# UPDATING THE LAW OF TARGETING FOR AN ERA OF CYBERWARFARE

BENJAMIN WEITZ*

## ABSTRACT

Cyberwarfare is quickly becoming the new norm in military action. From Russia, to the United States, to China, states—as well as non-state actors—are invested in cyber weapons and cyber capabilities. The legal world is struggling to keep up with this rapidly developing field and is currently engaged in the extended discussion of whether current international humanitarian law is sufficient to regulate the new field of cyberwarfare or whether an entirely new system must be created. This Comment argues that current frameworks of international humanitarian law have the potential to regulate cyberwarfare, but they must be updated and revised in order to effectively do so.

One major gap in international law regarding its application to the world of cyber is in the law of targeting. Specifically, the current regulation of the targeting of dual-use objectives, and the current precautions that commanders must take before and during attacks, are insufficient and must be updated in order to apply to the cyber realm. This Comment lays out a more explicit and revamped proportionality standard which should successfully mandate that commanders take into account various knock-on effects (secondary effects) when targeting a dual-use objective.

[*] J.D., 2018, University of Pennsylvania Law School; B.A., 2011, Middlebury College. I would like to thank Professor Christopher Yoo for his helpful feedback and advice. I am grateful to Benjamin Barsky, Shane Fischman, and the staff of the University of Pennsylvania Journal of International Law for their editing and revisions. All opinions expressed in this Comment are my own.

Additionally, this Comment suggests ways to change the precautions that a commander must take in targeting in order to avoid punishing states for investing in technological innovation. Finally, this Comment suggests the creation of panels of military experts, legal experts, and cyber experts, to approve all cyber targeting.

## TABLE OF CONTENTS

## 1. INTRODUCTION

In today's interconnected, heavily networked world, cyberwarfare has become one of the most common ways that war is waged, and its popularity and effectiveness is only growing.[1] The days of battlefield standoffs between infantry and tank brigades of opposing state armies and fighting in battles of attrition are quickly giving way to cyberwarriors: individuals, both state-affiliated and non-state affiliated, sitting behind a computer screen, waging war from the comfort of their home.[2] Cyberwarfare has become particularly attractive for a number of reasons. First, it is cheaper to wage a cyberwar than a kinetic war.[3] Attacks can be

[1] *See* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1012 (2010) (claiming that as of 2010 approximately 140 states had developed cyber capabilities); *see also* Brian J. Egan, State Dep't Legal Advisor, Address at UC Berkeley School of Law: International Law and Stability in Cyberspace (Nov. 10, 2016) ("The remarkable reach of the Internet and the ever-growing number of connections between computers and other networked devices are delivering significant economic, social, and political benefits to individuals and societies around the world. In addition, an increasing number of States and non-State actors are developing the operational capability and capacity to pursue their objectives through cyberspace.").

[2] Modern warfare is based on effects-based operations, rather than on battles of attrition. The move from attrition-based warfare to effects-based warfare is very important. In an attrition framework, "the enemy is defeated by progressively weakening its military." In an effects-based framework, "operations utilise selective targeting and choice of means and methods of warfare to achieve a desired effect." HEATHER HARRISON DINNISS, CYBERWARFARE AND THE LAWS OF WAR 23–24 (2012). Technological advances have also "evolved the ability to wage war to the point where the concept of a line marking the heart of the battle no longer makes sense; battlefields have become multidimensional and entire countries have become the battlespace." *Id.* at 22. This technology is "easy-to-use, and capable of deployment from virtually anywhere." Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1023 (2007).

[3] *See* Brenner & Clarke, *supra* note 1, at 1013. The cost-effectiveness of cyberwarfare is particularly attractive for weaker states or non-state actors who do not have access to the same resources that larger, better off states have. Michael Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, 87 INT'L L. STUD 89, 102 (2011); *see also* Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 897 ("because of the potentially grave impact of CNA [computer network attack] on a state's infrastructure, it can prove a high gain, low risk option for a state outclassed militarily or economically. Moreover, to the extent that an opponent is militarily and economically advantaged, it is probably

made with the click of a mouse, rather than with expensive equipment and machinery. This helps to level the playing field between sides with different economic resources.[4] A poor state or a non-state actor can launch a cyber-attack against a state with a defense budget in the hundreds of billions,[5] whereas in traditional

technologically-dependent, and, therefore, teeming with tempting CNA targets."). Non-state actors can also benefit from the "open source" nature of cyber weapons. *See* Jack M. Beard, *Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law*, 47 VAND. J. TRANSNAT'L L. 67, 92 (2014) ("A powerful addition to the cyber capabilities of nonstate actors may ironically come from the arsenals of the most technologically advanced states. Soon after powerful states use their most sophisticated cyber weapons, the information necessary to recreate these weapons may be readily available for downloading from the Internet.").

[4] Brian Contos, *Analysis: Why Cyberwarfare is the Great Equalizer*, USA TODAY (May 30, 2013), https://www.usatoday.com/story/cybertruth/2013/05/30/cyberwarfare-developing-nations-use-of/2371687/ [https://perma.cc/9Y33-TUTT] ("The amount of resources and effort that a country must employ to launch a cyber-attack is significantly lower than fielding tanks, launching satellites, developing a clandestine agency or refining uranium."); *see also* Hollis, *supra* note 2, at 1033 (cyber operations "presents . . . non-state actors new means for reaching and affecting nation-states"). Poorer states and non-state actors also have less possibility of being significantly harmed by a cyber-attack as "emerging and frontier countries throughout parts of Latin America, Europe, Africa and Asia are less dependent on computers." *Id.* In contrast, "[c]yberattacks present a great risk to industrialized nations, which are highly connected and extremely dependent on computers from the electric grid and financial services to transportation and national defense." *Id.*

[5] *Compare Bad Guys Can Launch Cyber-Attacks for Just $6*, REUTERS (June 15, 2016), http://fortune.com/2016/06/15/bad-guys-can-launch-cyber-attacks-for-just-6-dollars/ [https://perma.cc/K7DN-7AQG] (describing an online underground marketplace which sells access to more than 70,000 compromised servers for only $6 per server and noting that once purchased, the compromised servers come equipped with software to launch a variety of cyber-attacks; access to government servers is not much more expensive at only $7 per server), *and* Denis Makrushin, *The Cost of Launching a DDoS Attack*, SECURELIST, https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/ [https://perma.cc/QH2X-HWC8] (last visited Mar. 1, 2019) (stating that the cost of launching a short attack against an online store is only $5 and that launching an attack using a botnet of 1,000 workstations can be as low as $7 per hour), *with* U.S. DEP'T OF DEF. OFFICE OF THE COMPTROLLER/CHIEF FIN. OFFICER, PROGRAM ACQUISITION COST BY WEAPON SYSTEM: UNITED STATES DEPARTMENT OF DEFENSE FISCAL YEAR 2018 BUDGET REQUEST (2017), https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2018/fy2018_Weapons.pdf [https://perma.cc/344Z-UQ5S] (requesting $397.4 million for 45 combat aircraft, as well as $3.4 billion for combat vehicles).

kinetic warfare they would most likely be overmatched. Second, cyberwarfare is safer for the combatants involved than traditional kinetic warfare. War can be waged from the comfort of one's home, rather than on a traditional battlefield.[6] This entails much less personal physical risk. Third, it is very difficult to attribute a cyber-attack to a particular actor—state or otherwise—and therefore it is much more difficult to be held responsible for a cyber-attack and face the related consequences.[7] Cyberwarfare is not fought face to face, and various techniques such as IP spoofing are available to help the attacker hide her true identity.[8] Finally, with the increasing reliance on networks and electronic communications, the damage that can be done through cyber-attacks has become truly devastating, and in many instances can be more effective than a traditional kinetic attack.[9]

The rise of cyberwarfare leads to many new challenges, as scholars, states, and militaries scramble to figure out how to regulate this new type of technologically-advanced warfare. The question of whether the current system of international humanitarian law is sufficient to regulate cyberwarfare, or whether a new regulatory system altogether is needed, is a question that is being hotly debated.[10] Two distinct camps have emerged. The first

[6] *See* Brenner & Clarke, *supra* note 1, at 1014 ("unlike their counterparts in traditional military organizations, cyber warriors operate remotely and launch cyberattacks from within the territory of their own nation-state. The remoteness of cyberwarfare effectively eliminates the likelihood of injury or death in a physical encounter with forces from an opposing nation-state.")

[7] *See* Brenner & Clarke, *supra* note 1, at 1014.

[8] *See infra* Section 2.4.

[9] *See* HEATHER HARRISON DINNISS, CYBERWARFARE AND THE LAWS OF WAR 12–13 (2012) (discussing the increase in digitally stored information and computer-run networks).

[10] *See generally* Michael A. Newton, *Proportionality and Precautions in Cyber Attacks*, *in* INTERNATIONAL HUMANITARIAN LAW AND THE CHANGING TECHNOLOGY OF WAR 230 (Dan Saxon ed., 2013) ("the modern globally connected era driven by information and interconnected civilian and military communications infrastructures presents wholly new challenges for the lawful conduct of relations between states."); Eric Boylan, Note, *Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners*, 50 VAND. J. TRANSNAT'L L. 217, 220–21 (2017) ("The absence of law specifically written or designed to deal with the nuances of cyber warfare, combined with the prevalent application of other fields that are only tangentially related, leads to a host of issues for practitioners in the realm of cyber warfare.").

is made up of scholars who believe that current international law can and should be applied to regulate cyber operations.[11] This camp can be divided into those who believe that international law as it currently stands is sufficient, and those who believe that certain updates must be made. The second camp is made up of those who believe that the current legal structure cannot regulate cyber operations—even if updated— and a completely new system must be created.[12] Defining "attack" in cyberwar and the difficulties of state attribution create serious problems. However, these problems are beyond the scope of this Comment.[13]

[11] *See* Harold Hongju Koh, State Dep't Legal Advisor, Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) ("This is not the first time that technology has changed and that international law has been asked to deal with those changes. In particular, because the tools of conflict are constantly evolving, one relevant body of law—international humanitarian law, or the law of armed conflict—affirmatively anticipates technological innovation, and contemplates that its existing rules will apply to such innovation."); *see also* Kate Jastram & Anne Quintin, Seminar at Berkeley Law: The Internet *in Bello*: Cyber War Law, Ethics & Policy (Nov. 18, 2011), https://www.law.berkeley.edu/wp-content/uploads/2015/04/cyberwarfare-seminar-summary-complete.pdf [https://perma.cc/8XLC-GE5L] ("if cyber means and methods produce the same effects as kinetic operations, they are—and should be—governed by the same rules.").

[12] *See* Beard, *supra* note 3, at 70 (arguing that "due to the unusual properties of information itself, there are serious problems and perils in relying on such analogies to extend the IHL framework to most events in cyberspace."); *see also* Michael Schmitt, *Cyber Operations and the Jus in Bello*, *supra* note 3, at 106 ("The dilemma is that IHL was crafted during a period in which the cyber operations were but science fiction.").

