, 45(3) ISR. L. REV. 381, 382-83 (2012).

tion.[106] As a result, the Stuxnet attack damaged the centrifuges, which were spinning until they broke, while the computer systems of the facility showed that the centrifuges operate normally.[107]

Stuxnet is an example of how diligent and "humane" design of a cyber operation can end up achieving a military objective, without harming any civilians or civilian objects. Stuxnet was very cleverly designed to only harm computer systems manufactured by Siemens, having very specific configurations, in order to limit the effects to the computers resident at the nuclear plant in Natanz. When the worm infected these systems, it forced the centrifuges to speed up to a speed that essentially destroys those centrifuges. Otherwise, if the worm does not detect these specific configurations, it does not cause any effects at all, other than just existing on that computer system. In that context, experts concluded that "Stuxnet satisfies the criteria of distinction because the worm was designed for a specific military target – assuming the Natanz plant is not a civilian nuclear energy program – and did not indiscriminately destroy civilian computer systems."[108]

Stuxnet was not carried out in an armed conflict context, and, thus, was not evaluated under IHL norms and principles. Similar operations could take place during an armed conflict in the future, and it is then that the lessons from Stuxnet may be valuable for the purposes of protecting civilians and civilian objects from attacks. In addition, Stuxnet was both a disruptive and destructive cyber operation. The disruptive part manipulated the computer systems to show that the centrifuges are functioning properly, while the destructive resulted in irreversibly damage to the centrifuges. In that sense, Stuxnet is not a purely disruptive cyber operation, and here again, lessons regarding practice relating to *disruptive cyber operations* cannot be made necessarily. Finally, Stuxnet infected a variety of additional targets, but these were not damaged. Some claim that these "constant care" standard operation may suggest an emerging state practice on the duty to code humanely.[109]

B. *Rethinking the Proportionality Analysis*

The proportionality analysis (discussed *infra*) compares military advantage with incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof ("collateral damage") and prohibits

106. *See* Martin C. Libicki, What is Information Warfare? 77 (1995) ("A system under semantic attack operates and will be perceived as operating correctly, . . . but it will generate answers at variance with reality.").

107. *See* Oona Hathaway et al., *The Law of Cyber-Attack*, 100 Cal. L. Rev. 817, 819, 828 (2012).

108. Gervais, *supra* note 96, at 571.

109. *See* Jensen, *supra* note 93, at 203 ("[R]eports show that it spread much wider than that, presumably wider than the United States and Israel intended it to disseminate, which may have led to its discovery. Though no other damage was reported, the unintended spread of the virus at least implicates the constant-care standard and informs State practice on the issue.").

attacks that are expected to result in excessive collateral damage as opposed to the military advantage anticipated.[110] The meaning of the proportionality analysis, is that even if the cyber operation was coded humanely, it still does not mean that it is proportional.

If disruption is included in the scope of "attack," then it is inevitable for disruptive *effects* to be included as part of the collateral damage belonging to the proportionality analysis. In literature, a proportionality analysis that takes into account the *disruption* collateral damage is not uncommon.[111] The reason for that would be that simply including disruptive cyber operations within the ambit of attacks would not protect civilians from these operations, as it will be legal under IHL to cause *disruptive incidental* damage, if the attack is discriminate and not directly carried out against civilians. The matter really boils down to whether destructive or *disruptive cyber operations,* against military objectives should cause *proportionate disruptive* and other damages to civilians and civilian objects.

Eric Jensen proposes that IHL consider collateral damage employing the *functionality* approach.

> [S]ome have taken the view that damage also encompasses serious interruptions in functionality, such as would require replacing parts or reloading software systems. For example, in the kinetic analogy used above where a cyber attack shut down a communication port but left the rest of the computer unaffected, the computer would still turn on but its actual functionality might be seriously affected. If functionality is considered when determining damage, the kinetic analogy would be of limited value. The functionality approach seems to be the best application of the proportionality rule to the cyber realm as it takes into account the unique aspects of cyber operations, without going so far as to make the proportionality analysis unwieldy for commanders to apply. Armed conflict has always included effects on civilians that have caused inconvenience, irrita-

110. 1 Int'l Comm. of the Red Cross, Customary International Humanitarian Law 46 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., Cambridge Univ. Press 2005) ("Proportionality in Attack: Rule 14. 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, is prohibited.").

