CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis

Colonel David Wallace
Professor, Department of Law, United States Military Academy

Tallinn Paper no 11

Tallinn 2018

Previously in This Series

No. 1 Kenneth Geers “Pandemonium: Nation States, National Security, and the Internet” (2014)

No. 2 Liis Vihul “The Liability of Software Manufacturers for Defective Products” (2014)

No. 3 Hannes Krause “NATO on Its Way Towards a Comfort Zone in Cyber Defence” (2014)

No. 4 Liina Areng “Lilliputian States in Digital Affairs and Cyber Security” (2014)

No. 5 Michael N. Schmitt and Liis Vihul “The Nature of International Law Cyber Norms” (2014)

No. 6 Jeffrey Carr “Responsible Attribution: A Prerequisite for Accountability” (2014)

No. 7 Michael N. Schmitt “The Law of Cyber Targeting” (2015)

No. 8 James A. Lewis “The Role of Offensive Cyber Operations in NATO’s Collective Defence” (2015)

No. 9 Wolff Heintschel von Heinegg “International Law and International Information Security: A Response to Krutskikh and Streltsov” (2015)

No. 10 Katrin Nyman-Metcalf „A Legal View on Outer Space and Cyberspace: Similarities and Differences“ (2017)

About the author

Colonel David Wallace is the Professor and Head, Department of Law, United States Military Academy. In 2017, Colonel Wallace served as a Visiting Scholar at the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 21 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual 2.0, the most comprehensive guide on how International Law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise Locked Shields. Every spring the Centre hosts in Tallinn the International Conference on Cyber Conflict, CyCon, a unique event joining key experts and decision-makers of the global cyber defence community. As of January 2018 CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations - to this date Austria, Belgium, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Portugal, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Table of Contents

1. Introduction

In the decades that followed the creation of the Internet, cyberspace has become a domain of conflict as States enhance their cyber capabilities by creating advanced arsenals of cyber weaponry; adding specialized personnel and force structure, and engaging in and resourcing cutting edge research and development of offensive and defensive capabilities. It is estimated that approximately 140 countries have developed, or are developing, a capacity to wage cyber armed conflict.[1] In point of fact, in 2016 at the Warsaw Summit, NATO announced that cyberspace is now considered a domain of operations in which it must defend itself as effectively as it does in the air, on land, and at sea. This declaration is widely believed to be an acknowledgment that cyber threats are becoming more common, complex, and potentially damaging.[2] Central to this trend is the development and use of cyber weapons. To date, there are relatively few publicly acknowledged examples of cyber weapons. The most well-known and controversial cyber weapon is the so-called Stuxnet worm.

By way of background and context, in 2006, United States President George W. Bush wanted to derail or slow down the Iranian nuclear program. President Bush did not, however, want to launch airstrikes against the Iranian nuclear enrichment facility. He was looking for an option between doing nothing and a kinetic attack. Bush eventually settled on a cyber operation on the computer control systems at the Iranian nuclear enrichment facility at Natanz, Iran.[3] After creating and covertly inserting a cyber "beacon" into the Iranian computer network — which mapped the workings of the plant — a highly complex worm, sometimes referred to as "Stuxnet",[4] was inserted into the plant's computer controller systems. That control system ran thousands of centrifuges.[5] The Stuxnet worm took over some nuclear centrifuges and made them spin uncontrollably either too fast or too slow. This process made the centrifuges unbalanced and, in some cases, explode. Over time new variants of the Stuxnet worm were created

---

[1] Institute, Kevin Coleman Technolytics. "Coleman: The Cyber Arms Race Has Begun." CSO Online. January 28, 2008. Accessed December 17, 2017. http://www.csoonline.com/article/2122353/critical-infrastructure/coleman--the-cyber-arms-race-has-begun.html.

[2] "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit." CCDCOE. July 22, 2016. Accessed December 17, 2017. https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html. *See also*, Warsaw Summit Communiqué - Issued By the Heads Of State and Government Participating in the Meeting Of the North Atlantic Council in Warsaw, 8-9 July 2016
NATO - https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[3] Kaplan, Fred M. Dark territory: the secret history of cyber war. New York: Simon & Schuster Paperbacks, 2017. 203-4.

[4] A Belarus computer security firm was hired to troubleshoot a series of computers in Iran that were not operating properly. The security analysts with the firm found malicious files on one of the Iranian systems. See, Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired. June 03, 2017. Accessed December 18, 2017. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. Accessed December 17, 2017.

[5] Uranium Enrichment, United States Nuclear Regulatory Commission - Protecting People and the Environment, https://www.nrc.gov/materials/fuel-cycle-fac/ur-enrichment.html (last visited Oct 21, 2017). According to the United States Nuclear Regulatory Commission "[t]he gas centrifuge process uses a large number of rotating cylinders in series and parallel configurations. Gas is introduced and rotated at high speed, concentrating the component of higher molecular weight toward the outer wall of the cylinder and the lower molecular weight component toward the center. The enriched and the depleted gases are removed by scoops."

and surreptitiously inserted into the control system resulting in slightly different failures.[6] One of the important features of Stuxnet was that it was designed to leave no trace of the attackers.[7] But, an element of the digital worm inadvertently became public in the summer of 2010 because of a programming error that allowed it to escape the Natanz plant sending it around the world on the Internet.[8]

Commenting on Stuxnet, General Michael Hayden, the former director of the NSA and CIA and later a national security analyst for CNN, noted as follows:

[p]revious cyber-attacks had effects limited to other computers… This is the first attack of a major nature in which a cyber-attack was used to effect physical destruction. And no matter what you think of the effects—and I think destroying a cascade of Iranian centrifuges is an unalloyed good—you can't help but describe it as an attack on critical infrastructure…. Somebody has crossed the Rubicon. We've got a legion on the other side of the river now. Something had shifted in the nature and calculation of warfare, just as it had after the United States dropped atom bombs on Hiroshima and Nagaskai at the end of World War II.[9]