[13] The *Jus in Bello* regulations in the Geneva Conventions and the Additional Protocols only apply when an armed conflict occurs. Additional Protocol I applies in situations during an international armed conflict and Additional Protocol II applies in situations of non-international armed conflict. For the purpose of this Comment, I assume that an international armed conflict is present and that the cyber-attacks and operations contemplated rise to the level of an armed attack necessary for an armed conflict to be present and to render the Geneva Conventions and Additional Protocol I applicable. For a more in-depth discussion of armed attack and armed conflict in cyberwarfare, see generally David Turns, *Cyber War and the Concept of 'Attack' in International Humanitarian Law*, *in* INTERNATIONAL HUMANITARIAN LAW AND THE CHANGING TECHNOLOGY OF WAR (Dan Saxon ed., 2013); Christopher S. Yoo, *Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self Protective Measures*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (Jens David Ohlin, Kevin Govern & Claire Finkelstein eds., 2015); Beard, *supra* note 3; Yoram Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, 17 J. CONFLICT & SECURITY L. 261 (2012); Duncan B. Hollis, *Why States Need an International Law for Information*

This Comment will argue that current international law *can* effectively regulate targeting in cyberwarfare, but that significant changes must be made in order to update it for the modern age of warfare. The current framework of international humanitarian law has the capability of sufficiently regulating the problem of targeting, but it must be updated to match the realities of modern armed conflict.[14] This Comment will address two main issues related to the law of targeting. First, cyberwarfare exacerbates the dual-use problem that is also present in kinetic warfare. The interconnectedness of the cyber realm leads to many more dual-use targets—targets that serve both a civilian and a military function—than traditional kinetic warfare. The regulation of targeting dual-use infrastructure, and the proportionality assessment that goes along with it, must adapt for the reality that, arguably, almost any object can serve a military purpose.[15] Second, the law governing what precautions must be taken by commanders and other officials who are responsible for ordering attacks is insufficient in the course of cyberwarfare. The current precautions detailed in Article 57 of Additional Protocol I create unacceptable disparities between technologically-advanced states and non-technologically-advanced states in the precautions they must take to determine and verify

*Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007); Michael N. Schmitt, *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 CHI. J. INT'L L. 511 (2005); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999); Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, 89 INT'L L. STUD. 252 (2013).

[14] Note that Additional Protocol I contemplates the development of new weapons and states that a party to the protocol must determine whether the new weapon would be prohibited by the protocol. This suggests that the Protocol was developed with the intention and flexibility that it be modified and updated to keep up with advances in technology. Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 36, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]. For a discussion of how Article 36 applies to cyber weapons, *see* Jastram & Quintin, *supra* note 11 (comments by Anne Quintin, Public Affairs Officer, International Committee of the Red Cross).

[15] *See* Robin Geiss & Henning Lahmann, *Cyberwarfare: Applying the Principal of Distinction in an Interconnected Space*, 45 ISRAEL L. REV. 381, 383 (2012) ("because of the systemic technological setup of cyberspace in times of an armed conflict, basically every cyber installation—possibly even cyberspace as such—potentially qualifies as a military objective.").

objects of attack, and the means and methods of attack that must be used. These imbalances are much more apparent and troublesome in cyberwarfare than in kinetic warfare and can punish states for technological investment. This imbalance must be corrected through a more concrete, minimum standard of care that a commander is required to take to ensure that the object of attack is a military objective, and that the attack itself will not be otherwise unlawful in the methods and means used. Additionally, due to the technical nature of cyberwarfare, commanders should have to receive approval of a panel made up of a lawyer, a cyber expert, and a military commander, before launching a cyber-attack. This should make up for the knowledge gap that military technological innovation is bound to create.

The increased confrontation with dual-use infrastructure and the unbalanced rules regarding precautions to be taken before an attack leave an unacceptable amount of discretion and open-ended analyses in the hands of commanders, who may or may not be sufficiently trained to make important decisions in cyberwarfare. This Comment argues that current international law has the potential to effectively regulate cyberwarfare and military commanders in the area of targeting but must be seriously updated in order to do so effectively.

This Comment will proceed in four parts. Part I discusses major types of cyber operations that have occurred in recent history and are frequently used. Part II shifts to looking at the rise in investment in cyberwarfare capabilities, both domestically and internationally. Two major cyber operations, Stuxnet and the Russia-Estonia incident of 2007 are also explained. Part III looks at the current status of the regulation of targeting in international law and analyzes important provisions of Additional Protocol I to the Geneva Convention. Part IV discusses two major ways in which the current regulation of targeting falls short in the cyber context. In this section, I suggest updates to the current regulatory framework in order to make it more effective. Finally, I finish with a short conclusion.

## 2. TYPES OF CYBER OPERATIONS

While there are many ways that states and non-state actors can launch cyber operations in an effort to harm an opposing force, there are four main types of cyber operations that occur today.

This Part will briefly outline denial of service attacks, malicious programs, logic bombs, and IP spoofing. This is not intended to be an exhaustive detailing of all types of cyber operations, but instead it is intended to provide sufficient background information for a reader to understand how a cyber operation or cyber-attack could occur, how the law of targeting is affected, and in what manner certain updates would be beneficial.

### *2.1. Denial of Service ("DoS") Attack*

A Denial of Service ("DoS") attack is an attack that bombards a network with so many requests that access to the network or system is severely slowed down or interrupted.[16] Take, for example, a network that receives, on average, fifty requests per hour. Now imagine that the same network is bombarded with thousands of requests per minute. The network then shuts down due to an inability to handle the increased activity, and whatever services the network offered or sites it supported, are rendered unavailable. This can be incredibly important if governmental services websites are shut down, or an electronic banking network is shut down. A good analogy for a DoS attack is a doorway faced with exponentially increased pedestrian activity. If a few people try to enter through the doorway every minute or hour, it functions normally, but if thousands of people suddenly try to enter over the course of one minute, they will get stuck and will not be able to get through. The doorway will be unable to fulfill its function of letting people through and accessing whatever is inside. Its normal operation is disrupted. This is a very popular form of cyber operation as it requires very limited resources to execute. A permutation of the traditional DoS attack is a distributed denial of service ("DDoS") attack.[17] In a DDoS attack, many infected computers or systems attack one network or system.[18] In this

[16] Ari J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 63 A.F. L. REV 121, 134 (2009).

[17] The famous cyber-attack in 2007 on Estonia by Russia is an example of a DDoS attack. For a more detailed description of this attack, *see infra* notes 58-59 and accompanying text.

[18] *See* Schaap, *supra* note 16, at 134.

situation, the requests that will eventually shut down a network are coming from many different nodes, rather than from a single node. A DDoS attack is tremendously difficult to stop, as blocking one infected source of the attack will not stop the attack. The other thousands of nodes will continue to bombard the network with requests, even after one node is effectively neutralized.

### *2.2. Malicious Programs*

Malicious programs (often referred to as malware) are programs that either disrupt the normal functioning of computers or allow remote attackers to gain control of computers and manipulate them to disrupt their normal functioning.[19] Malicious programs often work by deleting files or corrupting them to the point that they are unusable. Examples of malware include viruses, worms, and Trojan horses. A virus will attach to a program or file and in this way spread from computer to computer. Viruses are attached to an executable file, meaning that it will only begin to infect a computer when a user opens or runs the malicious program.[20] In this way, a virus may exist on a computer but remain dormant until a user activates the virus by opening or running the program. A worm is similar to a virus but can travel without being activated by a user. It can replicate itself without the infected program or file even being opened.[21] A Trojan Horse is a harmful piece of software that is disguised as something that looks legitimate but in fact is just a piece of malware.[22] A user is then tricked by the appearance of legitimacy into opening the program and activating the malicious program. Unlike viruses and worms, Trojan Horses do not spread through infecting files or through self-replication.[23] They need to be opened or downloaded in order to work.

[19] *Id.* at 135.

[20] *Id.* at 136.

[21] *What is the Difference: Viruses, Worms, Trojans, and Bots?*, CISCO, https://www.cisco.com/c/en/us/about/security-center/virus-differences.html [https://perma.cc/992M-LDV5] (last visited Feb. 16, 2018).

[22] *Id.*

[23] *Id.*

### 2.3. *Logic Bombs*

A logic bomb is a malicious code that will execute its programmed task if a specific event occurs at a predetermined time.[24] Examples of events that would trigger a logic bomb could be a certain time or date, a specific file being deleted, or a pre-set amount of disk space being filled.[25] When the specific event occurs and the logic bomb is triggered, the logic bomb can perform a variety of different actions including deleting data or activating a DoS attack.[26] Imagine a disgruntled employee who creates a malicious code to self-execute in the event that the employee is fired. An example of the actual use of a logic bomb is a cyber-attack that struck computers at three banks and two media companies in South Korea in March 2013. The specified triggering event was a certain time and date, and once this specific time and date was reached, malware began to delete data from the computers.[27]

### 2.4. *IP Spoofing*

IP spoofing occurs when an attacker impersonates a different machine by faking the IP address of a trusted source and then uses this fake IP address to gain access to a machine or network.[28] The fake IP address then conceals the identity of the attacker or sender and makes it seem as if the information or virus being sent is coming from a trusted source or even from a machine within the receiver's network. IP spoofing is one of the most used methods of

[24] *See* Schaap, *supra* note 16, at 137.

[25] Stephen Northcutt, *Logic Bombs, Trojan Horses, and Trap Doors*, SECURITY LABORATORY, https://www.sans.edu/cyber-research/security-laboratory/article/log-bmb-trp-door [https://perma.cc/6HZP-UAFP] (last visited Feb. 16, 2018).

[26] *See* Schaap, *supra* note 16, at 137.

[27] Kim Zetter, *Logic Bomb Set Off South Korea Cyberattack*, WIRED (Mar. 21, 2013), https://www.wired.com/2013/03/logic-bomb-south-korea-attack/ [https://perma.cc/CKN3-2DL8].

[28] What is IP Spoofing? IP LOCATION, https://www.iplocation.net/ip-spoofing [https://perma.cc/L2VZ-8AHY] (last accessed Feb. 25, 2018).

carrying out an illicit cyber operation. By engaging in IP spoofing, an attacker can make it very difficult for an attack to be attributed to him.