111. *See* Herb Lin, *Cyber Conflict and International Humanitarian Law*, 94 Int'l. Rev. Red Cross 515, 526 (2012) ("Under the provisions related to proportionality, some degree of collateral damage is allowable, but not if the 'expected' collateral damage is disproportionate compared to the 'anticipated military advantage'. 16 If, for example, a power plant is the target of a cyber attack, an assessment must be made as to whether the harm to the civilian population caused by disruption of electrical service is not disproportionate to the military advantage that might ensue from attacking the plant. Before such an assessment could be made, the commander would have to have adequate intelligence about the plant (and what was dependent on the plant) on which to base the judgement.").

> tion, stress and fear, but these have traditionally not been part of the commander's analysis of damage required by the proportionality analysis. By focusing on functionality, the commanders can easily understand the legal standard and apply it to modern cyber operations.[112]

The functionality seems to make sense. It includes not only physical collateral damage, but also damage in the form of loss of functionality, whether "replacing parts or reloading software systems." However, disruption that does require replacing parts or reloading software should be included. For example, disruption due to a DDoS attack on a specific governmental website does not result in reloading software or replacing any hardware parts, but requires either waiting it out, or attacking the source(s) of the DDoS attack to stop its disruptive effects.

The primary shortcoming of a narrow reading of collateral damage is that the most severe disruptive cyber operations would be far more humanitarianly dangerous than physical destroying a house belonging to a civilian.[113] That is to say, that disruption effects can be far more serious than physical ones. In that sense, reconsidering the scope of collateral damage is essential.

C. *The Persistent Problem with Operations against Data*

Data as a target of cyber operations poses a very specific, complicated challenge. Even if we consider cyber operations targeting data as "attacks," the remaining question is whether data can constitute an "object," because

---

112. Jensen, *supra* note 93, at 206-07.

113. See Geiβ & Lahmann, *supra* note 105105, at 397 (offering a similiar example, explaining that, "It would appear counter-intuitive that only the physical destruction of a civilian object should be taken into consideration, whereas functionality loss – even if it affects the civilian population much more severely – should be irrelevant. Indeed, a narrow reading of the phrase 'damage to civilian objects' that is limited to physical destruction would lead to the following result. Whereas the destruction of a single civilian car would amount to legally relevant, albeit rather insignificant, 'collateral damage', the disconnection of thousands or millions of households, companies and public services from the internet or other communication services, or the severance of online financial transactions for a country's entire economy and the corresponding economic and societal effects as such would not count as relevant elements to be factored into the proportionality calculus. Only when and where these effects foreseeably resulted in the loss of civilian life, injury to civilians or damage to civilian objects could they be considered as factors relevant for the proportionality calculus.70 Given that it is extremely difficult to determine in advance what the foreseeable physical effects of a large-scale attack against cyber infrastructure components may be – in the interconnected domain of cyberspace such operations may have a number of cascading effects that are hard to predict – the inclusion of direct effects such as the loss of functionality into the list of proportionality-relevant factors would greatly facilitate the application of the proportionality principle, especially in the cyber domain. Evidently, the more cyber-reliant a society is – and in the future this reliance will only increase in a growing number of states – the more detrimental the effects of such functionality loss on the civilian population will be.").

the distinction principle only protects "civilian *objects*" from direct attacks. The classification of data as an object (or non-object) is essential to its protection in the civilian context. In other words, critical civilian data may be compromised if IHL fails to classify data as an *object* protected from direct attacks.[114]

The absolute exclusion of data from the scope of "object" appears in the *Tallinn Manual*. Rule 37 of the *Tallinn Manual* provides that "[c]ivilian objects shall not be made the object of cyber attacks. Computers, computer networks, and cyber infrastructure may be made the object of attack if they are military objectives."[115] Rule 38 of the *Tallinn Manual* adopts some of Additional Protocol I provisions, and provides that:

> Civilian objects are all objects that are not military objectives. Military objectives are 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. Military objectives may include computers, computer networks, and cyber infrastructure.[116]

The *Tallinn Manual* experts found that "the meaning of the term 'object' is essential in understanding this and other Rules found in the *Manual*. An 'object' is characterized in the ICRC Additional Protocols Commentary as something 'visible and tangible.' "[117] The IGE continued their commentary by adding that an ". . .object should not be interpreted as data. Data is intangible and therefore neither falls within the 'ordinary meaning' of the term object."[118] This assertion is counterintuitive, and does not conform with technological and societal developments taking place in the last few decades.