The above incident has been and continues to be analysed and dissected. One of the reasons for the great interest in Stuxnet is simply that the curtain has been pulled back slightly, giving the world a glimpse of cyber weaponry. That peek raised many interesting legal, policy, and practical issues including the thorny issue of cyber weapons reviews under International Humanitarian Law (IHL). To frame and discuss this issue, it is necessary to note and clarify that the provisions of IHL that concern weaponry fall into two general categories. The first concerns the legality of the weapons themselves. That is, are the weapons and weapons systems unlawful *per se*? The second category involves the conduct of hostilities provisions as applied to the use of weapons. Under IHL, most weapons are not illegal *per se*. Their use may be lawful under some circumstances and unlawful under others, such as if they are used to attack combatants who are *hors de combat*.[10] These rules are separate and distinct from the first category and are critically important, but are beyond the scope of this paper. Accordingly, this paper is limited to the first category.

Moving forward, there is unquestionably widespread interest in and enthusiasm for cyber weapons now and into the foreseeable future. The eagerness and zeal to develop such weapons is reflected not only

---

[6] "How a Secret Cyberwar Program Worked." The New York Times. May 31, 2012. Accessed December 18, 2017. http://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html.

[7] Szoldra, Paul. "A new film gives a frightening look at how the US used cyberwarfare to destroy nukes." Business Insider. July 07, 2016. Accessed December 18, 2017. http://www.businessinsider.com/zero-days-stuxnet-cyber-weapon-2016-7.

[8] Sanger, David E. "Obama Ordered Wave of Cyberattacks Against Iran." The New York Times. June 01, 2012. Accessed December 18, 2017. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[9] Kaplan, *supra* note 4 at 215.

[10] "Department of Defense Law of War Manual." Office of General Counsel, Department of Defense, United States. June 2015, updated December 2016, 337. Accessed December 18, 2017. https://www.defense.gov/Portals/1/Documents/law_war_manual15.pdf

in official rhetoric, but also is amplified in national cyber strategies and policies as well as in the global upswing of dedicated funding to such efforts.[11] This paper will investigate and critically analyze one narrow aspect of the overall issue of cyber weapons: *i.e.*, the cyber weapons review process in the context of the normative framework of IHL. It will do so in a three-part process. The first part involves a synopsis of the law of weaponry generally and the weapons review process specifically under IHL. To provide greater context, this part will briefly consider the historical development of the law of weaponry and the weapons review process. The second part examines the *Tallinn Manual 2.0's* treatment of cyber weapons reviews. The third and final part involves an analysis of the development and use of cyber weapons specifically under IHL. It will highlight three particularly thorny issues. Initially, it will consider the overarching question of what constitutes a cyber weapon. Next, it will address potential concerns about the indiscriminate nature of cyber weapons. Finally, the paper will address the inherent challenges posed by the timing of cyber weapons reviews. It will end with some concluding thoughts about the future.

[11] "Science, Technology, and the Future of Warfare." Modern War Institute. December 09, 2016. Accessed December 18, 2017. https://mwi.usma.edu/science-technology-future-warfare/ (last visited Dec 11, 2017).

2. Weapons review and the Law of Weaponry

From a historical perspective, prohibitions and limitations on particular weapons are woven deeply into the fabric of IHL. For example, in approximately 200 AD, the Hindu Code of Manu included a provision that prohibited poison arrows.[12] Under Innocent II, the use of the crossbow was forbidden in warfare as "deadly and odious to God" by the Catholic Second Lateran Council in 1139.[13] In 1863, the 157-article Lieber Code reinforced the prohibition on the use of poisons in the context of a provision that prohibited the infliction of suffering for the sake of suffering.[14] Shortly thereafter, in 1868, the St. Petersburg Declaration was adopted and is regarded as the first major treaty prohibiting the use of a particular weapon in armed conflict.[15] More specifically, the Declaration banned the use of an explosive projectile of unprecedented wounding power for its time.[16] Beyond the specific prohibition on the projectile, the St. Petersburg Declaration also presciently addressed the regulation of the development and use of future weapons. It provided, in part, as follows:

[t]he Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view of future improvements which science may effect in the armament of troops, in order to maintain the principles which they have established, and to conciliate the necessities of war with the laws of humanity.[17]

The twentieth century witnessed an exponential growth in IHL provisions banning or limiting weapons. In some cases, the restrictions were found in broader international agreements such as the Hague Regulations of 1907[18] and the Additional Protocol I to the 1949 Geneva Conventions.[19] In other

---

[12] Boothby, William H. Weapons and the law of armed conflict. Oxford: Oxford University Press, 2016, 8.

[13] Solis, Gary D. The law of armed conflict: international humanitarian law in war 5 (2017).

[14] "Instructions for the Government of Armies of the United ..." Accessed December 18, 2017, art. 16.https://www.loc.gov/rr/frd/Military_Law/Lieber_Collection/pdf/Instructions-gov-armies.pdf. As a codification of the customs and usages of war, the Lieber Code was written for and binding on Union forces in the American Civil War, and it was promulgated as General Order 100.

[15] Treaties, States Parties, and Commentaries – St. Petersburg Declaration relating to Explosive Projectiles, 1868. Accessed December 18, 2017. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=3C02BAF088A50F61C12563CD002D663B. The St. Petersburg Declaration had its origin in 1863 with Russia's invention of a bullet which exploded on contact with hard substances and whose primary object was to destroy ammunition wagons. In 1867, that projectile was modified in such a way as to explode on contact with soft substances. Accordingly, that type bullet was deemed as an inhumane instrument of warfare.