### 3. EXAMPLES OF CYBER OPERATIONS AROUND THE WORLD

Over recent years, cyber operations[29] have become a very popular way of waging warfare throughout the world.[30] Across the globe, state, as well as non-state actors, have begun to invest

[29] Terminology is important in the cyber context. Although the definitions of cyber operation and cyber-attack are hotly debated, and no one definition has been settled on, a useful starting place are the definitions offered by the Joint Chiefs of Staff in 2011. In a memorandum, they state that a cyber operation is "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyber space." Vice Chairman of the Joint Chiefs of Staff, U.S. Dep't of Def., Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands Directors of the Joint Staff Directorates: Joint Terminology for Cyberspace Operations (2011). A cyber-attack is defined as "A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions." *Id.* Cyberwarfare is defined as "An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber-attack, cyber defense, and cyber enabling actions." *Id.* The Tallinn Manual defines a cyber-attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0]. It is important to note in these definitions that cyber operations are a broader category that is inclusive of cyber-attacks. Michael N. Schmitt argues that "A cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects." Michael Schmitt, *Cyber Operations and the Jus in Bello*, *supra* note 3, at 94. For a more in-depth discussion of definitions and terminology in the cyber context, *see* Oona A. Hathaway & Rebecca Crootof, *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 817 (2012) (examining cyber operations within the existing framework provided by the law of war, international treaties, and domestic criminal law); Daniel Hughes & Andrew Colarik, *The Hierarchy of Cyber War Definitions*, *in* PACIFIC-ASIA WORKSHOP ON INTELLIGENCE AND SECURITY INFORMATICS 15 (2017) (analyzing the origins and patterns of usage of cyber terminology across over one hundred documents). For a more detailed discussion of what actions rise to the level of a cyber-attack, *see supra* note 13.

[30] *See supra* notes 2–9.

heavily in creating cyber capabilities, both offensive and defensive. As of 2013, more than 140 countries had some form of funded cyber development program.[31] While many states have developed cyber capabilities, a few states have been leaders in technological development, innovation, and use in this field. This Part will look at cyber operations and investment in cyber capabilities of China, North Korea, Russia, and the United States.

### *3.1. China*

China has stated that its goal is to "achieve global 'electronic dominance' by 2050." This would enable it to target the financial markets, military, critical infrastructure and civilian communications of other countries through cyber means.[32] China is also extremely vulnerable to a cyber-attack since it has the world's largest internet using population. Therefore, it has also decided to invest significant funds in cyber defense. Over the last fifteen years, China has engaged in a number of cyber operations such as "Titan Rain"[33], "Aurora"[34], "Night Dragon"[35] and "Shady Rat"[36]. Importantly, in 2015 China established the Strategic

[31] Peter Suciu, *Why Cyber Warfare is So Attractive to Small Nations*, FORTUNE (Dec. 21, 2014), http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/ [https://perma.cc/5L26-6DCU].

[32] ANDREW F. KREPINEVICH, CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS, CYBER WARFARE: A "NUCLEAR OPTION"? 27 (2012).

[33] Titan Rain was a campaign of coordinated attacks originating in china and beginning in 2003 in which the hackers targeted American defense contractor computer networks in order to extract sensitive information. It is disputed as to whether the attacks were an initiative of the Chinese government or were committed by individual Chinese citizens. *Id* at 31–32.

[34] Aurora was a cyber-attack occurring in 2009 in which a computer attack originating in China was able to penetrate Google, as well as other companies and organizations, and steal information. *Id* at 35–37.

[35] Night Dragon was a set of coordinated cyber-attacks aimed against global oil and energy companies. William Pentland, *Night Dragon Attacks Target Technology in Energy Industry*, FORBES (Feb. 19, 2011), https://www.forbes.com/sites/williampentland/2011/02/19/night-dragon-attacks-target-technology-in-energy-industry/#409e066c1d49 [https://perma.cc/4U7Q-VPQH].

[36] Shady Rat was an operation, also occurring around 2009, targeting fourteen different countries through spear phishing that included an email with

Support Force (SSF) which guides its space and cyber missions.[37] The SSF has been described as an organization that "uniquely conducts several different missions simultaneously that in the U.S. would be happening at the National Security Agency, Army, Air Force, Department of Homeland Security, NASA, State Department and Cyber Command . . . . If you combined all of those government entities and added companies like Intel, Boeing and Google to the mix, then you would come close to how the SSF is built to operate."[38] The creation of the SSF is part of a strategy to catch up to the U.S. in cyber capabilities. In an effort to catch up, "China is improving training and domestic innovation to achieve its cyber capability development goals. PLA [People's Liberation Army] researchers advocate seizing 'cyberspace superiority' by using cyber operations to deter or degrade an adversary's ability to conduct military operations against China."[39] The U.S. Department of Defense warns that "the PLA may seek to use its cyberwarfare capabilities to collect data for intelligence and cyber-attack purposes; to constrain an adversary's actions by targeting network-based logistics, communications, and commercial activities; or to serve as a force-multiplier when coupled with kinetic attacks during times of crisis or conflict."[40] China is a country with a history of cyber operations, that has made a commitment to expanding its future cyber capabilities.

malware. Information obtained through this attack included "national secrets, source code, databases and SCADA configurations." *See* KREPINEVICH, *supra* note 32, at 34–35.

[37] U.S. DEP'T OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 34 (2017), https://dod.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF [https://perma.cc/9DCB-7DME]. Elsa Kania, a U.S. national security analyst, stated that while it is difficult to determine the budget or manpower of the SSF, she anticipated that both are sizable. *See* Chris Bing, *How China's Cyber Command is Being Built to Supersede its U.S. Military Counterpart*, CYBERSCOOP (June 22, 2017), https://www.cyberscoop.com/china-ssf-cyber-command-strategic-support-force-pla-nsa-dod [https://perma.cc/4MHM-9SQS] ("I would anticipate that both will be sizable — given the SSF's apparent scope and scale, as well as the importance of these missions").

[38] *See* Bing, *supra* note 37.

[39] *Id.* at 51.

[40] *Id.* at 59.

### *3.2. North Korea*

North Korea is another country that has focused heavily on building cyber capabilities over recent years. Much of North Korea's cyber program was developed when Kim Jung Un came to power after his father's death in 2011.[41] The centerpiece of the North Korean cyber program is Bureau 121, an elite cyber unit comprised of North Korean Hackers.[42] In 2014, Bureau 121 entered the international spotlight following a cyber operation on computers at Sony Pictures Entertainment. Allegedly this hacking was in response to Sony's release of "The Interview," a comedy about an assassination attempt on Kim Jung Un.[43] While the North Koreans have denied a role in this attack, overwhelming evidence points to their involvement.[44] In addition to hacks against

[41] David E. Sanger, David D. Kirkpatrick & Nicole Perlroth, *The World Once Laughed at North Korean Cyberpower. No More.*, N.Y. TIMES (Oct. 15, 2017), https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html [https://perma.cc/2BVZ-JD6A].

[42] *See* Dave Lee, *Bureau 121: How Good Are Kim Jong-Un's Elite Hackers?*, BBC NEWS (May 29, 2015), http://www.bbc.com/news/technology-32925503 [https://perma.cc/F6W5-FZWY] (reporting on North Korea's elite hackers). The best computer science students in North Korea are chosen for this unit and are given additional training in countries such as China, Japan, or various European countries. *Id.* It is estimated that approximately 1,800 hackers make up this elite unit. *See* Ju-Min Park & James Pearson, *In North Korea, Hackers Are a Handpicked, Pampered Elite*, REUTERS (Dec. 5, 2014), https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205 [https://perma.cc/C4N7-SVU5]. Many of these hackers learned their computer skills in New York universities while working for North Korean missions to the United Nations. Sanger, Kirkpatrick & Perlroth, *supra* note 41.

[43] *See* David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES (Dec. 17, 2014), https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html [https://perma.cc/8EE8-5CJ7S]. The attack caused the four largest movie theater chains in the U.S. to cancel showings of the movie. *Id.*

[44] *See* Press Release, FBI National Press Office, Update on Sony Investigation (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation [https://perma.cc/BSW8-9WHW] ("As a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions."); *see also* Sam Frizell, *NSA Director on Sony Hack: "The Entire World is Watching"*, TIME (Jan. 9, 2015), http://time.com/3660757/nsa-michael-rogers-sony-hack/

America, North Korea has allegedly committed cyber-attacks against South Korea, both in a series of DDoS attacks from 2009–2011 and then again in 2013 with cyber-attacks targeting banking, media, and governmental targets in South Korea.[45] Recently, the U.S., along with a number of other countries, accused North Korea of being behind the WannaCry ransomware attack.[46] This attack targeted computers running the Microsoft Windows operating system and affected computers in over 150 countries. In 2016 General Vincent Brooks, Commander of U.S. forces in South Korea, told Senate leaders "While I would not characterize them [North Korea] as the best in the world, they are among the best in the world and the best organized."[47] North Korea is a good example of a relatively poor country seeking to level the playing field through the use of more cost-effective cyber-attacks.[48] Cyber weapons are

[https://perma.cc/9DGS-EJ4J] (quoting NSA Director Michael Rogers, "I remain very confident: this was North Korea."). Some analysts and journalists argue that North Korea might not have been responsible for the attack. *See, e.g.*, Michael Hitzik, *The Sony Hack: What if it isn't North Korea?*, L.A. TIMES, (Dec. 19, 2014), http://www.latimes.com/business/la-fi-mh-the-sony-hack-20141219-column.html [https://perma.cc/R298-8SQZ ] (detailing the concerns of some security experts regarding North Korean involvement).

[45] U.S. DEP'T OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA 11 (2013), https://apps.dtic.mil/dtic/tr/fulltext/u2/a596219.pdf [https://perma.cc/93UA-93X3].

[46] *See* Thomas P. Bossert, *It's Official: North Korea is Behind WannaCry*, WALL STREET J. (Dec. 18, 2017), https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537 [https://perma.cc/H6XK-KZ23] (stating that the United Kingdom also agrees that North Korea is behind the attack); *see also White House Says WannaCry Attack Was Carried Out by North Korea*, CBS NEWS (Dec. 19, 2017) https://www.cbsnews.com/news/white-house-says-wannacry-attack-was-carried-out-by-north-korea/ [https://perma.cc/2ENC-8HW4 ] (noting that Canada, New Zealand and Japan also agree that North Korea is behind the attack).

[47] Paul Szoldra, *A US Army General Says North Korea Has Some of the World's Best Hackers*, BUS. INSIDER (May 10, 2016), http://www.businessinsider.com/north-korea-worlds-best-hackers-2016-5 [https://perma.cc/8QKC-QGEG ].

[48] U.S. DEP'T OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (2013), *supra* note 45, at 11; *see also* KREPINEVICH, *supra* note 32, at 76–77 ("What may prove significant is North Korea's ability to execute a fairly sophisticated cyber-attack despite its status as one of the world's most backward nations, especially when it comes to its IT infrastructure and the IT literacy of the vast majority of its people); Sanger, Kirkpatrick & Perlroth, *supra* note 41 (quoting Chris Inglis, a former

far less expensive for the relatively poor country to develop and since North Korea does not have very technologically-advanced infrastructure, it leaves them less open to a cyber-attack than a more developed nation. North Korea's cyber program has grown tremendously over the last decade, and experts expect it to continue to grow.[49]

### *3.3. Russia*

Russia has arguably the most sophisticated cyber capabilities of any nation. Professor James Wirtz of the Department of National Security Affairs at the Naval Postgraduate School has stated, "Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyberwarfare into a grand strategy capable of achieving political objectives."[50] In 2014, the Russian government announced that it was going to create a special military cyber unit which would be responsible for both offensive and defensive operations. The original budget for this unit was to be approximately $70 million and was to be completed by 2017.[51] Much of Russia's governmental cyber capabilities are intertwined with the cyber capabilities of the Russian Business Network (RBN),[52] a non-governmental criminal group based in St.

deputy director of the NSA, "Cyber is a tailor-made instrument of power for them . . . . There's a low cost of entry, it's largely asymmetrical, there's some degree of anonymity and stealth in it's use . . . . You could argue that they have one of the most successful cyber programs on the planet, not because it's technically sophisticated, but because it has achieved all of their aims at very low cost.").