Similarly, Prof. Schmitt, argues that "data should not be characterized as an object in itself."[119] Schmitt argues that operations against data could be a violation of the principle of distinction if "the consequences attendant to its

---

114. For more on this debate, *see, e.g.*, Michael Schmitt, *The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision*, 48 ISR. L. REV. 81 (2015) (arguing that data should not be characterized as an object in itself); Kubo Macak, *Military Objectives 2.0: The Case for Interpretive Computer Data as Objects under International Humanitarian Law*, 48 ISR. L. REV. 55 (2015) (arguing that data out to be an 'object'); Heather Harisson Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives,* 48 ISR. L. REV. 39 (2015) (arguing that data should be recognized as object to better protect civilians).

115. INTERNATIONAL GROUP OF EXPERTS, *supra* note 59, at 124.

116. INTERNATIONAL GROUP OF EXPERTS, *supra* note 59, at 125.

117. INTERNATIONAL GROUP OF EXPERTS, *supra* note 59, at 126 (Commentary 4 to Rule 38); *see also* INT'L COMM. OF THE RED CROSS, *supra* note 14, at para. 2008.

118. INTERNATIONAL GROUP OF EXPERTS, *supra* note 59, at 127 (Commentary 5 to Rule 38).

119. Schmitt, supra note 75, at 96.

destruction involve the requisite level of harm to protected physical objects or persons."[120] Although Schmitt's approach on data as object might seem as data-inclusive, it is in fact a data-exclusive. Schmitt argues that data should be seen as object only if there are physical manifestations to the manipulation or destruction of such data. Therefore, Schmitt does not view the data as valuable for civilian knowledge, information, order and well-being, that is, data as having an intrinsic value.[121] In his riposte piece, Schmitt simply argued that "Since data is not an object, then on that basis it is not subject to the prohibition on attacking civilian objects; it is instead necessary to look to the consequences of its damage or destruction to determine whether the prohibition applies."[122] That approach is somewhat dated, in the sense that digital data is a relatively new concept, when compared to the notions held by IHL years and years ago.[123]

Prof. Heather Dinniss, among the leading cyber warfare scholars, holds a similar view, by arguing that code, that is, a type of data, "may qualify as a military objective by providing an effective contribution to military action either through its nature, location, purpose or use."[124] Dinniss argues that:

> [I]n today's world of increasing virtualisation and extensive interdependence between military and civilian infrastructure, requiring tangibility results in a manifestly unreasonable result. Such a result is inconsistent with other treatments of intangibility in international humanitarian law and contrary to the expressed purpose of providing effective protection to civilians and civilian objects.[125]

A minority among the International Group of Experts, as part of the commentary to Rule 38 of the *Tallinn Manual*, argued that "data *per se* should be regarded as an object. In their [minority Experts] view, failure to do so would mean that even the deletion of extremely valuable and important civilian datasets would potentially escape the regulatory reach of the law

120. *Id.*

121. *See id.* Though Schmitt does make some effort to address data with intrinsic value – "some data have intrinsic value. An example would be digital art. If the data are destroyed, the art is as well," that approach is still under-inclusive as it disregards massive amounts of data with intrinsic value that are not art.

122. Schmitt, *supra* note 75, at 97.

123. *See* Macak, *supra* note 114, at 67 (arguing that, in accordance with the Vienna Convention on the Law of Treaties (VCLT), the term 'object' should be interpreted to encompass data, by providing that Tallinn Manual's use of ICRC Commentary definition of an object as "visible and tangible" is dated, mainly because the possibility of cyber warfare, or even digital data, did not cross the minds of the commentators in 1987. In addition, Macak argued that the claim that data is an object is supported by teleological interpretation, as mandated by the VCLT).

124. Dinniss, *supra* note 114, at 54.

125. *Id.*

of armed conflict".[126] Since the *Tallinn Manual* required unanimity to adopt its rules, the question on whether data could constitute object was unsettled.[127] In addition, although the majority of Experts concluded that data is not an object, Rule 71 of the *Tallinn Manual* seems to be contradicting that assertion, by providing that ". . .data that form[s] an integral part of the operations or administration of medical units and transports. . . may not be made the *object* of attack".[128]

These views are more persuasive than the data-excluding ones, yet the shortcoming in the data-inclusive arguments presented here, is that they end up being over-inclusive. Macak himself realizes that while "an innocuous e-mail" belonging to a civilian is an object, and destruction of such letter "would indeed probably not be lawful under IHL", it is unlikely, according to Macak, "that states would, within the scope of an armed conflict, engage in a military operation the sole aim of which would be to destroy one civilian letter (or one such email)".[129]

Data should be viewed as an object as any other proposition would compromise data completely. The consideration whether the cyber operation targeting data is an "attack" should rely on the three factors: (1) an operation beginning in cyberspace or a computer system; (2) it is interruptive in nature – that is, the compromise or loss of data is interrupting the day-to-day lives of civilians; and (3) it is violent, that is, the data is critical, the damage is irreversible, the effects are prolonged and more.