[16] Best, Geoffrey. Humanity in warfare: the modern history of the international law of armed conflicts. London: Metheuen, 1980, 159.

[17] St. Petersburg Declaration, *supra* note 16.

[18] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907. Articles 22 and 23 are foundational to the development of weapons law. Article 22 provides that "[t]he right of belligerents to adopt means of injuring the enemy is not unlimited." Article 23 articulates a number of specific prohibitions including that it is forbidden "[t]o employ arms, projectiles, or material calculated to cause unnecessary suffering."

[19] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

instances, the treaties banned or restricted particular weapons or an entire class of weaponry including, but not limited to, the 1925 Geneva Gas Protocol, as well as the Biological,[20] Chemical,[21] and Conventional Weapons Conventions[22] among others. Of particular note and relevance is the so-called Martens Clause.[23] This provision, which first appeared in the preamble to the 1899 Hague Convention (II), has been subject to multiple interpretations over the decades. In the context of the rapid evolution of military technology, the Martens Clause reinforces the notion that something which is not explicitly prohibited by a treaty, such as a new weapon, is not *ipso facto* permitted under IHL. The lawfulness of such new weapons still must be assessed under customary international law according to the principles of humanity and the requirements of the public conscience.[24]

Speaking more broadly, some of the specific prohibitions or limitations of weapons law under IHL are customary and binding on all States while others are based upon conventional law and thus are only binding on the States that are party to a particular treaty.[25] The portions of IHL that relate to the development and use of weapons are prohibitive in nature. Namely, principles and provisions forbid or limit certain weapons rather than serving as positive norms to authorize the weapons. Put differently, the lawfulness of the development and use of a type of weapon does not depend on the presence or absence of authorization under IHL. Rather, the question is whether or not the weapon is prohibited. In the context of emerging technologies such as cyber, the mere fact that a weapon is markedly different than other means of warfare does not translate into that weapon being illegal under IHL. International Humanitarian Law does not require States to establish a general practice of using a weapon before it is to be regarded as legal. The corollary is equally true. That is, a new weapon should not be presumed to be automatically prohibited because there is an absence of State practice supporting its use.[26]

The most important IHL provision concerning weapons review is Article 36 of Additional Protocol I. A State's weapons review obligations depend, in part, upon whether they are currently one of the 174 State parties to Additional Protocol I. In fact, the *Tallinn Manual 2.0* rule on weapons review is bifurcated between a general statement that is applicable to all States and a more specific rule that is derived from

---

[20] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, 10 April 1972.

[21] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, 13 January 1993.

[22] Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects. Geneva, 10 October 1980.

[23] The Marten's Clause was based upon and took its name from a declaration read by Professor von Martens, the Russian delegate at the Hague Peace Conferences 1899. The clause states:

> Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience.

[24] Ticehurst, Rupert. "The Martens Clause and the Laws of Armed Conflict." *International Review of the Red Cross*, 1997, volume 37, issue 317, pp. 125-134. https://www.icrc.org/eng/resources/documents/article/other/57jnhy.htm.

[25] Boothby, *supra* note 13 at 340-41.

[26] DoD Law of War Manual, *supra* note 11 at 338.

Article 36. The International Group of Experts could not reach consensus on the question of whether Article 36 reflects customary international law.[27] Article 36 provides as follows:

In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[28]

The Commentary to Article 36 highlights, among other things, the purpose of the provision is to require States to analyze and consider whether the employment of a weapon for its normal or expected use would be prohibited under some or all circumstances under IHL. To put a finer point on the thinking behind Article 36, States are certainly not required to foresee all possible misuses of a weapon because almost any weapon can be misused in ways that would be prohibited.[29] Additionally, the review of weapons for consistency with IHL obligations should consider at least two fundamental questions.[30]

The first, using the language of Article 36, is whether the "weapon, means and methods" of warfare is of a nature to cause superfluous injury or unnecessary suffering.[31] There are a number of weapons that have historically been characterized as being of a nature to cause superfluous injury or unnecessary suffering including, but not limited to: serrated-edged bayonets; expanding and explosive bullets; poison and poisoned weapons; biological and chemical weapons; and projectiles filled with broken glass.[32] As noted in the Commentary to *Tallinn Manual 2.0*, only in the rare case will cyber weapons violate the prohibition on causing superfluous injury or unnecessary suffering.[33] The second question is far more

---

[27] Michael N. Schmitt & Liis Vihul, Tallinn manual 2.0 on the international law applicable to cyber operations 465 (2017).

[28] Additional Protocol I, Art. 36, *supra* note 20.

[29] Ibid.

[30] DoD Law of War Manual, *supra* note 11 at 338. The prohibition on unnecessary suffering and on indiscriminate weapons are the most important issues in the weapons review process, but there are others. For example, a weapon should be reviewed to ensure it is not intended or may be expected to cause widespread, long-term, and severe damage to the natural environment. Also, it is necessary to ensure that a weapon does violate any specific treaty or customary law norm that would prohibit it.

[31] Doswald-Beck, Louise, and Jean-Marie Henckaerts. Customary international humanitarian law. Cambridge: Cambridge University Press, 2005, 237. The basis for this principle, which reflects customary international law, is Article 23(e) of the Hague Regulations and Article 35(2) of Additional Protocol I.

[32] Ibid. at 244-45.