[49] *See* Sanger, Kirkpatrick & Perlroth, *supra* note 41.

[50] James J. Wirtz, *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy, in* CYBER WAR IN PERSPECTIVE: RUSSIAN AGGRESSION AGAINST UKRAINE (Kenneth Geers ed., 2015).

[51] MICHAEL CONNELL & SARAH VOGLER, CNA ANALYSIS & SOLUTIONS, RUSSIA'S APPROACH TO CYBER WARFARE 8 (2017), https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf [https://perma.cc/FET9-USBW].

[52] It is unclear exactly what connection the Russian government has to the RBN and what influence they have. *See* John Markoff, *Before the Gunfire, Cyberattacks,* N.Y. TIMES (Aug. 12, 2008),

Petersburg. Russia has been accused of using cyber-attacks alongside more traditional kinetic attacks.[53] In its invasion of Georgia in the summer of 2008, Russia allegedly aided and complemented their ground invasion of Georgia with a series of DoS attacks designed to take down Georgian networks and websites.[54] These DoS attacks often coincided with Russian air strikes, strengthening the case that the cyber-attacks were government sponsored attacks designed to aid in the overall campaign.[55] Russia has also used cyber operations to coerce other states into taking certain actions that would benefit them. In 2009, Russia launched a series of DDoS attacks against Kyrgyzstan, taking down websites and email accounts throughout the country.[56] The attacks coincided with the Russian pressure on Kyrgyzstan to terminate U.S. access to an airbase at Manas, a city in Kyrgyzstan. The U.S. had been using the airbase to aid in its military efforts in Afghanistan. Shortly after these DDoS attacks, Kyrgyzstan ended U.S. use of the airbase.[57] One of the earliest, and most famous, large scale cyber operations was Russia's DoS attacks in Estonia in 2007. In 2007, Estonian officials moved a Soviet-era memorial that celebrated an unknown Russian who died while fighting against the Nazi's in World War II from Central Tallinn to a cemetery on the outskirts of the city.[58] This led to violent, deadly

https://www.nytimes.com/2008/08/13/technology/13cyber.html [https://perma.cc/GE5A-ZBLA].

[53] Russia uses cyber operations as a "multiplier, which is a military term that describes a weapon or tactic that, when added to and employed along with other combat forces, significantly increases the combat potential of that force." *See* Schaap, *supra* note 16, at 133.

[54] The DoS attacks succeeded in taking down important government websites and disrupting government communications. *See* CONNELL & VOGLER, *supra* note 51, at 17.

[55] *See id.* at 53–54. While Georgia accuses the Russian government of carrying out these operations, the Russian government denies this. *See* Markoff, *supra* note 52.

[56] *Id.* at 55.

[57] *Id.* at 56.

[58] *See* David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 MINN. J. INT'L L. 347, 349 (2013). The attack coincided with the date that Russia celebrates Victory in Europe Day. *See* Emily Tamkin, *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?*, FOREIGN POL'Y (Apr. 27, 2017), http://foreignpolicy.com/2017/04/27/10-years-after-the-

protests, and then to a series of DDoS attacks against Estonian government websites. The volume of the attacks caused the websites to shut down for hours at a time over the course of weeks.[59] Eventually NATO and the U.S. sent cyber experts to try to help Estonia. Estonia has blamed Russia for the attack, but Russia has never taken responsibility. Russia has also used cyber operations in order to achieve intended kinetic effects. In 2015, Russia attacked Ukraine's power grid through coordinated cyber operations. They attacked three distribution centers of a Ukrainian power company in Western Ukraine.[60] This caused major power outages throughout the country. Perhaps Russia's most famous cyber operations, though, have been its alleged attempts to influence the 2016 U.S. presidential election.[61]

### *3.4. United States of America*

The U.S. also places great importance on developing cyber capabilities, both offensive and defensive. In 2015 the Department of Defense listed three primary missions in cyberspace. The first is to "defend its own networks, systems, and information."[62] The

landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/ [https://perma.cc/L34E-NU2X].

[59] *Id.* at 350. Online bank accounts and newspapers also became inaccessible during the attacks. *See* Tamkin, *supra* note 58.

[60] *See* CONNELL & VOGLER, *supra* note 51, at 20–21.

[61] *See* Ellen Nakashima, *Cybersecurity Firm Finds Evidence that Russian Military Unit was Behind DNC Hack* WASH. POST (Dec. 22, 2016) https://www.washingtonpost.com/world/national-security/cybersecurity-firm-finds-a-link-between-dnc-hack-and-ukrainian-artillery/2016/12/21/47bf1f5a-c7e3-11e6-bf4b-2c064d32a4bf_story.html?utm_term=.07a72e343410 [https://perma.cc/8ASS-VB5H] (providing evidence showing Russia's involvement with the hack of the Democratic National Committee); Adam Entous and Ellen Nakashima, *FBI in Agreement with CIA that Russia Aimed to Help Trump Win White House*, WASH. POST (Dec. 16, 2016), https://www.washingtonpost.com/politics/clinton-blames-putins-personal-grudge-against-her-for-election-interference/2016/12/16/12f36250-c3be-11e6-8422-eac61c0ef74d_story.html?utm_term=.8a7a37bec6a2 [https://perma.cc/XG8B-KP48] (detailing FBI and CIA assessments of Russia's involvement in the 2016 election).

[62] U.S. DEP'T OF DEFENSE, CYBER STRATEGY 4 (2015), http://archive.defense.gov/home/features/2015/0415_cyber-

second is to "defend the United States and its interests against cyber-attacks of significant consequence."[63] This includes conducting cyber operations to counter an attack against the U.S. or U.S. interests. The third mission is that DoD "must be able to provide integrated cyber capabilities to support military operations and contingency plans."[64] The DoD includes a special Cyber Mission Force (CMF) to help the DoD carry out its cyber mission. The CMF is made up of 6,200 people, including members of the military, civilians, and contractors. Once fully completed and operational, the CMF will be composed of 133 teams, each with its own mission.[65]

The U.S. has identified a number of key cyber threats which it must protect against. These include countries such as Russia, China, North Korea, and Iran, as well as non-state actors such as ISIL and various criminal actors.[66]

DoD's budget reflects the growing importance it places on developing cyber capabilities. In the budget request for 2017, Defense Secretary Ash Carter requested $6.7 billion for a cyber budget, a 15% increase over the previous year.[67] Over the course of 2017-2021, the budget would call for $34.6 billion to be spent on cyber capabilities. Included in this budget are funds to support training, weapons development, deterrence capabilities, capabilities to disrupt incoming attacks, offensive capabilities, as well as funds to support research and development.[68]

strategy/final_2015_dod_cyber_strategy_for_web.pdf [https://perma.cc/5KJV-M9MB].

[63] *Id.* at 5.

[64] *Id.* at 5–6.

[65] *Id.* at 6–8. As of June 2016, 46 of the 133 teams were fully operational. *See also* William Matthews, *Unpacking DoD's Cyber Strategy and $6.7B Spending Plan*, GOVTECH WORKS (Jul. 13, 2016), https://www.govtechworks.com/unpacking-dods-cyber-strategy-and-6-7b-spending-plan/ [https://perma.cc/RC5B-3PE3].

[66] *Id.* at 8.

[67] Matthews, *supra* note 65.

[68] Secretary of Defense Ash Carter, Submitted Statement to the Senate Armed Services Committee on the FY 2017 Budget Request for the Department of Defense (Mar. 17, 2016), at 23–24, https://www.armed-services.senate.gov/imo/media/doc/Carter_03-17-16.pdf [https://perma.cc/2Z4M-ULWS].

Importantly, in 2017 the DoD initiated a process to elevate U.S. Cyber Command to a unified combatant command.[69] President Trump stated that "[t]his new combatant command will strengthen our cyberspace operations and create more opportunities to improve our nation's defense."[70] The Cyber Command, led by the NSA director, was established in 2009 and is currently a subordinate Unified Combatant Command of U.S. Strategic Command. The Cyber Command "plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[71]

The United States, along with Israel, launched perhaps the most infamous cyber-attack to date, Stuxnet. Stuxnet was a joint project between the U.S. and Israel to disrupt the Iranian nuclear program, initiated under the code name "Olympic Games" in 2006.[72] In 2010 it reached a computer through an employee flash drive in an underground Iranian nuclear facility in Natanz.[73] The virus took the form of a worm that suddenly sped up and slowed

[69] The other Unified Combatant Commands are United States Africa Command (USAFRICOM), United States Central Command (USCENTCOM), United States European Command (USEUCOM), United States Northern Command (USNORTHCOM), United States Pacific Command (USPACOM), United States Southern Command (USSOUTHCOM), United States Special Operations Command (USSOCOM), United States Strategic Command (USSTRATCOM), and United States Transportation Command. The most recently created was USAFRICOM in 2007. *See* U.S. DEP'T OF DEF., UNIFIED COMMAND PLAN, https://www.defense.gov/About/Military-Departments/Unified-Combatant-Commands/ [https://perma.cc/6E9S-KZTE] (showing the list of unified combatant commands).

[70] Jim Garamone & Lisa Ferdinandi, *DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command*, U.S. DEP'T OF DEF. (Aug. 18, 2017), https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/ [https://perma.cc/EP93-P2N5].

[71] U.S. DEP'T OF DEF., U.S. CYBER COMMAND FACT SHEET (May 25, 2010), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf [https://perma.cc/3L4H-9M4N] (last visited Mar. 1, 2019).

[72] Weissbrodt, *supra* note 58, at 351.

[73] *Id.*

down the centrifuges being used to enrich uranium, causing the centrifuges to break. Even though the centrifuge speed was rapidly changing, the worm was designed in such a way that the monitoring computers showed that the centrifuges were functioning at a normal speed.[74] Eventually there was an error in the program that allowed the worm to spread, and it infected over 100,000 computers worldwide. The worm did prove to be effective though, and some claim that it set the Iranian nuclear program back by approximately 18 months.[75]

### 4. CURRENT REGULATION OF THE LAW OF TARGETING

The law of targeting, and the principle of distinction, which calls for the distinction between combatants and military objectives on the one hand, and civilians and civilian objects on the other hand, is thought of as one of the most important, if not *the* most important principal in international humanitarian law.[76] The principle was first stated in the preamble to the 1868 St. Petersburg Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight: "The only legitimate object, which States should endeavor to accomplish during war, is

[74] *Id.*

[75] *Id.* at 352.