D. *Existing Frameworks*

Certain frameworks have already made attempts to address cyber operations in the context of IHL, particularly in relation to "attack." Although there is no internationally binding framework, these frameworks are important in understanding the current view on these issues. The U.S. DoD Law of War Manual represents the view of the Department of Defense alone,[130]

126. INTERNATIONAL GROUP OF EXPERTS, *supra* note 59, at 127 (Commentary 5 to Rule 38).

127. *See* Schmitt, *supra* note 114, at 82-83.

128. INTERNATIONAL GROUP OF EXPERTS, *supra* note 59, at 206.

129. Macak, *supra* note 114, at 75-76.

130. *See generally* Office of Gen. Counsel U.S. Dep't of Defense, Department of Defense Law of War Manual 1005 (2015), available at available at http://www.defense.gov/Portals/1/Documents/pubs/Law-of- War-Manual- June-2015.pdf. ("This manual is an institutional publication and reflects the views of the Department of Defense, rather than the views of any particular person or DoD component. An effort has been made to reflect in this manual sound legal positions based on relevant authoritative sources of the law, including as developed by the DoD or the U.S. Government under such sources, and to show in the cited sources the past practice of DoD or the United States in applying the law of war.").

"This manual is an institutional publication and reflects the views of the Department of Defense, rather than the views of any particular person or DoD component. An effort has been made to reflect in this manual sound legal positions based on relevant authoritative sources of the law, including as developed by the DoD or the U.S. Government under such sources, and

though it might be used by other departments, as well as officially by the U.S.

The *Tallinn Manual* on the International Law Applicable to Cyber Warfare, is a NATO sponsored non-binding codification of the international law norms applicable to the wartime use of cyber-attacks.[131] The *Tallinn Manual* deals, *inter alia,* with the IHL applicability to cyber warfare. However, even though the *Tallinn Manual* represents *lex lata,* rather than *lex ferenda,* it is not legally binding.[132]

The Group of Governmental Experts (GGE) Report on Developments in the Field of Information and Telecommunications in the Context of International Security, is an effort to bring experts from twenty different countries, who "examined existing and potential threats arising from the use of ICTs [information and communication technologies] by States. . . including norms, rules, principles and confidence-building measures. . . the Group examined how international law applies to the use of ICTs by States. Building on the work of previous Groups, the present Group made important progress in those areas."[133]

1. U.S. DoD Law of War Manual

The *Law of War Manual* begins its cyber operations and *jus in bello* (IHL) part by stating the basic, and most obvious assumption: "[i]f a cyber operation constitutes an attack, then the law of war rules on conducting attacks must be applied to those cyber operations. For example, such operations must comport with the requirements of distinction and proportionality".[134] On the contrary, the *Manual* posits that "a cyber operation that does not constitute an attack is not restricted by the rules that apply to attacks. Factors that would suggest that a cyber operation is not an "attack" include whether the operation causes only reversible effects or only temporary effects. Cyber operations that generally would not constitute attacks include: defacing a government webpage; a minor, brief disruption of internet services; briefly disrupting, disabling, or interfering with communications; and disseminating propaganda."[135]

---

to show in the cited sources the past practice of DoD or the United States in applying the law of war."

131. International Group of Experts, *supra* note 59, at 1.

132. International Group of Experts, *supra* note 59, at 5.

133. G.A. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 2, U.N. Doc. A/70/150 (July 22, 2015) [hereinafter GGE Report].