[33] *Tallinn Manual 2.0*, *supra* note 28 at 454-55. The experts offered a thought-provoking example of when a cyber weapon and operation could violate the prohibition on causing superfluous or unnecessary suffering. It is as follows:

> [f]or example, consider an enemy combatant who has an Internet-addressable pacemaker device with a built-in defibrillator. It would be lawful to take control of the pacemaker to kill that individual or render him *hors de combat*, for example by using the defibrillation function to stop the heart. However, it would be unlawful to conduct the operation in a manner that is intended to cause additional pain and suffering for their own sake, that is, unrelated or patently excessive to the lawful purpose of the operation. Examples of such unlawful actions would include stopping the target's heart and then reviving him multiple times before killing him.

applicable to cyber warfare. That is, whether the weapon is inherently indiscriminate. Under the principles and provisions of IHL, indiscriminate weapons are those that cannot be directed at a military objective or whose effects cannot be limited.[34] Indiscriminate cyber weapons will be analyzed in depth below. Before moving onto the critical analysis of cyber weapons review, it is important to briefly synopsize how the *Tallinn Manual 2.0* Experts treat the cyber weapons review process.

[34] Doswald-Beck & Henckaerts, *supra* note 32 at 244. This principle, which reflects customary international law, is based upon Additional Protocol I, Article 51(4)(b) and (c).

3. *Tallinn Manual 2.*0 and Cyber Weapons Review Deterrence failures in recent history

For national legal advisors, policymakers, military leaders, and those having an interest in international law as it relates to cyber weaponry, an important point of departure for analysing how IHL applies to cyber operations and weapons is the *Tallinn Manual 2.0*. The 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* addresses the question of weapons review as well as many other vital issues spanning public international law in its nearly 600 pages of highly informative rules and commentary. To appreciate the importance of the *Tallinn Manual 2.0*, it is necessary to briefly provide some background and historical context. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), a renowned cyber research and training institution in Tallinn, Estonia, [35] invited an extraordinary group of independent experts to produce a manual on the international law governing cyber warfare.[36] This project brought together a distinguished group of international law scholars and practitioners—the International Group of Experts—to explore and articulate how extant legal norms apply to cyber warfare.[37] In 2013, the *Tallinn Manual on International Law Applicable to Cyber Warfare* was published and released. As a result of the success of the first Tallinn Manual, the NATO CCD COE initiated a follow-up project to expand the scope of coverage with an updated manual to include the international law governing cyber activities during peacetime.

The NATO CCD COE convened a second, more internationally diverse group of experts for the follow-up effort. Their dedicated work led to the creation and publication of *Tallinn Manual 2.0* in February 2017. The significantly expanded manual not only incorporates and updates the materials from the first Tallinn manual, but also includes coverage of legal regimens implicated by peacetime cyber activities and incidents.[38] Impressively, *Tallinn Manual 2.0* has 154 rules, including a specific rule on the weapons review process under IHL, Rule 110. The detailed commentary accompanying each rule not only offers some tremendously important insights into the deliberations and thought processes of the experts regarding the legal basis and justification for the rules and their normative context, but also offers practical implications of the rules' application in a cyber context. This level of detail is particularly helpful for national legal advisors and academics. Additionally, the commentaries to the rules articulate positions by the experts in their discussions such that it makes clear when either the experts all reached agreement or when they could not reach consensus on a particular issue. Finally, and most importantly, it should be noted that the experts were limiting themselves to a restatement of the *lex lata*. They avoided including statements reflecting the *lex ferenda*.[39]

Tallinn Manual 2.0, Rule 110: Weapons review provides as follows:

---

[35] "About Cyber Defence Centre." CCDCOE. February 02, 2017. Accessed December 18, 2017. https://ccdcoe.org/about-us.html. The mission of the NATO Cooperative Cyber Defence Centre of Excellence is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence through education, research and development, lessons learned and consultation.

[36] Tallinn Manual 2.0, *supra* note 28 at 1.

[37] Ibid.

[38] Ibid.

[39] Ibid. at 3.

(a) All States are required to ensure that the cyber means of warfare that they acquire or use comply with the rules of the law of armed conflict that bind them.

(b) States that are Parties to Additional Protocol I are required in the study, development, acquisition, or adoption of a new means or method of cyber warfare to determine whether its employment would, in some or all circumstances, be prohibited by that Protocol or by any other rule of international law applicable to them.[40]

There are at least six overarching points to consider with respect to Rule 110. First, Rule 110 must be read through the lens of the *Nuclear Weapons* advisory opinion of the International Court of Justice (ICJ). In that case, the ICJ debunked the notion that IHL does not apply to new weapons. Even though cyber weapons were invented after the majority of the principles and rules of IHL had already come into existence, it is wrong to conclude that IHL does not apply. Additionally, as noted by the ICJ, it would be incompatible with the intrinsically humanitarian character of the legal principles which permeates the entirety of IHL to maintain that IHL does not apply to new weapons. International humanitarian law applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present, and those of the future.[41] Second, and reinforcing that point, classifying something as a cyber weapon also means that it must comply with IHL.

Thirdly, subparagraph (a) reflects customary international law and flows from a general duty to comply with IHL.[42] Subparagraph (b) is derived from Article 36.[43] By any measure, the obligations outlined in subparagraph (b), which are not limited to IHL, but extend to the entirety of international law, are significantly broader and more comprehensive than the ones in subparagraph (a).[44] Fourth, like Article 36, subparagraph (b) neither specifies nor requires a particular methodology for conducting a cyber weapons review. Likewise, States are not obligated to make their weapons reviews public. In the context of cyber weapons, this is particularly germane because of the highly classified nature of such weapons. As in all weapons reviews pursuant to IHL, the determination of the legality of a cyber weapon must be made in reference to its normal, expected use at the time of the evaluation.[45]

Fifth, if a State receives a cyber weapon from another State to use in its operations, the fact that a supplying State has already conducted a review does not relieve the acquiring State of its obligations with respect to that cyber weapon. The acquiring State may consider the review done by the supplying

---

[40] Ibid. at 464.

[41] *Nuclear Weapons advisory opinion*, para. 86 available at http://www.icj-cij.org/en/case/95.

[42] Tallinn Manual 2.0, *supra* note 28 at 465.