[76] *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 257 (July 8) ("The cardinal principles contained in the texts constituting the fabric of humanitarian law are the following. The first is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants; States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets."); Elizabeth Mavropoulou, *Targeting in the Cyber Domain: Legal Challenges Arising From the Application of the Principle of Distinction to Cyber Attacks*, 4 J.L. & CYBER WARFARE 37 (2015) ("the principle of distinction forms the cornerstone on which international humanitarian law stands."); Alexandre Cabral Campelo Hierro Lopes, Conduct of Hostilities: Precautions in Attack (2015) (unpublished master's dissertation, Universidade Catolica Portuguesa), https://repositorio.ucp.pt/bitstream/10400.14/20456/4/Conduct%20of%20Hostilities.pdf [https://perma.cc/N964-X6U6] ("The Principle of Distinction is one of the most important rules of IHL, having the responsibility of avoiding or at least reducing nasty consequences of war for the civilian population.").

to weaken the military forces of the enemy."[77] It was further refined in the Hague Convention of 1899, revised in 1907, forbidding parties "[t]o employ arms, projectiles, or material calculated to cause unnecessary suffering."[78]

Today, the principle of distinction, and the other laws regulating targeting in international armed conflicts are located in Part IV of Additional Protocol I to the Geneva Conventions, which specifically deals with the treatment of civilians.[79]

Article 48 articulates the basic rule of respect for civilians and civilian objects, stating that "the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[80]

Article 51 deals specifically with the civilian population and states that civilians should not be made the object of attack unless they directly participate in the hostilities.[81] Additionally, Article 51 prohibits indiscriminate attacks, which are attacks that (a) are not directed at a specific military objective, (b) employ a means or method which cannot be directed at a specific military objective, or (c) employ a means or method that are of a nature to strike civilian objects and military objectives without distinction.[82] Perhaps most importantly for the purposes of this Comment, Article 51 contains the principle of proportionality. It states 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,

[77] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Dec. 11, 1868, 138 Consol. T.S. 297, 298.

[78] Conventions Respecting the Laws and Customs of War on Land art. 23, Oct. 18, 1907, 36 Stat. 2277.

[79] Additional Protocol I, *supra* note 14. 173 out of 193 states are party to this Protocol. Although certain notable states are not party to Additional Protocol I, they are still bound to follow the provisions as they are now reflective of customary international law. *See* Michael N. Schmitt & Eric W. Widmar, *"On Target": Precision and Balance in the Contemporary Law of Targeting*, 7 J. NAT'L SECURITY L. & POL'Y 379, 381 (2014) (Dispelling the notion that IHL targeting law is inapplicable in cases where a non-signatory state is involved, because Additional Protocol I is generally regarded as customary international law).

[80] Additional Protocol I, *supra* note 14, art. 48.

[81] *See id.* art. 51(1)–(3).

[82] *Id.* art. 51(4).

which would be excessive in relation to the concrete and direct military advantage anticipated" is illegal and violates international law.[83]

Article 52 importantly states that civilian objects should not be attacked, and then defines a military objective as, "limited to 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, offer a definite military advantage."[84] Additionally, Article 52 states that in the case of doubt as to whether an objective is being used for military or civilian purposes, it should be presumed to be civilian.[85]

Article 54 calls for the protection of objects indispensable to the survival of the civilian population.[86]

Finally, Article 57 details precautions that commanders must take in planning and carrying out an attack.[87] This Article calls for those who plan or decided upon an attack to (i) do everything feasible to determine that the objects or population under attack is civilian, and (ii) to take feasible precautions in choosing the means and methods of attack to minimize collateral damage.[88] Article 57 goes on to state that the duty to take precautions is an ongoing duty and an attack should be canceled if it becomes apparent that the target is not military or if the attack is expected to cause excessive collateral damage. Finally, Article 57 states that when

[83] *Id.* art. 51(5)(b).

[84] *Id.* art. 52(2). Article 52(2) lists four ways that an objective could become military. The commentary to Additional Protocol I discusses these ways further. Nature "refers to objects which, by their 'nature,' make an effective contribution to military action." INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 636 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) [hereinafter ICRC COMMENTARY ON PROTOCOL I]. Location refers to objects that don't have a military function, but contribute to military action based solely on where they are located. *Id.* Purpose refers to the intended future use of the object. *Id.* This is differentiated from use which refers to the current use of the object. *Id.* Civilian object is defined in the negative, as "civilian objects are all objects which are not military objectives." Additional Protocol I, *supra* note 14, art. 52(1).

[85] Additional Protocol I, *supra* note 14, art. 52(3).

[86] *Id.* art. 54.

[87] *Id.* art. 57.

[88] *Id.* art. 57(2).

there is a choice between targeting military objectives that will provide a similar military advantage, the commander should choose to target the objective that will cause the least danger to civilians and civilian objects.[89] While these Articles are designed to regulate traditional kinetic warfare, this Comment will argue that they do have the potential to also effectively regulate cyberwarfare, subject to updates in two important areas that will be detailed in Part IV.

### 5. THE LAW OF TARGETING IN CYBERWARFARE

This Part will focus on the main theme of this Comment: that the current international law regulating targeting in cyberwarfare is insufficient and must be updated in order to regulate modern cyberwarfare. So far, the most extensive work on regulating cyberwarfare has been the Tallinn Manual. This project started in 2009 when the NATO Cooperative Cyber Defense Centre of Excellence ("NATO CCD COE"), based in Tallinn, Estonia, invited an independent group of international law experts to create a manual on regulating cyberwarfare.[90] In 2013, this group published the first edition of the Tallinn Manual, which focused exclusively on cyber operations occurring in the context of armed conflicts. In 2017, the group of experts published the second edition of the Tallinn Manual ("Tallinn Manual 2.0") which supersedes the first edition and also discusses international law relating to cyber operations during peacetime.[91] The Tallinn Manual is not binding, nor does it represent the opinion of any state or international organization. It is intended to be "an objective restatement of the *lex lata*."[92] In writing the Tallinn Manual, the experts acted under the presumption that existing international law could be applied to cyber operations and saw their task as determining how existing international law applies in

[89] *Id.* art. 57(3).

[90] *See generally* TALLINN MANUAL 2.0, *supra* note 29.

[91] *Id.* at 3.

[92] *Id.*

the cyber context.[93] The Tallinn Manual 2.0 is made of 154 rules, and accompanying commentary in the categories of (1) General International Law and Cyberspace, (2) Specialized Regimes of International Law and Cyberspace, (3) International Peace and Security and Cyber Activities and (4) The Law of Cyber Armed Conflict. This Comment recognizes much of the work of the Tallinn Manual as a good starting point and relies on a similar method of attempting to update existing international law for cyberwarfare, rather than developing a new system altogether.

This Comment will discuss two different areas that must be updated. Section 5.1 will discuss the targeting of dual-use objectives and will focus on the problems caused by the increased confrontation with dual-use objectives in cyberwarfare, as compared with traditional kinetic warfare. Section 5.2 will argue that the rules regulating the precautions a commander must take before launching an attack, and while the attack is occurring, are insufficient for cyberwarfare. This Section will argue that the current regulation encourages a race to the bottom and places an unfair burden on states and non-state actors that choose to invest in technological advancement. In each case, this Comment argues that while the general framework of international humanitarian law, and specifically Additional Protocol I, has the potential to effectively regulate targeting in cyberwarfare, certain updates and modifications must be made to the Articles of Additional Protocol I in order to properly do so.

### 5.1. *Targeting Dual-Use Infrastructure in Cyberwarfare*

The regulation targeting the dual-use objectives must be updated for cyberwarfare in order to take into account knock-on effects in the proportionality assessment, and to give commanders enough explicit guidance to determine whether their cyber-attacks pass the proportionality analysis.

[93] *Id.*

### *5.1.1. The Exacerbation of the Dual-Use Problem in Cyberwarfare*

While dual-use objects and infrastructure are present in traditional kinetic warfare, they are far more prevalent in cyberwarfare.[94] This is due to the increasing importance of the Internet, computer networks, and cyberspace in the 21st century. Often the military uses civilian networks for communications purposes.[95] In fact, it is estimated that 98% of government communications travel through civilian networks and lines.[96] Additionally, the military relies heavily on civilian providers for military computer software and hardware, as well as related services and maintenance.[97] The military information being sent over civilian lines and civilian networks includes, presumably, classified orders, instructions for carrying out military operations, and intelligence reports, all of which would be categorized as military objectives.[98] While Additional Protocol I does not explicitly mention dual-use objects in its definition of military

[94] *See* Henry Shue & David Wippman, *Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions*, 35 CORNELL INT'L L.J. 559 (2002) ("as technologically developed societies become ever more dependent on the uninterrupted functioning of basic infrastructure for the satisfaction of both civilian and military needs, the problems posed by attacks on such infrastructure will only increase.").

[95] *See* Jastram & Quintin, *supra* note 11, at 3 ("Cyber space is characterized by interconnectivity. According to a recent Department of Defense report, DOD employees operate 15,000 computer networks with 7 million computers at hundreds of locations around the world. Nearly all military cyber infrastructure relies on civilian networks.").

[96] *See* Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1533 (2010); *see also* Eric Talbot Jensen, *Unexpected Consequences From Knock-On Effects: A Different Standard For Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1158–59 (2003) ("unless an attack originates on a Department of Defense ("DOD") computer and travels solely over military communications equipment to an enemy's military communications network, it will at some point be conducted by some medium that is civilian in nature and therefore, involve civilian objects.").

[97] Jensen, *Cyber Warfare*, *supra* note 96, at 1533.

[98] *Id.* at 1542.

objectives, it is well established that if an object has both a civilian and a military use, it should be considered a military objective.[99]

The integration of civilian and military networks could potentially render almost any civilian object military.[100] Just because a dual-use object is categorized as a military objective, however, does not necessarily mean that it can be attacked. It is still subject to a proportionality analysis which weighs harm to the civilian population against the expected military advantage to be gained. Specifically, the proportionality principle is stated as a prohibition on "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."[101] If the harm to the civilian population is disproportionate to the expected military advantage, the attack is unlawful, regardless of whether or not the attack is against a military objective.[102] While the proportionality assessment does reign in the potential for attacks on dual-use infrastructure, a more explicit and inclusive proportionality analysis is needed in the cyber context. The current proportionality assessment as expressed in Article 51(5)(b) is too heavily dependent on the subjective analysis of a specific commander.[103] It also is not

[99] *See* Geiss & Lahmann, *supra* note 15, at 389 (the general view appears to be that any military use, however minimal, would render a civilian object a military objective).