134. Office of Gen. Counsel U.S. Dep't of Defense, *supra* note 131, at 1003-04 (Rule 16.5.1).

135. Office of Gen. Counsel U.S. Dep't of Defense, *supra* note 131, at 1005 (Rule 16.5.2).

a. The Manual's Shortcomings

There are two shortcomings in the *Manual*'s treatment of disruptive cyber operations (or non-attack cyber operations). First, the *Manual* uses the "reversible effects or only temporary effects" test,[136] which does not necessarily help determining whether a cyber operations reached the level of "attack." For example, a cyber operation that causes bodily injury or physical destruction could still be reversible or temporary in its effects, yet it would definitely be considered an "attack" due to its clear physical consequences. Second, the examples provided by the Manual are "inconvenience" sort of harms, which would not necessarily be considered as particularly disruptive (depending on the degree of inconvenience), and the language used by the Manual hints towards that notion – "defacing" and "minor, brief disruption" is a language that denotes lack of *violent* effects, as argued earlier in this paper, yet the Manual does not directly grapple with effects on *functionality*, *data, essential services*, all of which, if targeted, could result in *violent* effects, thus invoking the IHL regime applicable to "attacks". All in all, the Manual seems to leave somewhat of a gap between cyber operations causing minor inconveniences and ones that cause severe physical effects.

Furthermore, the Manual holds an opposing view to this paper's main argument, that disruptive cyber operations "may be directed at civilians or civilian objects." However, "such operations must not be directed against enemy civilians or civilian objects unless the operations are militarily necessary" and "even if a cyber operation is not an "attack" or does not cause any injury or damage that would need to be considered under the proportionality rule, that cyber operation still should not be conducted in a way that unnecessarily causes inconvenience to civilians or neutral persons."[137] It is impor-

136. OFFICE OF GEN. COUNSEL U.S. DEP'T OF DEFENSE, *supra* note 131, at 1005 (Rule 16.5.2 states that, "A cyber operation that does not constitute an attack is not restricted by the rules that apply to attacks. Factors that would suggest that a cyber operation is not an 'attack' include whether the operation causes only reversible effects or only temporary effects. Cyber operations that generally would not constitute attacks include: defacing a government webpage; a minor, brief disruption of internet services; briefly disrupting, disabling, or interfering with communications; and disseminating propaganda. Since such operations generally would not be considered attacks under the law of war, they generally would not need to be directed at military objectives, and may be directed at civilians or civilian objects. Nonetheless, such operations must not be directed against enemy civilians or civilian objects unless the operations are militarily necessary. Moreover, such operations should comport with the general principles of the law of war. For example, even if a cyber operation is not an 'attack' or does not cause any injury or damage that would need to be considered under the proportionality rule, that cyber operation still should not be conducted in a way that unnecessarily causes inconvenience to civilians or neutral persons.").

137. OFFICE OF GEN. COUNSEL U.S. DEP'T OF DEFENSE, *supra* note 131, at 1005 (Rule 16.5.2).

tant to note that the Manual does not consider disruption, economic harms, and inconvenience as part of the proportionality evaluation.[138]

In addition, the Manual offers somewhat of a hint towards a limited protection against activities that are not attacks, yet seize or destroy enemy property nonetheless, by providing that "[a] cyber operation that would not constitute an attack, but would nonetheless seize or destroy enemy property, would have to be imperatively demanded by the necessities of war."[139] That could mean that disruptive cyber operations, which are allegedly not "attacks" under the Law of War Manual approach, would still need to be justified under the military necessity rule, thus possibly limiting its effects on civilians and civilian infrastructure. However, the Manual's position on *disruptive* cyber operations is very limited, leaving much room for carrying out these operations against civilians without an accountability regime.

2. Tallinn Manual

The *Tallinn Manual* defines "cyber attack" as a "cyber operation, whether offensive or defensive, that is reasonable expected to cause injury or death to persons or damage or destruction to objects."[140] The *Manual* also reaffirms that to qualify as "attack" an action needs "violent effects" rather than release of kinetic force.[141] Although the *Manual* employs a physical-effects approach to the concept of "attack," it still provided that the IGE were divided with regard to operations that interfere with functionality of objects, with the majority holding the view that it would constitute an attack if "replacement of physical components" is required.[142] Within those experts, there was no consensus on whether reinstalling the operating system could suffice for the purposes of "attack,"[143] however, a few of the experts believed that if such operation "necessitates data restoration," it should be considered an attack.[144]

The *Tallinn Manual* adopts a pretty narrow, traditional perspective on "attack", but it is still submitted that majority of experts agreed that "there might be logic" in characterizing largely disruptive cyber operations as "at-

