Protecting Critical Infrastructure in Cyber Warfare: Is It Time for States to Reassert Themselves?

David A. Wallace[†*] *and Shane R. Reeves*[**]

When Russia uses a "combination of instruments, some military and some non-military, choreographed to surprise, confuse, and wear down" Ukraine, it is termed hybrid warfare.[1] *The term also refers to conflicts, which are both international and non-international in character, such as the ongoing conflict in Syria.*[2] *Overlapping conventional and asymmetric tactics in an armed conflict — as when Russia simultaneously conducted cyber-attacks during a conventional invasion of Georgia in 2008 — also gets the hybrid warfare label.*[3] *Or, as Professor Bobby Chesney wrote regarding U.S. operations in Somalia, hybrid warfare can include "a sophisticated approach that layers together a panoply of low-visibility (to*

* Professor & Head, Department of Law, United States Military Academy, West Point.

** Associate Professor & Deputy Head, Department of Law, United States Military Academy, West Point.

1 *See What Russia Wants: From Cold War to Hot War*, ECONOMIST (Feb. 12, 2015), https://www.economist.com/briefing/2015/02/12/from-cold-war-to-hot-war [https://perma.cc/Y89X-49U3].

2 *See generally* David Wallace, Amy McCarthy & Shane R. Reeves, *Trying to Make Sense of the Senseless: Classifying the Syrian War Under the Law of Armed Conflict*, 25 MICH. ST. INT'L L. REV. 555 (2017) (discussing the various elements of conflict in Syria, to include state and non-state factions).

3 *See* Shane R. Reeves & Robert E. Barnsby, *The New Griffin of War: Hybrid International Armed Conflicts*, HARV. INT'L REV., Winter 2013, at 16-17 (discussing the international legal challenges presented by hybrid warfare).

the public both here and there) tools" to conduct counter-terrorism operations in failing states.[4]

In other words, "hybrid warfare" has become a shorthand way to describe the various complexities of the modern battlefield. Hybrid warfare — regardless how the term is used — clearly raises several challenging and important legal issues. Some of these issues include finding a workable approach to enforcing the principle of distinction, properly classifying conflicts, and understanding the roles of the military and law enforcement in contemporary warfare. Yet, perhaps no aspect of hybrid warfare generates more legal questions than operations in cyberspace.

Cyberspace, defined as "a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the internet and telecommunication networks,"[5] *is quickly becoming the decisive battleground in warfare.*[6] *National armed forces, and more specifically technologically advanced militaries, rely upon their information networks for command and control, intelligence, logistics, and weapon technology, making protecting these assets a priority.*[7] *Arguably, however, the greatest vulnerability for an advanced State engaged in an armed conflict is its reliance on the cyber domain to operate the critical infrastructure essential for societal functions.*

The catastrophic results of losing the essential services provided by critical infrastructure are immense and, potentially, could result in a State being incapable of conducting military operations. Recognizing this vulnerability, this Essay therefore critically examines how the law of armed conflict protects such objects and activities. In doing so, the Essay concludes that heightened protections for critical infrastructure from cyber-attacks are necessary and suggests looking to the existing framework of special precautionary protections as a model for greater legal safeguards.

---

[4] Robert Chesney, *American Hybrid Warfare: Somalia as a Case Study in the Real American Way of War in 2016*, LAWFARE (Oct. 17, 2016, 7:06 AM), https://www.lawfareblog.com/american-hybrid-warfare-somalia-case-study-real-american-way-war-2016 [https://perma.cc/YNZ6-496H].

[5] U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010) [hereinafter QUADRENNIAL REPORT].

[6] *See, e.g.*, RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 69 (2010); Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, Winter 2008-2009, at 60 (discussing the desperate actions of the Georgian government after it found itself unable to communicate through the internet during the 2008 Georgian-Russian conflict).

[7] *See* QUADRENNIAL REPORT, *supra* note 5, at 37.

TABLE OF CONTENTS

> "The single biggest existential threat that's out there, I think, is cyber."[8]
>
> —Admiral (ret.) Michael Mullen

INTRODUCTION

As the Chairman of the Joint Chiefs of Staff, Admiral Michael Mullen served as the principal military adviser to Presidents George W. Bush and Barack Obama, and was the senior ranking member of the Armed Forces of the United States.[9] As such, his views on existential threats

[8] Micah Zenko, *The Existential Angst of America's Top Generals*, FOREIGN POL'Y (Aug. 4, 2015, 9:00 AM), https://foreignpolicy.com/2015/08/04/the-existential-angst-of-americas-top-generals-threat-inflation-islamic-state [https://perma.cc/3WC4-B85K].