[43] Ibid. at 465. The Experts were split on whether Article 36 reflects customary international law.

[44] Ibid. at 465-66. For example, a weapons review would also include consideration of any applicable arms control agreements.

[45] Ibid. at 466-67.

State, but the acquiring State must satisfy itself as to its obligations under IHL.[46] Sixth, in terms of what to review, for the State Parties to Additional Protocol I, the answer is a "new weapon, means or method of warfare".[47] What specifically constitutes cyber weapons, means, or method will be addressed below. Arguably, *all* States, regardless of whether they ratified Additional Protocol I or not, are required to systemically assess the legality of new weapons, means, and methods. This obligation flows logically from a general duty of compliance with IHL and the fact that States are prohibited from using illegal weapons, means, or methods of warfare.

[46] Ibid. at 466.

[47] Additional Protocol I, Art. 36, *supra* note 20.

4. Reviewing Cyber Weapons under IHL: A Critical Analysis Deterrence failures in recent history

A. What is a Cyber Weapon under IHL?

An obvious first step is to define what is a cyber weapon. From an IHL perspective, if a cyber capability amounts to "weapons, means, or methods of warfare", it triggers not only a weapons review under Article 36[48], but also under all of the related IHL prohibitions and limitations. Currently, there is no international consensus on a definition of a cyber weapon. Below are three possible formulations of a definition. First, the Commentary to Rule 103 of the *Tallinn Manual 2.0* defines cyber weapons as "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack."[49] And, more specifically, a cyber means would include any cyber device, material, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber-attack.[50] Next, articulating the definition in a slightly different manner, respected authors Thomas Rid and Peter McBurney conceptualize a cyber weapon as computer code that is "used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things."[51] Finally, in its regulation on the *Legal Reviews of Weapons and Cyber Capabilities*, the United States Air Force defines weapons as "devices designed to kill, injure, disable or temporarily incapacitate people, or destroy, damage or temporarily incapacitate property or material." To its credit, the proponents of the U.S. Air Force regulation recognized and highlighted that most cyber capabilities are not devices. Rather, they are software packages or techniques. [52] Accordingly, the Air Force regulation defined that concept of a cyber capability and stated "an Air Force cyber capability requiring a legal review prior to any employment is any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities."[53] Of note, the U.S. Air Force was the first of the U.S. military services to issue

[48] And, for the States that are not parties to Additional Protocol I, they still must ensure that the cyber means of warfare that they acquire or use comply with the rules of IHL.

[49] Tallinn Manual 2.0, *supra* note 28 at 452.

[50] Ibid. at 453. In the context of cyber, there is a difference between the computer system, which qualifies as a means of warfare, and the cyber infrastructure that serves as the conduit between the cyber weapon and its target.

[51] Thomas Rid & Peter McBurney (2012) Cyber-Weapons, The RUSI Journal, 157:1, 6-13, 7 DOI: 10.1080/03071847.2012.664354, available at https://doi.org/10.1080/03071847.2012.664354.

[52] U.S. Air Force Instruction 51-402, Legal Reviews of Weapons and Cyber Capabilities, 27 July 2011, available at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-053.pdf.

[53] Ibid.

a regulation specifically addressing the issue of how to review cyber capabilities.[54] The common thread running through all of the definitions is that cyber weapons are instruments of harm.[55]

In light of the above definitions and commentary, there are several observations that can reasonably be made or inferred about cyber weapons. First, much like their physical or kinetic counterparts, cyber weapons span a wide spectrum from specific, highly sophisticated weapons to more generic, less sophisticated ones. For example, one may acquire, develop and use customized, stealthy malware that will exploit a zero day[56] or unknown software vulnerabilities causing a tremendous amount of damage to an adversary's computer networks. As a slight variant, weapons can also use known but common unpatched vulnerabilities, like WannaCry or NotPetya.[57] This type of cutting-edge cyber weapon is able to penetrate networks and systems, even isolated and protected ones, and autonomously inflict harm.[58] Not surprisingly, the development and use of these types of cyber weapons usually takes a considerable amount of time, expertise, and resources.[59] By analogy, these types of cyber weapons could be compared to a sophisticated, fire-and-forget missile such as an anti-radiation weapon. Much like a highly complex malware weapon, fire-and-forget weapons' technology is expensive, requires significant investments for research and development, and also depends upon intelligence about the intended target programmed into the system itself.[60]

By comparison, a somewhat generic, less sophisticated cyber weapon may be the software used to conduct a DDoS operation. DDoS attacks are likely to be clunky and easy to detect but may garner media and public attention such as the use of a botnet to cause a denial of service to a single or multiple targets.[61] Put in a slightly different manner, this type of cyber weaponry may be capable of influencing computer networks and systems from the outside, but is unable to cause direct harm by penetrating the networks and systems.[62] Although outside the confines of an armed conflict, the 2007 DDoS attacks against Estonia by Nashi, a small group of Russian activists associated with a pro-Kremlin youth group, would be an example of the use of such a generic, less sophisticated cyber weapon.[63] In the case of Estonia in 2007, the cyber weapon used was relatively crude and low-tech, but did have the effect of overwhelming and shutting down some Estonian websites for government ministries, political parties, newspapers, banks, and companies.[64] These DDoS attacks were disproportionately impactful on

---

[54] Brown, Gary D., and Andrew O. Metcalf. *Journal of National Security Law & Policy*, 2014, volume 7, no. 1, pp. 115-138. Of note, the U.S. DoD Law of War Manual, which was published several years after the U.S. Air Force regulation, also addressed the legal review of weapons that employ cyber capabilities. *See* DoD Law of War Manual, supra note 11 at 999.

[55] Thomas Rid and Peter McBurney, Cyber-Weapons, *RUSI Journal* 157, no 1, 2012, 6, available at https://doi.org/10.1080/03071847.2012.664354 (last visited Dec. 13, 2017).