[100] *Id.*, at 389 ("It follows that in a future 'cyber war' the established definition of military objectives, despite striking an accepted balance between military needs for flexibility and civilian protection in traditional armed conflicts, could render basically every component of the cyber infrastructure a legitimate military objective"). Specific examples of traditionally civilian objects that may fall into the dual-use category in cyberwarfare include "computer networks of certain research facilities, air traffic control networks that regulate both civilian and military aircraft, computerized civilian logistics systems upon which military supplies will be moved, electronic power grid control networks, communications nodes and systems, including satellite and other space-based systems, railroad and other transportation systems, civilian government networks, and oil and gas distribution systems." *See* Jensen, *Unexpected Consequences*, *supra* note 96, at 1159–60.

[101] Additional Protocol I, *supra* note 14, art. 51(5)(b).

[102] *See* Schaap, *supra* note 16, at 157.

[103] *See* Lopes, *supra* note 76 ("Its [the proportionality assessment's] practical application is however very difficult for the concepts that form this principle . . .

structured to sufficiently take into account knock-on effects, which can be difficult to predict.

### *5.1.2. Attempts by the Tallinn Manual Experts to Regulate the Targeting of Dual-Use Objectives*

The Tallinn Manual attempts to regulate the targeting of dual-use objects, and states in rule 101 that "[c]yber infrastructure used for both civilian and military purposes is a military objective."[104] In this way it mirrors Article 52 of Additional Protocol I. In the commentary to rule 101, the Tallinn Manual states that "[t]his principle confirms that all dual-use objects and facilities are military objectives, without qualification."[105] The Tallinn Manual contemplates the unique challenges that dual-use objectives pose in cyberwarfare, describing a network that is used for both civilian and military purposes.[106] Unlike in traditional kinetic warfare, it may be impossible to differentiate which part of the network will carry military transmissions. The Tallinn Manual states that "in such cases, the entire network (or at least those aspects in which transmission is reasonably likely) qualifies as a military objective."[107] Therefore, as long as it passes the proportionality analysis, it could legitimately be attacked as a military objective.

While the Tallinn Manual provides a good starting place, in that it specifically refers to dual-use objectives, gives a general rule on how they should be treated, and discusses a few pertinent

are quite subjective. It is indeed understandable that in some war situations, deciding if an attack will or will not have an excessive damage, might be an extremely complicated task. Especially if we consider that the balance between excessive collateral damage and military advantage, is very thin and extremely subjective."). The proportionality analysis for a cyber-attack has the potential to be much more complicated that the proportionality analysis to be done for a traditional kinetic attack. *See* Jensen, *Unexpected Consequences*, *supra* note 96, at 1158-59 ("When using kinetic weapons, determining, at least in the short term, what injury and damage will occur can be much clearer. This may not be so clear in relation to CNA.").

[104] *See* TALLINN MANUAL 2.0, *supra* note 29, at 445.

[105] *Id.*

[106] *Id.* at 446.

[107] *Id.*

examples, it does not go far enough in its discussion of how to treat dual-use objects. It still leaves the military commander with a very difficult proportionality assessment to make. How is the commander to determine what the knock-on effects[108] of a cyber-attack will be? How can the expected damage to be caused be estimated, especially when the commander may not have extensive experience in the cyber context, or have extensive examples of cyber-attacks and their potential destruction to draw on?

### *5.1.3. A More Explicit Regulation of Targeting and an Updated Proportionality Standard*

A more explicit regulation is needed for the proportionality analysis to be undertaken in the event of an attack on a dual-use objective, a regulation that takes away some of the uncertainty and human error inherent in the proportionality analysis.[109] This proportionality analysis must explicitly direct the commander to take into account both direct effects of the attack, as well as knock-on effects that could possibly occur.[110]

In allowing the standard to be inclusive of knock-on effects in an age of cyberwarfare, where the effects may be more difficult to predict, the wording of the proportionality principle must also be changed so that it limits an attack which *risks causing* collateral damage, rather than its current regulation against an attack which

[108] Knock-on effects refer to secondary or indirect effects.

[109] *See* Gabriella Blum, *On a Differential Law of War*, 52 HARV. INT'L L.J. 163 (2011) ("For critics and defenders alike, it is evident that the application of the principle of proportionality is highly contingent on interpretation, context, and ultimately, the development of a sub-codex of rules for particular circumstances.").

[110] The inclusion of indirect effects is discussed and adopted in the Tallinn Manual, but the calculation of how they should work alongside direct effects, or how a military commander should calculate them is not discussed. TALLINN MANUAL 2.0, *supra* note 29, at 472. In discussing precautions a commander must take to reduce collateral damage, the Tallinn manual states that, "the issue of indirect effects is central to cyber operations because of the interconnectivity of cyber infrastructure, particularly between military and civilian systems." *Id.* at 480.

"may be expected" to cause collateral damage.[111] In this way it will be more inclusive of harder to predict knock-on effects, and will direct a commander to more deeply examine the wide range of potential knock-on effects that could be present in the event of a cyber-attack.

A commander must also be able to properly differentiate between different types of knock-on effects and weigh them accordingly based on the likelihood of occurrence. Collateral damage that is directly expected as a result of a cyber-attack should be evaluated differently than knock-on effects which are fairly unlikely to occur, but which could potentially occur. In accordance with this comparison, knock-on effects should be classified into three different categories: (1) knock-on effects likely to occur, (2) knock-on effects that could reasonably occur, and (3) knock-on effects which could potentially occur. These should be differentiated from direct effects and collateral damage anticipated. The greatest weight in the proportionality equation, after direct effects and collateral damage anticipated, should be given to those knock-on effects which are likely to occur, followed by knock-on effects that could reasonably occur, and then lastly knock-on effects which could potentially occur. Each commander must be forced to do the proper assessment taking into account each of these categories before an attack can be ordered.

The collateral damage and potential harm to civilians (the combination of the direct effects and the various categories of knock-on effects) must then be weighed against the concrete and direct military advantage expected. Unlike the calculation of potential collateral damage, which must include collateral damage that may potentially occur but might be unlikely to occur, the calculation of military advantage should be based only on a concrete and direct advantage anticipated. It should not take into

[111] The "risks causing" standard was contemplated by several states in drafting Additional Protocol I. *See* ICRC COMMENTARY ON PROTOCOL I, *supra* note 84, at 2209 ("Some would have preferred the words 'which risks causing' rather than 'which may be expected to cause'."). The new proportionality principle, as expressed in Article 51(5)(b) would then be a prohibition on "an attack which risks causing 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." *See id.*; Additional Protocol I, *supra* note 14, art. 51(5)(b).

account potential advantages that could possibly be gained but that are unlikely.

Therefore, the specific proportionality analysis to be done in the context of an attack on a dual-use object in cyberwarfare, would be a balancing on one side of direct effects, likely knock-on effects, reasonably possible knock-on effects, and potential knock-on effects, against direct and concrete military advantage. For example, the equation could be expressed as: $concrete\ and\ direct\ advantage\ anticipated = 4 * (direct\ collateral\ damage\ anticipated) + 3 * (knock\ on\ effects\ likely\ to\ occur) + 2 * (knock\ on\ effects\ that\ could\ reasonably\ occur) + (knock\ on\ effects\ that\ could\ potentially\ occur)$. The estimate of direct collateral damage would be multiplied by four, the knock-on effects likely to occur would be multiplied by three, the knock-on effects that could reasonably occur would be multiplied by two, and finally the knock-on effects that could potentially occur would be multiplied by one. This would demonstrate the relative importance of each category. These figures would then be added together. If the left side of the equation outweighs the right side of the equation, the attack would be permissible since the concrete and direct advantaged anticipated would be greater than the potential collateral damage. If the right side of the equation outweighs the left side of the equation, the attack would be rendered impermissible.

Consider, for example, a cyber-attack on the computers of air traffic control center A in an effort to take down a specific airplane.[112] The concrete and direct advantage anticipated would be causing the specific airplane that has been identified as a military object (perhaps it is carrying weapons or enemy soldiers) to crash. The direct collateral damage anticipated might be whatever damage the airplane would cause when it crashes. The knock-on effects likely to occur might be damage caused to other airplanes that are controlled by the same air traffic control center. Knock-on effects that could reasonably occur would be damage to

[112] A cyber-attack on an air traffic control center is certainly not a far-flung hypothetical. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-221, INFORMATION SECURITY: FAA NEEDS TO ADDRESS WEAKNESSES IN AIR TRAFFIC CONTROL SYSTEMS (2015).

airplanes controlled by other air traffic control centers, but which might be affected by the airplanes controlled by air traffic control center A. Knock-on effects that could potentially occur, would be those effects generally resulting from decreased use and efficiency of the airspace in the region of control center A. The commander would then weigh and compare the direct and concrete military advantage obtainable through the attack, against the direct collateral damage and knock-on effects. The same exercise could be done for a cyber-attack that doesn't cause any direct physical damage, but only causes physical damage as a knock-on effect.

For a less hypothetical example, it is useful to consider the Stuxnet virus.[113] Recall that Stuxnet was a joint American/Israeli project, created in an effort to disrupt the Iranian nuclear program. While many would declare Stuxnet a success—in that by many estimates it set the Iranian nuclear program back by one and half to two years—it did have unintended consequences and eventually led to the infection of over 100,000 computers worldwide. Looking at the new, more explicit proportionality equation stated above, the left side of the equation would consist of the concrete and direct advantage anticipated. This would be the disruption of the Iranian nuclear program. The right side of the equation would consist of the various levels of potential knock-on effects, as well as the direct collateral damage anticipated. The damage to the facility would fall into the category of direct collateral damage anticipated. However, In the case of the Stuxnet, the knock-on effects reached a very wide and dispersed audience, due to an engineer who took his computer home with him and then ended up infecting over 100,000 computers worldwide. It seems likely that the virus might spread to other computers in Iran, which it did at a high rate. The infections in Iran would fall into the category of knock-on effects likely to occur. Yet it seems much less likely that the virus would spread to computers in Bahrain, Ecuador, and Singapore—which it also did. These infections would fall into the category of knock-on effects that could potentially occur. If the commanders who ordered the Stuxnet attack had followed the updated, more explicit proportionality test proposed by this Comment, they would have had to take into account the wide range of collateral damage and

[113] *See supra* Section 3.4.

knock-on effects that the attack risked causing, weighted them properly, and then balanced them against the concrete and direct advantage anticipated. If the direct and concrete advantage anticipated outweighed the direct collateral damage and the knock-on effects, the attack would be permissible. If not, the attack would be impermissible.

The practical result that this updated proportionality principle should have is to diminish the number of cyber-attacks that can be taken against dual-use objects, as well as to require that a commander do an extremely thorough analysis before ordering an attack. The updated proportionality standard will have a higher likelihood of resulting in no attack being ordered. The detailed equation and categorization should force commanders to consider all potential damage and require them to be especially diligent in accounting for knock-on effects, which are very prevalent in the cyber context.