138. Office of Gen. Counsel U.S. Dep't of Defense, *supra* note 131, at 1004 (Rule 16.5.1.1).

139. Office of Gen. Counsel U.S. Dep't of Defense, *supra* note 131, at 1004 (Rule 16.5.1).

140. International Group of Experts, *supra* note 59, at 106.

141. International Group of Experts, *supra* note 59, at 106-07 (Commentary 3 to Rule 30).

142. International Group of Experts, *supra* note 59, at 108 (Commentary 10 to Rule 30).

143. International Group of Experts, *supra* note 59, at 108 (Commentary 10 to Rule 30).

144. International Group of Experts, *supra* note 59, at 109 (Commentary 11 to Rule 30).

tacks."[145] However, these experts also claimed that IHL "does not presently extend this far", and a minority of these experts predicted that the international community will most likely characterize such operations as "attacks," should they occur in the future.[146] The *Tallinn Manual*, therefore, protects civilians from direct attacks only if the cyber operation in question fits the definition provided by the Manual, which focuses on physical consequences.[147]

With regard to the applicability of the proportionality rule, the *Tallinn Manual* provides that "cyber operations may cause inconvenience, irritation, stress, or fear. Such consequences do not qualify as collateral damage . . ."[148] The *Manual* does not define the scope of these terms, nor does he directly deal with *violent* disruption effects as collateral damage.

3. GGE Report

Unlike the Law of War and *Tallinn Manuals*, the GGE Report has a broader scope than simply analyzing IHL in relation to cyber operation. The GGE Report generally focuses on threats to international peace and security posed by the development of information and communication technologies ("ICTs").[149] The GGE Report notes "the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction."[150] However, the GGE Report does not specifically analyze how these IHL principles apply to cyber operations, nor does it deal with "attacks" or disruptive cyber operations in that context. The main importance of the GGE Report is to incrementally come up with a set of rules applicable to activities in cyberspace, and possible, address these specific gaps and ambiguities in further detail in future reports.

V. Conclusion

Disruptive cyber operations during an armed conflict could become a major threat to civilians, civilian property, and civilian wellbeing in the future. The purpose of this paper is to introduce the notion of disruptive cyber operations as "attacks" under IHL, thus limiting their use in accordance with the principles of distinction, proportionality, and prohibition on indiscriminate attacks. Disruption itself, is a new form of violence, which ought to be

145. International Group of Experts, *supra* note 59, at 109 (Commentary 12 to Rule 30).
146. International Group of Experts, *supra* note 59, at 109 (Commentary 12 to Rule 30).
147. International Group of Experts, *supra* note 59, at 113 (Commentary 13 to Rule 32).
148. International Group of Experts, *supra* note 59, at 160 (Commentary 5 to Rule 51).
149. GGE Report, *supra* note 133, at 6, para. 1.
150. GGE Report, *supra* note 133, at 13, para. 28(d).

incorporated in the ordinary meaning of "violence" in the context of "attacks." Violence is incrementally changing, and the effects that can be brought about by cyber operations are increasing and posing a great challenge to contemporary legal frameworks, IHL being only one of them. These arguments are certainly not prohibiting the use of cyber operations entirely, whether destructive or disruptive, but limiting them using well-established norms relating to the protection of civilians and civilian objects during an armed conflict.

Current frameworks dealing with IHL and cyberspace are not addressing disruption as a possible harm due to cyber operations, and more work is required to mitigate future threats against civilians in that sense. Even the most conservative readers of "attack" admit that state practice could develop in a way that restricts the use of disruptive cyber operations in an armed conflict, realizing how harmful these operations are when conducted against civilians and civilian object.[151]

Disruptive cyber operations that reach the threshold of "attacks" by being *violent* have a practical and normative implication on current IHL. First, is that disruptive cyber operations should be designed *humanely,* in accordance with the *duty to code humanely*. Parties to a conflict are under obligation to ensure that these operations are capable of distinguishing between civilians and military targets, and that they are directed against military objectives alone. Secondly, to strengthen the standing of disruption as a legitimate harm, the proportionality analysis should take into account possible disruption harm to civilians as collateral damage. Similarly, the debate on data as an "object" is based on obsolete distinction between tangible and intangible, which are untenable in the digital age, where data is sometimes more valuable than physical objects, with which traditional international law is so inexplicably obsessed.

The common theme in this paper is the changing nature of conflict, weapons, and targets. International law, remaining somewhat stagnant, needs to catch up and adapt to this changing nature before it takes its toll. However, realizing that international lawmaking has its own limitations, it is unclear whether a treaty or custom will eventually address these emerging, threatening, phenomena.

151. *See* Schmitt, *supra* note 61.