[56] Zero-day vulnerabilities are software coding or design errors that can be accessed and exploited by a hacker which are unknown to the target of attack.

[57]

[58] Rid & McBurney, *supra* note 62 at 11.

[59] Carr, Jeffrey. Inside cyber warfare. Beijing: O'Reilly, 2012, 152.

[60] Rid & McBurney, *supra* note 56 at 6. As generally understood, "fire and forget" means that the missile or munition is able to guide itself to its target once fired.

[61] Ibid.

[62] Ibid. at 7.

[63] Tallinn Manual 2.0, *supra* note 12 at 564-5.

[64] Dinniss, Heather Harrison. Cyber warfare and the laws of war. Cambridge: Cambridge Univ. Press, 2014, 38-39.

Estonia because it is a State that is highly technologically dependent on the Internet for everything from grocery shopping, parking, banking, and voting, among other things.

Second, and a related point, is that cyber weapons produce different effects. The primary effects are on the targeted computers and networks. These effects include, but are not limited to, the deletion, corruption, or alteration of data or the disruption of an adversary's computer network.[65] Conversely, the secondary effects may involve the destruction or incapacitation of cyber infrastructure.[66] Lastly, tertiary impacts are those on persons affected by the secondary effects. For example, these effects would include people affected by the loss of electrical power or water by a cyber operation that targeted a power plant or water filtration facility respectively.[67] As noted by author Marco Roscini, "[p]hysical damage to property, loss of life and injury to persons, then, are never the primary effects of a cyber operation: damage to physical property can only be a secondary effect, while death or injury of persons can be a tertiary effect of a cyber operation."[68] In sum, both cyber and physical weapons can result in death, injury, damage and destruction. Generally speaking, the difference lies in the fact that with physical weapons, death, injury, damage and destruction are, in many cases, the primary effects.

A third observation is the other side of the proverbial coin, *i.e.*, what is *not* a cyber weapon. For example, a highly sophisticated piece of software developed and used for the sole purpose of espionage is *not* a cyber weapon.[69] To appreciate the fineness of the distinction between cyber weapons and non-weapons, a State could, for example, develop and use an extremely complex piece of malware that is intended to commit cyber espionage against another State, including the exfiltration of the targeted State's data. Such malware would not be considered a cyber weapon.[70] But, to complicate the analysis slightly, suppose the intelligence gathering malware mentioned above is an indispensable precursor to the development and use of a cyber weapon to the point that the two are inextricably linked; does that subject the intelligence gathering malware to a weapons review as a "weapons, means or methods of warfare" pursuant to Article 36? Or, is the better approach to treat the obligation to perform the weapons review separate and distinct from an overall obligation to ensure a particular cyber operation is done in compliance with IHL? In the same vein, there are some highly regarded cyber experts who view a "cyber weapon" as a vulnerability or zero-day defect found in an adversary's network or system. For them, the malware that exploits that defect is secondary and far less important than actually finding the defect in the first place. In reinforcement of this view, zero-day vulnerabilities can be bought and sold and have a life-expectancy. And it is believed that State intelligence and military organizations stockpile such vulnerabilities and have "large arsenals" of such zero-day vulnerabilities at their disposal. Even though such a perspective is inconsistent with the definition of a cyber weapon in *Tallinn Manual 2.0*, the definition offered by authors Rid and McBurney, and the U.S. Air Force regulation, it does raise fascinating questions about what precisely is a cyber weapon.

A fourth observation concerns the dichotomy between offensive and defensive cyber weapons. Generally speaking, defense includes, but is not limited to, such actions as patching systems, tracking

---

[65] Roscini, Marco. Cyber operations and the use of force in international law. New York: Oxford University Press, 2016. 52.

[66] Ibid.

[67] Ibid. at 52-3.

[68] Ibid. at 53.

[69] Rid & McBurney, *supra* note 56 at 7.

[70] Ibid. at 11.

down unusual behaviour on the network, and finding, analyzing, and responding to unusual code found in one's computer networks. By contrast, offense looks to overcome all of those measures and violate the confidentiality, integrity, or availability of data of an adversary's system.[71] Some States are particularly sensitive to the offensive use of cyber weapons, in part, because they do not want to be seen as using the same means and methods as some authoritarian regimes. They would rather focus on simply defending their networks.[72] Such concerns are rooted more in strategy and policy than in law. That point aside, the line between offensive and defensive in cyberspace, much like on a conventional battlefield, is fuzzy to say the least.[73] For example, is a "weaponized honeypot" an offensive or defensive weapon? The term "honeypot" has come to mean:

[a] deception technique in which a person seeking to defend computer systems against malicious cyber operations uses a physical or virtual environment designed to lure the attention of intruders with the aim of: deceiving the intruders about the nature of the environment, having the intruders waste resources on the decoy environment, gathering counter-intelligence about the intruders' intent, identity, and means and methods of cyber operations. Typically, the honeypot is co-resident with the actual systems the intruder wishes to target.[74]

Honeypots can be multiple resources such as servers, laptops, web-facing applications, or other technological ploys established to monitor and record the actions of cyber intruders.[75] Honeypots are deployed in various ways to make them attractive for hackers. In some cases, they appear to be the "crown jewels" of an organization, such as operational plans or financial reports. To be effective, the honeypot must appear realistic. If it looks or feels fake in any way, intruders' suspicions will be raised and the honeypot will not work.[76] Honeypots can be weaponized. That is, the honeypot would contain data or files that, once exfiltrated, will cause significant damage or disruption to the intruder's system.[77] Are such weaponized honeypots offensive or defensive? Are conventional weapons such as tanks, airplanes, rifles, or artillery offensive or defensive?