There are two related counter arguments to the updated proportionality principle as I have expressed it. The first would be that commanders are neither skilled enough nor tech-savvy enough to accurately give numerical weight to the different types of knock-on effects. One solution to this problem would be, as will be discussed further in Section 5.2, to mandate that every cyber-attack be approved by a panel made up of (1) a lawyer, (2) a military commander, and (3) a cyber expert. Another possibility would be to mandate the creation of a detailed manual, expressing what weight should be given to different potential knock-on effects. The manual would give extensive examples of cyber-attacks and the effects they could create. It would be written by a group of international experts, similar to the group that wrote the Tallinn Manual. In order to effectively balance the proportionality equation, the commander would only have to insert the types of relevant effects and their weights. The second counter argument would be that due to the difficulty of cyber-attacks passing the proportionality threshold, commanders would revert to ordering traditional kinetic attacks at a higher rate. There are two responses to this counterargument. First, if the commander has succeeded in accurately balancing both sides of the proportionality equation, and the cyber-attack doesn't pass, he should not order the cyber-attack. This does not mean that he can immediately order a kinetic attack. The kinetic attack will have to pass the proportionality analysis as well. If, however, the cyber-attack doesn't pass the proportionality assessment because the commander is unsure of how to weigh each effect, and he therefore chooses to resort to a more familiar kinetic attack, this is the type of problem the panel and the detailed manual are intended to solve. If a commander can rely on the manual to appropriately weigh direct effects and knock-on effects, he should be expected to reach an answer regarding whether the objective can be targeted by performing the proportionality analysis.

### *5.2. Taking Precautions When Attacking a Target: Correcting the Imbalance*

The current precautions that commanders must take before launching a cyber-attack, as well as the ongoing precautions they must take during the course of an attack, are unfit for modern cyberwarfare and have the potential to hold more technologically-advanced states—or states who invest heavily in military technology—to an unfairly high standard when compared to states that are less technologically-advanced or choose not to invest in cyber capabilities. While this is problematic even in traditional kinetic warfare,[114] the damage it causes is exacerbated in the much more technologically-advanced cyber context. The current regulations also give too much decision-making power to military commanders who may or may not be technologically proficient or have a sufficient understanding of cyber weapons or cyberwarfare. The relevant legal structure must be revised to hold all nations to a minimum standard of conduct, as well as to ensure that commanders and decision makers have the qualifications and information necessary to make important decisions in the cyber context.

[114] For an in-depth discussion of Common but Differentiated Responsibilities (CDRs) in a non-cyber context, *see* Blum, *supra* note 109. Blum specifically discusses both the compliance with the proportionality principle, as well as precautions to be taken before launching an attack and during the course of the attack, as examples of standards that could be interpreted as putting unequal weight on different actors. Blum also analogizes to International Environmental Law and International Trade law as areas where differential standards are becoming widely accepted.

### *5.2.1. A Problematically Differentiated Standard*

Article 57 of Additional Protocol I to the Geneva Conventions mandates certain precautions that commanders must take both before ordering an attack, as well as during the course of an attack. Those who plan or decide upon an attack (presumably military commanders) must do everything *feasible* to verify that an objective is military and not civilian and take all *feasible* precautions regarding the means and methods of attack to minimize collateral damage. Additionally, they must cancel an attack that is already underway if they realize that they are attacking a civilian objective or if they believe that the attack will fail the proportionality test.[115]

[115] Additional Protocol I, *supra* note 14, art. 57(2)(a)(i–iii). Different states have unique definitions for how the word "feasible" should be interpreted. Canada's Use of Force Manual states that, "'Feasible' is understood as that which is practicable or practicably possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations. Planners and commanders are expected to act reasonably and in good faith. Decisions concerning the use of force shall be reached on the basis of an assessment of the information reasonably available at the relevant time and that such decisions cannot be judged on the basis of information which has subsequently come to light. Reasonable, good faith efforts must be made to gather intelligence and to review the available intelligence. This standard is one of 'reasonableness', not 'perfection'. The test for determining whether the required standard of care has been met is an objective one: 'Did the commander, planner or staff officer do what a reasonable person would have done in the circumstances?'" DEP'T OF NAT. DEFENCE (CAN.), CHIEF OF THE DEFENCE STAFF, B-GJ-005-501/FP-001, USE OF FORCE FOR CF OPERATIONS §112.6 (2008). Australia's Defence Force Manual defines feasible as "precautions which are practicable or practically possible taking into account all circumstances ruling at the time, including humanitarian and military considerations." AUSTL. DEFENCE FORCE, OPERATIONS SERIES, ADFP 37, MANUAL ON LAW OF ARMED CONFLICT (1994). Leading up to the signing Additional Protocol I, the United Kingdom stated that, "the word 'feasible' means that which is practicable or practically possible, taking into account all circumstances at the time including those relevant to the success of military operations." United Kingdom, Reservations and declarations made upon ratification of the 1977 Additional Protocol I, 28 Jan. 1998. The commentary to Additional Protocol I states that the UK's definition is too broad by including considerations "relevant to the success of military operations," but it stated that the "interpretation will be a matter of common sense and good faith." ICRC COMMENTARY ON PROTOCOL I, *supra* note 84, at 681–82. The United Kingdom eventually conceded to the adoption of the ICRC's standard. In the Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, the feasibility requirement stated that "A military commander must set up an effective intelligence gathering system to collect and

Finally, they are required to take feasible precautions in choosing a means and method of attack to minimize collateral damage. The feasibility requirement of Article 57 requires commanders to display a certain specified conduct rather than achieve a particular result.[116] Based on the information at their disposal, they must do everything feasible to verify the status of an object, decide on the means of attack, and ensure that the attack is lawful while it is occurring, as well as that circumstances haven't changed which would necessitate canceling the attack.[117] The information available to a commander in making these decisions is dependent upon the technology and information-gathering capabilities he is provided with.[118] Presumably, the more information available to a commander, and the better quality the information is, the better he can comply with his legal obligations. Since Article 57 is conduct-

evaluate information concerning potential targets. The commander must also direct his forces to use available technical means to properly identify targets during operations." ICTY, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia* para. 29.

[116] The reliance on a conduct standard is in stark contrast to "[m]any IHL norms [which] are articulated in absolute terms: the intentional killing of civilians is always a war crime, the use of chemical and biological weapons is absolutely prohibited, the torture of prisoners of war or civilians is never lawful, and the carrying out of attacks while posing as a civilian is illegal perfidy." Blum, *supra* note 109, at 186.

[117] In today's interconnected world, an unprecedented amount of information is available, and this information can be "gathered, assessed and disseminated remotely at a very fast rate." Kimberly Trapp, *Great Resources Mean Great Responsibility: A Framework of Analysis for Assessing Compliance with API Obligations in the Information Age*, *in* INTERNATIONAL HUMANITARIAN LAW AND THE CHANGING TECHNOLOGY OF WAR 153, 154 (Dan Saxon ed., 2013).

[118] *Id.* at 164; *see* Jen-Francois Queguiner, *Precautions Under the Law Governing the Conduct of Hostilities*, 88 INT'L REV. RED CROSS 793, 797 (2006), https://www.icrc.org/en/doc/assets/files/other/irrc_864_queguiner.pdf [https://perma.cc/RZR9-5NZN] ("The obligation to verify the nature of the objective to be attacked obviously requires that close attention be paid to the gathering, assessment and rapid circulation of information on potential targets. These activities are naturally dependent on the availability and quality of the belligerents' technical resources."); *see also* Beard, *supra* note 3, at 106 ("To the extent that feasibility relates to making an 'informed decision' in this context, it will focus on what cyber intelligence-gathering operations must or can be conducted in order to make that informed decision.").

based and not result-based,[119] compliance with Article 57 is determined based on the process followed and not the result achieved. Presumably, a commander who took all feasible precautions before launching a cyber-attack would not be found to be in violation of Article 57, even if the attack ended up causing tremendous collateral damage.[120] On the other hand, a commander who caused very little collateral damage, but did not take all feasible precautions could be found to have violated Article 57. Similarly, since it is widely agreed upon that cyber weapons have the ability to be more precise than traditional kinetic weapons and therefore cause less collateral damage[121]—and Article 57 calls on commanders to use the means and methods of attack which will cause the least collateral damage—it would seem that once a country developed a precise, technologically-advanced cyber weapon, it would be limited to using this weapon over other kinetic weapons which might be less precise and cause more collateral damage.[122]

[119] *See also* Trapp, *supra* note 117, at 155 ("The distinction between obligations of conduct and obligations of result is derived from the Civil Law tradition and turns on an analysis of whether the primary rule requires absolutely that State conduct produce a certain result (obligation of result), or whether it requires only that a State make certain efforts to produce a desired, but uncertain, result (obligation of conduct).").

[120] *See generally* Queguiner, *supra* note 118, at 810 ("The basic challenge raised by the expression 'feasible' is in determining whether, and to what extent, it can be interpreted as legitimizing mistakes. For example, information sought and gathered in good faith may lead a party to believe that an object is a military objective, while in fact it is entirely civilian in nature.").

[121] *See* DINNISS, *supra* note 2, at 183; Jensen, *Unexpected Consequences*, *supra* note 96, at 1168 (2003) ("CNA [Computer Network Attack] provides a relatively bloodless means of attack compared to traditional means of force.")

[122] *See* Jensen, *Unexpected Consequences*, *supra* note 96, at 1169 (2003) ("Once the commander has shown the capability to limit the use of kinetic force by advanced weapons technology, some will say that he is now required under humanitarian law to exercise that option in every case."); Queguiner, *supra* note 118, at 802 ("It has also been argued that imposing an obligation to use the most precise weaponry possible would have the perverse effect of slowing the development of sophisticated and expensive weapon systems. By avoiding the development of advanced systems, a party could lawfully use weapons that are less precise and much cheaper, thereby lowering its precision standards when applying the proportionality principle."); Eric Jaworski, *"Military Necessity" and "Civilian Immunity": Where is the Balance?*, 2 CHINESE J. INT'L L. 175, 201 ("A strong requirement of using the best possible technology may actually create a world where some nations are held to a higher standard of care regarding the rule of

Based on the current structure of Article 57, a state with significant intelligence-gathering capabilities and advanced technology in the cyber realm will be held to a much higher result standard than a country will lesser capabilities.[123] A state that invests billions of dollars in technologically-advanced intelligence gathering capabilities, and other cyber capabilities, will be expected to use those resources to ensure that their actions are lawful and minimize collateral damage, while a state who chooses not to make these investments will be held to a much lower standard and will be given more leeway to launch attacks that don't completely verify that the target is a military objective and that collateral damage will be minimized, or to launch attacks using a means or method that causes more extensive collateral damage.[124] The conduct expected of a commander in a technologically-advanced state necessary to comply with Article 57 will be much higher than the conduct expected from a commander in a less technologically-advanced state.[125] This seems to

proportionality than others based solely on the higher level of technology at their disposal."); DINNISS, *supra* note 2, at 213 ("Ironically, the requirement for an attacker to take all feasible precautions in the choice of means and methods of warfare may require that states that have the ability to launch computer network attacks to use that ability in preference to more traditional means.").