[9] *See Chairman of the Joint Chiefs of Staff*, JOINT CHIEFS OF STAFF, http://www.jcs.mil/About/The-Joint-Staff/Chairman (last visited Dec. 26, 2019) [https://perma.cc/JR7R-9YD6]. Admiral Mullen became the seventeenth Chairman of the Joint Chiefs of Staff on October 1, 2007. *17th Chairman of the Joint Chiefs of Staff: Admiral Michael Glenn Muller*, JOINT CHIEFS OF STAFF, https://www.jcs.mil/About/The-Joint-Staff/Chairman/Admiral-Michael-Glenn-Mullen/ (last visited Dec. 26, 2019) [https://perma.cc/SUQ7-SE2J].

facing the country are not only relevant and weighty, but also alarming. It is not difficult to understand Admiral Mullen's fears as cyberspace increasingly allows an adversary to exploit, disrupt, deny, and degrade almost all of a State's important military and civilian computer networks and related systems.[10] Most concerning, these cyber vulnerabilities include those that run a State's critical infrastructure — whether it be the electronic grid, commercial or market activities, transportation networks, water and distribution systems, or emergency services. Incapacitating or destroying any of these systems or assets would "have a debilitating impact on security, national economic security, national public health or safety"[11] and adversely affect thousands (perhaps millions) of civilians. Consequently, social unrest and chaos would follow.[12]

The threat of a paralyzing cyber-attack on critical infrastructure is neither theoretical nor academic. It is real. President Obama made this clear in 2013 when he stated:

> Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United

[10] *See* U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 3-4 (2011).

[11] Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739 (Feb. 12, 2013).

[12] *See* Bret Brasso, *Cyber Attacks Against Critical Infrastructure Are No Longer Just Theories*, FIREEYE (Apr. 29, 2016), https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html [https://perma.cc/54HM-CHEN]. Recognizing the consequences associated with cyber-attacks on critical infrastructure, the United Nations Group of Governmental Experts ("UNGGE") on Information Security specifically noted in their 2015 report that "[a] State should not conduct or knowingly support [information and communications technology] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." U.N. Grp. of Governmental Experts, *Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 13(f), U.N. Doc. A/70/174 (July 24, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [https://perma.cc/U5A8-JEWR]. The 2015 UNGGE report contains recommendations developed by governmental experts from twenty States addressing threats from uses of information and communications technologies by States and non-State actors alike and, in doing so, builds upon reports issued in 2010 and 2013. *Id.* at 4. These reports have become a significant focal point for international discussions on the applicability of international law to States with respect to cyberspace and operations. Elaine Korzak, *The 2015 GGE Report: What Next for Norms in Cyberspace?*, LAWFARE (Sept. 23, 2015, 8:32 AM), https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace [https://perma.cc/9RNH-QS2L].

> States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats.[13]

More recently, in describing his concerns about a cyber-attack against critical infrastructure, former National Security Agency Director Admiral Michael Rogers predicted, "[i]t is only a matter of the when, not the if, that we are going to see something traumatic."[14] Unfortunately, State activities in cyberspace have proven these statements true. For example, on December 23, 2015, a cyber-attack shut down Ukraine's relatively secure power grid.[15] More specifically, the Ukrainian Kyivoblenergo, a regional electricity distribution company, suffered severe power outages affecting 225,000 customers due to a malicious malware.[16] Not long after the incident occurred, the Ukrainian government publicly attributed the highly sophisticated cyber intrusion[17] to Russian security services.[18]

While similar events are transpiring regularly,[19] the attack on the Ukrainian critical infrastructure is particularly important as it took place during a period of armed conflict.[20] Undoubtedly, it is relevant

---

[13] Exec. Order No. 13,636, 78 Fed. Reg. at 11,739.

[14] Amelia Smith, *China Could Shut Down U.S. Power Grid with Cyber Attack, Says NSA Chief*, NEWSWEEK (Nov. 21, 2014, 11:07 AM), http://www.newsweek.com/china-could-shut-down-us-power-grid-cyber-attack-says-nsa-chief-286119 [https://perma.cc/Y3XR-N4LV].

[15] *See* Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid [https://perma.cc/54ZC-J35V].

[16] *See* ROBERT M. LEE ET AL., ELEC. INFO. SHARING & ANALYSIS CTR., ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID, at iv (2016), https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [https://perma.cc/Z3FR-LAZU].

[17] *See* Zetter, *supra* note 15.

[18] *See* LEE ET AL., *supra* note 16, at iv.