Perhaps a better way to think about cyber weapons is to equate them with their physical or conventional counterparts. Tanks, airplanes, rifles, and artillery are neither offensive nor defensive. They are simply means or tools of warfare that States may use, subject to the laws of armed conflict, to fight an armed conflict. It would be preposterous and, quite frankly, unworkable to categorize some means of warfare as offensive and others as defensive. Commanders need to have the operational flexibility—both offensively and defensively—to use the tools in in their tool kits to successfully fight and win on the modern battlefield. Beyond the threshold question of determining what constitutes a cyber weapon under IHL, the next inquiry involves their indiscriminate nature.

---

[71] Klimburg, Alexander. *The darkening web: the war for cyberspace*. New York: Penguin Press, 2017. 71.

[72] "NATO Mulls 'Offensive Defense' With Cyber Warfare Rules." U.S. News & World Report. Accessed January 19, 2018. https://www.usnews.com/news/world/articles/2017-11-30/nato-mulls-offensive-defense-with-cyber-warfare-rules.

[73] Klimburg, *supra* note 72 at 80.

[74] Schmitt & Vihul, *supra* note 28 at 565.

[75] Tari Schreider, Honeypots & Cyber Deception, 3 CISO Series on Today's Critical Issues (2017) available at https://ciso.eccouncil.org/wp-content/uploads/2017/06/Honeypots-Cyber-Deception.pdf.

[76] Edward Amorosa, Cyber Security 153 (2007).

[77] Schmitt & Vihul, *supra* note 28 at 174.

B. Are Cyber Weapons Impermissibly Indiscriminate?

As mentioned previously, one of the most important inquiries in a weapons review under IHL is to determine whether a weapon is inherently indiscriminate. In a cyber context, Rule 105 – Indiscriminate means or methods of the *Tallinn Manual 2.0* provides as follows:

It is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature. Means or methods of cyber warfare are indiscriminate by nature when they cannot be:

(a) directed at a specific military objective, or

(b) limited in the effects as required by the law of armed conflict

and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction.[78]

With respect to the requirement in subparagraph(a), an example of physical weapons that could not be directed were the imprecise Scud missiles from by Iraq in 1991 against Israel and coalition targets in Saudi Arabia.[79] The interests protected by this prohibition are somewhat obvious and reflect a central organizing principle of IHL, *i.e.*, the balance between humanitarian aims and military necessity. In terms of humanitarian considerations, IHL is fundamentally intended to protect civilians from attack. In terms of military necessity, the interest lies in ensuring that weapons are able to have their destructive effects as accurately and reliably as possible directed at the military capability of the enemy.[80]

Although the development and use of cyber weapons are among the most guarded secrets States possess, it can be reasonably assumed that cyber weapons, particularly those developed by technologically advanced States, show great promise in meeting the requirements of subparagraph (a). That is, cyber weapons can be carefully and methodically designed and narrowly tailored to garner a particular effect based upon extensive intelligence about a target and its vulnerabilities. It can also be reasonably assumed that as cyber technology moves ahead into the future, the capability of meeting this requirement will continue to improve. The publicly available information about Stuxnet supports this conclusion, particularly in terms of sophisticated cyber weapons. Amplifying the comments above on Stuxnet, it is widely believed that it was introduced in such a manner that defeated an "air gapped"[81] security measure and targeted a very specific type of Supervisory Control and Data Acquisition system software manufactured by a German company, Siemens. Beyond being incredibly precise in its target

---

[78] Ibid. at 455.

[79] Dinstein, Yoram. The Conduct of Hostilities under the Law of International Armed Conflict. Cambridge, UK: Cambridge University Press, 2004, 118.

[80] Ibid. at 68.

[81] Rosenzweig, Paul. Cyber warfare: how conflicts in cyberspace are challenging America and changing the world. Santa Barbara, CA: Praeger, 2013, 7. Air gapping a computer system simply means maintaining a gap with nothing but air between the system and the Internet. Air gapping can be overcome by someone introducing the malware into the protected system with, for example, a thumb drive used by a human agent intentionally or inadvertently.

acquisition, Stuxnet, working autonomously, manipulated the speed of rotors in nuclear enrichment centrifuges causing them not to work properly while disabling and bypassing digitally operated safety systems intended on ensuring that the centrifuges ran at a fixed and safe speed. Reasonable minds may differ, but looking at the evidence of Stuxnet's capabilities should make even the most sceptical critics comfortable that cyber weapons can be directed at a specific military objective.

By contrast, subparagraph (b) involves effects that cannot be limited. By analogy, biological weapons would reasonably be considered a class of weapons whose effects cannot be limited. The *Tallinn Manual 2.0* provides an illustrative example of a cyber weapon violating this provision. For example, a State employs malware against another State in the context of an armed conflict. The malware is, in fact, directed at a military objective, *i.e.,* the military computer networks of its enemy. However, once the malware is deployed, it will inevitably and harmfully spread into civilian computer networks.[82] This scenario illustrates a violation of subparagraph (b) because the effects of malware cannot be limited and are now indiscriminate. There are, however, a couple of important qualifications with respect to this provision. First, as noted by the *Tallinn Manual 2.0* Experts, the uncontrolled effects must be harmful in a way amounting to the incidental loss of civilian life, injury to civilians, or damage to civilian objects.[83] The threshold is that it would amount to collateral damage -- mere inconvenience or irritation is not sufficient harm.[84] Again, using the Stuxnet example, even though the worm spread to an estimated 10 million machines worldwide, it did no harm because it was only intended to damage a very specific type of cyber infrastructure. Accordingly, it did not violate this provision. Second, in order to violate subparagraph (b), the indiscriminate effects that cannot be limited must be foreseeable. If there is a malfunction or other type of unexpected occurrence that leads to the spread of the cyber weapon, it would not violate this provision.[85] Finally, as highlighted in the analysis of subparagraph (a), as cyber technology continues to improve, so does the capability of ensuring that the cyber weapons effects do not spread uncontrollably.