[123] 6 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS 228 (1977) ("[Article 57] will apply in accordance with the limits of capability, practical possibility and feasibility of each Party to the conflict."). Gabriella Blum discusses this problem in a non-cyber context saying, "[c]apabilities raise expectations: the greater intelligence and precision capabilities a military possesses, the greater expectation that it will use them to avoid civilian harm." Blum, *supra* note 109, at 194.

[124] Trapp, *supra* note 117, at 166 ("The less technologically advanced a State Party to an armed conflict, the more discretion military commanders will have in deploying particular resources to gather relevant precautionary measure information."). The commentary to Additional Protocol I noted that a Party with technological capabilities must use them, stating that "it is reprehensible for a Party possessing such means not to use them." ICRC COMMENTARY ON PROTOCOL I, *supra* note 84, at 600. Discussing this asymmetry, the commentary notes, "one delegation remarked that the identification of objectives depended to a large extent on the technical means of detection available to the belligerents. This remark seems to be correct. For example, some belligerents might have information owing to a modern reconnaissance device, while other belligerents might not have this type of equipment." *Id.* at 682.

[125] This would apply to various provisions of Article 57. Presumably a commander in a more technologically-advanced nation would have better access

incentivize a race to the bottom, and disincentivize technological advancement. A party who chooses not to invest in developing technological capabilities would not be shackled and constricted in the same manner as a party that does not. We should avoid "disincentivizing" states from developing cyber capabilities in this manner.

### *5.2.2. Attempts by the Tallinn Manual Experts to Regulate Necessary Precautions*

The Tallinn Manual discusses the application of Article 57 in the cyber context, although it does not discuss the potential race to the bottom or the inequality between technologically-advanced states and less technologically-advanced states. The experts break Article 57 into a number of different rules including: (1) Rule 114: Constant Care,[126] (2) Rule 115: Verification of Targets,[127] (3) Rule 116: Choice of Means or Methods,[128] (4) Rule 117: Precautions as to Proportionality,[129] (5) Rule 118: Choice of Targets,[130] (6) Rule 119:

to information to help him determine from the outset whether an object is a military objective, he will have more precise means of attack to help him minimize collateral damage, and he will have better access to incoming information as the attack develops which will help him decide whether to cancel or suspend the attack if he realizes it will not pass the proportionality analysis.

[126] TALLINN MANUAL 2.0, *supra* note 29, at 476 ("During hostilities involving cyber operations, constant care shall be taken to spare the civilian population, individual civilians, and civilian objects.").

[127] *Id.* at 478 ("Those who plan or decide upon a cyber-attack shall do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection.").

[128] *Id.* at 479–80 ("Those who plan or decide upon a cyber-attack shall take all feasible precautions in the choice of means or methods of warfare employed in such an attack, with a view to avoiding, and in any event to minimizing, incidental injury to civilians, loss of civilian life, and damage to or destruction of civilian objects.").

[129] *Id.* at 481 ("Those who plan or decide upon attacks shall refrain from deciding to launch any cyber-attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.").

[130] *Id.* at 481 ("For States Parties to Additional Protocol I, when a choice is possible between several military objectives for obtaining a similar military

Cancellation or Suspension of Attack,[131] (7) Rule 120: Warnings,[132] and (8) Rule 121: Precautions Against the Effects of Cyber Attacks.[133] Importantly, the Tallinn Manual discusses the word "feasible" in the cyber context as "that which is practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations."[134] The Tallinn Manual also lists examples of what taking feasible precautions might look like in the cyber context.[135] Importantly, the Tallinn Manual states that "there is no obligation to take measures that are not feasible."[136]

### *5.2.3. Revising Article 57 and Necessary Precautions*

There are a few ways that this problem of misaligned incentives and the potential race to the bottom that is created by

advantage, the objective to be selected for cyber-attack shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects."). The experts involved in writing the Tallinn Manual could not come to a consensus as to whether this rule (which is based on Article 57(3) of Additional Protocol I), had become part of customary international law and therefore applies to states who are not party to Additional Protocol I. A majority of the experts thought that it had become customary international law. *Id.* at 482.

[131] TALLINN MANUAL 2.0, *supra* note 29, at 483 ("Those who plan, approve, or execute a cyber-attack shall cancel or suspend the attack if it becomes apparent that: (a) the objective is not a military one or is subject to special protection; or (b) the attack may be expected to cause, directly or indirectly, incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof that would be excessive in relation to the concrete and direct military advantage anticipated.").

[132] *Id.* at 484 ("effective advance warning shall be given of cyber-attacks that may affect the civilian population unless circumstances do not permit.").

[133] *Id.* at 487 ("The parties to an armed conflict shall, to the maximum extent feasible, take necessary precautions to protect the civilian population, individual civilians, and civilian objects under their control against the dangers resulting from cyber-attacks.").

[134] *Id.* at 479 (quoting the Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as Amended on 3 May 1996).

[135] *Id.* (examples include "gathering intelligence on the networks through mapping or other processes in order to allow those responsible reasonably to determine the attacks likely effects, particularly on the civilian population or civilian objects.").

[136] *Id.*

Article 57, could be solved. First, Article 57 could be revised to institute a minimum standard of care that every commander must abide by when taking precautions before launching an attack and during an attack. This would ensure that states investing in technology and cyber capabilities are not punished for their decision to invest as all states would be held to a higher standard. It might also serve to encourage less technologically-advanced states to invest in cyber capabilities. One way to institute this minimum standard would be to introduce a detailed check list of specific tasks that need to be completed by a commander before an attack is launched and in order to monitor an attack while it is occurring. This list of specific tasks would be the same for all states, regardless of their level of technological advancement.

A second solution would be to replace the word "feasible" with a stronger adjective that would not be dependent upon the resources of the specific country. Perhaps, mandating that a commander take all "necessary" precautions in the choice of means and methods of attack and do everything "necessary" to verify that objectives to be attacked are military and not civilian, would take the subjectivity out of the standard.[137] It is important to note that "necessary" was the specific adjective used in the International Criminal Tribunal for the former Yugoslavia case of *Prosecutor v. Tadic*.[138]

Finally, changing the standard from a conduct-based standard to a results-based standard would help prevent the disincentivizing of technological advancement.[139] If the

[137] The relevant portions of Article 57 would then read that (1) a commander must do everything *necessary* to verify that the objectives to be attacked are neither civilians nor civilian objects and (2) that commanders must take all *necessary* precautions in the choice of means and methods of attack.

[138] "In the conduct of military operations . . . all necessary precautions should be taken to avoid injury, loss or damage to civilian populations." Prosecutor v. Tadic, Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 111 (Int'l Crim. Trib. For the Former Yugoslavia Oct. 2, 1995), http://www.icty.org/x/cases/tadic/acdec/en/51002.htm [https://perma.cc/65T9-K3NJ].

[139] A move to a result-based test would more closely mirror the rest of international humanitarian law. *See* Blum, *supra* note 109, at 165 ("Some exceptions notwithstanding, IHL obligations bind all parties equally, regardless of

"feasibility" requirement was replaced by a specific result requirement (perhaps mirroring the proportionality requirement, stating that precautions must be taken to ensure that collateral damage is not excessive in relation to the concrete and direct military advantage anticipated), states would not be held to a lower standard for not developing cyber capabilities.

### *5.2.4. Ensuring Capable Decision Makers*

In addition to updating Article 57 to remove the potential race-to-the-bottom problem, Article 57 must be revised to require states to ensure that the people tasked with making decisions and carrying out attacks are, pursuant to Article 57, capable of making decisions relevant to a cyberwarfare scenario. Commanders making decisions regarding Article 57 precautions are held to a standard of reasonableness regarding their assessment of the targetable status of an object and whether or not an attack will pass the proportionality requirement.[140] Reasonableness is an overbroad standard that must be defined more specifically.

One way to remedy this deficiency would be to mandate that the "reasonable" commander or decision maker have familiarity with technology and cyberwar capabilities and problems. Commanders who are trained in kinetic warfare and have extensive knowledge and experience in kinetic warfare aren't necessarily equipped to order and evaluate more technologically-advanced cyber-attacks. Commanders who have less cyber knowledge and experience should be required to consult more closely with advisors and reports that can help inform them and fill the information gap.

A second way to ensure that commanders are able to make intelligent and legal targeting decisions would be to require every cyber-attack to be approved by a panel comprised of a lawyer, a cyber expert, and a military commander. This would ensure that the attack is approved by people with sufficient knowledge and

the type of way they fight, the justness of their respective causes, or the disparities in power and capabilities between them.").

[140] *See* Trapp, *supra* note 117, at 164.

expertise to determine that the necessary precautions have been taken and that the attack will be legal.

## 6. CONCLUSION

Modern warfare is rapidly becoming more technologically-advanced and cyber-attacks are becoming the norm, rather than the exception. Dozens of countries have developed cyber capabilities, and many states have begun to heavily invest in cyber weapons and cyber defense. Although many scholars argue that an entirely new system of international humanitarian law is needed to effectively regulate cyberwarfare, it is this Comment's belief that an updated version of the current international law, namely Additional Protocol I, is sufficient. The Tallinn Manual has made a good start, but it has not gone far enough. Specifically, in the law of targeting, two important updates must be made.

First, the law of targeting must be updated to take into account the targeting of dual-use objectives. While dual-use objectives are present in traditional kinetic warfare, they are far more prevalent in cyberwarfare, and the civilian and military parts of the objective are more difficult to separate. In order to effectively regulate the targeting of dual-use objectives, the traditional proportionality principle, found in Article 51(5)(b) of Additional Protocol I must be updated. It must first expand its ability to include hard-to-predict knock-on effects by substituting the "expected to cause" standard with a "risk of causing" standard. The new standard would then prohibit "an attack which *may risk* causing 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." In addition to this change, an explicit equation must be added to the proportionality principle which requires commanders to take into account and properly weigh not only direct collateral damage, but also likely knock-on effects, reasonably possible knock-on effects, and potential knock-on effects. These must then be weighed against the direct and concrete military advantage that an attack would produce. In making this assessment, the commander would be required to consult with a panel which would include himself, a lawyer, and a cyber expert.

Second, the precautions a commander must take before ordering an attack, after an attack has begun, and in choosing the means and method of attack, must be updated. The current standard risks penalizing states for technological innovation, for developing more precise cyber weapons, and for developing enhanced intelligence gathering means to determine whether an objective is military or civilian. There are a few possible ways to revise this standard. First, Article 57 could be revised to institute a minimum standard of care that commanders must meet when taking precautions for an attack. This minimum standard would be the same for all states. Second, the word "feasible" in Article 57 could be replaced with the word "necessary" — revising the relevant standard so that commanders must "do everything *necessary* to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives" and "take all *necessary* 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." Finally, the precautions standard could be improved by changing it from a conduct standard to a result standard and mandating a specific result.

Overall, the result of these revisions would be to update international humanitarian law to specifically take into account the interconnectedness of cyberspace and the dangers posed by a world of military commanders inexperienced in cyberwarfare.