As a caveat to the above comments, it is important that cyber weapons reviewers not be too cavalier about the indiscriminate nature of cyber weapons for a variety of reasons. First, even if a cyber weapon can only harm a very specific target, once it spreads, other actors, to include cyber criminals, may use the weapon or parts of it for their own malevolent purposes. Using the above example, it was not long after discovery of Stuxnet before some six attack methods were being used for cybercrime.[86] Second, "mere inconvenience or irritation" may involve a substantial resource commitment to investigate and implement security measures by innocent civilians with respect to responding to cyber weapons found on their computers and networks. In sum, cyber weapons have the potential to be extremely precise, but legal reviewers must be cognizant that even the most highly sophisticated cyber weapons will spread, so it is vitally important to consider the second- and third-order effects of that consequence.

---

[82] Schmitt & Vihul, *supra* note 28 at 456.

[83] Ibid. at 472.

[84] Ibid. at 457.

[85] Of course, the complex interactions between malware and various other programs can make it extremely difficult to determine the foreseeability of indiscriminate effects.

[86] Neil C. Rowe, Challenges of Civilian Distinction in Cyberwarfare, contained in Taddeo, Mariarosaria. Ethics and policies for cyber operations. Place of publication not identified: Springer International, 2016. 39.

C. Timing of Cyber Weapons Reviews

Finally, the timing of cyber weapons reviews may be problematic. Given the State-centric nature of IHL obligations, it is not at all surprising that the temporal application of Article 36 is quite broad.[87] Ultimately, it is within the discretion of each State to determine the most appropriate time for the review of a weapon to ensure compliance with IHL.[88] If a State's assessment of a new weapon being developed leads to a conclusion that its future use would breach IHL, a decision to terminate the development of the weapon should be undertaken. From the ICRC's perspective, there should be an assessment of the legality of new weapons at the "study, development, acquisition or adoption".[89] These benchmarks would cover the traditional stages of the weapons procurement process, *i.e*., "the initial stages of the research phase *(i.e.,* conception, study), the development phase (*i.e.*, development and testing of prototypes), and the acquisition phase (including "off-the-shelf" procurement)."[90]

Again, stipulating that the development of most cyber weapons is cloaked in extreme secrecy, it is assumed that the cyber weapons development process is fundamentally more dynamic and iterative relative to other weapons subject to review. The reason for this conclusion is that a cyber weapon, particularly a highly sophisticated one, is being tailored to do extraordinarily complex actions in relation to a particular target. The reasonably anticipated effects of employment of the cyber weapon may change even though its intended use or the concept of an operation may stay constant. The significance of this condition is that an updated legal assessment should be conducted when changes have been made to the cyber weapon that substantially alter the cyber weapon's operational performance or its intended effects. As such, legal advisors tasked with providing such advice should be sensitive to this dynamic and respond accordingly. As with other issues in IHL, legal advisors are critically important to the process and add enormous value.

---

[87] "A Guide to the Legal Review of New Weapons, Means and Methods of Warfare Measures to Implement Article 36 of Additional Protocol I of 1977." International Committee of the Red Cross. Accessed December 17, 2017. https://www.icrc.org/eng/assets/files/other/irrc_864_icrc_geneva.pdf, 23-24.

[88] Boothby, *supra* note 13 at 345.

[89] ICRC, A Guide to the Legal Review of New Weapons, *supra* note 86 at 23.

[90] Ibid.

5. Conclusion

Unquestionably, there is a wide range of significant and complex legal, policy, and practical issues associated with cyber weapons reviews under IHL. The above paper is but a sampling of those issues and should be seen as a clarion call for greater research and study in this critically important area. The embryonic nature of this research is illustrated by the fact that there is no consensus even on a precise definition of a cyber weapon, let alone all of the implications that flow from applying traditional IHL weapons review principles and concepts to this emerging technology. This ambiguity, however, does not mean in any way that IHL does not apply in full measure. It does. The Tallinn Manual Experts made important contributions to sketching out a reasonable view on the *lex lata* with insightful commentary with respect to the review of cyber weapons. It is now up to States to build on this effort as international law reflects consensus among States as to the norms that govern their interactions.[91]

Although it is admittedly speculative on how the content, interpretation, and application of the IHL related to the legal review of cyber weapons may mature and develop in the coming decades, this author believes that the normative evolution of this aspect of IHL will be quite challenging. The main reason for this conclusion is the security environment surrounding cyber weapons. Namely, it is impossible to overstate the uniqueness of the environment in which cyber weapons are conceived, developed, and ultimately used. Cyber arsenals are shrouded in mystery, secrecy and denial. States do not publicly acknowledge their development, capabilities or use. Moreover, in cyberspace, one can hide behind aliases, use proxy servers, and surreptitiously enslave other computers making attribution extremely difficult. Additionally, some States believe that maintaining legal ambiguity in cyberspace fosters operational and strategic flexibility. And, in relative terms, cyber weapons can be developed with modest technological infrastructure. These considerations, as well as others, make it is highly unlikely that States will agree to any specific regulations as to cyber weapons. It is more likely States may agree on specific legal norms related to heightened protections from cyber-attacks on certain critical infrastructure rather than any on regulations on cyber weapons. Of course, the security environment is not the only obstacle. There are others. For example, there is no authoritative definition of what even constitutes a cyber weapon and the State-centric nature of the weapons review process make any international regulation highly problematical. Given all of the above, this author believes that the normative architecture of the IHL weapons review process will be at the trailing edge of any change.

[91] Schmitt, Michael N., The Law of Cyber Warfare: Quo Vadis? (September 4, 2013). 25 Stanford Law & Policy Review 273 (2014).