[19] For example, Russia recently used malicious computer code known as Triton to gain control over a safety shut-off system — considered critical to defending against catastrophic events — at a petrochemical plant in Saudi Arabia. *See* Dustin Volz, *Researchers Link Cyberattack on Saudi Petrochemical Plant to Russia*, WALL ST. J. (Oct. 23, 2018, 3:20 PM), https://www.wsj.com/articles/u-s-researchers-link-cyberattack-on-saudi-petrochemical-plant-to-russia-1540322439 [https://perma.cc/56SV-VQB9]. This intrusion is the first reported breach of a safety system at an industrial plant. *See id.*

[20] Although the precise contours of the armed conflict in the Ukraine are difficult to determine, it appears to be international and non-international armed conflicts occurring in parallel. *See* Shane R. Reeves & David Wallace, *The Combatant Status of the "Little Green Men" and Other Participants in the Ukraine Conflict*, 91 INT'L L. STUD. 361, 372-83 (2015); *see also International Armed Conflict in Ukraine*, RULAC, http://www.rulac.org/browse/conflicts/international-armed-conflict-in-ukraine [https://perma.cc/E3UU-2HMB] (last updated Sept. 12, 2017). As an international armed conflict was occurring at the time of the cyber-attack on the power grid, the law of armed conflict applied. *See id.*

and important to understand how international law regulates interactions between States when one intrudes upon the other's critical infrastructure outside of armed conflict.[21] However, this Essay focuses on the equally important topic of cyber targeting of critical infrastructure during a period of armed conflict — such as the Russian hack of the Ukrainian power grid — and whether the current normative framework of the law of armed conflict provides sufficient protections from such attacks.[22]

Through this analysis, it becomes apparent that existing protections for critical infrastructure in armed conflict are inadequate and heightened legal safeguards are necessary. To support this proposition, the Essay begins with a brief description of critical infrastructure and explains why these systems are vulnerable in cyberspace. A general overview of the law of armed conflict's provisions on targeting follows. The Essay then applies these principles and rules to critical infrastructure in cyberspace to illustrate that the existing law — *lex lata*[23] — does not go far enough in protecting these essential assets. The Essay thus concludes with a *lex ferenda* argument[24] in favor of a new treaty that provides additional protections against cyber-attacks for critical infrastructure during armed conflict.

I. WHAT IS CRITICAL INFRASTRUCTURE? WHY SHOULD WE WORRY?

There is no universal definition of "critical infrastructure." Instead, States subjectively determine the assets, systems, or capabilities that are critical to their national security. In the United States, for example,

[21] For a comprehensive general overview of international law in cyberspace, see generally INT'L GRP. OF EXPERTS, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt et al. eds., 2017) [hereinafter TALLINN MANUAL 2.0].

[22] The law of armed conflict, which is often also called international humanitarian law, is a "set of rules which seek, for humanitarian reasons, *to limit the effects of armed conflict*. It protects persons who are not or are no longer participating in the hostilities and restricts the means and methods of warfare." ADVISORY SERV. ON INT'L HUMANITARIAN LAW, INT'L COMM. OF THE RED CROSS, WHAT IS INTERNATIONAL HUMANITARIAN LAW? (2004), https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf; *see also* U.S. DEP'T OF DEF., DIRECTIVE 2311.01E, ¶ 3.1 (2006), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/231101e.pdf [https://perma.cc/8S47-QPA8] (defining the law of war as the part of international law that regulates the "conduct of armed hostilities" and is often called "the law of armed conflict").

[23] *Lex lata* is defined as "what the law is." J. Jeremy Marsh, Lex Lata *or* Lex Ferenda*? Rule 45 of the ICRC Study on Customary International Humanitarian Law*, 198 MIL. L. REV. 116, 117 (2008).

[24] *Lex ferenda* is defined as "what the law should be." *Id.*

critical infrastructure is defined as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[25] Characterized in a slightly different manner, critical infrastructure are assets or systems vital for the maintenance of essential societal functions[26] and serve as the backbone of a State's economy, security, and health.[27]

Importantly, most of the assets or services essential to a society are interconnected. Damage, destruction, or disruption in one system, therefore, would naturally have significant negative consequences in other important systems necessary for the operation of an advanced State.[28] Recognizing this interconnectedness risk, States increasingly characterize large groupings of assets, systems, or capabilities as "critical infrastructure." By doing so, States are attempting to protect not just a particular asset or service, but rather the entire ecosystem that underlies its national security.[29] For example, the United States Department of Homeland Security — aside from the generic definition provided above — now identifies sixteen critical infrastructure sectors including: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services,

[25] Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c (2019). The statute provides, among other things, "that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States . . . ." *Id.*

[26] *Migration and Home Affairs: Critical Infrastructure*, EUR. COMM'N, https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (last visited Dec. 26, 2019) [https://perma.cc/LF9P-DUEZ].

[27] *See CISA Infrastructure Security: Supporting Policy and Doctrine*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/what-critical-infrastructure (last visited Dec. 26, 2019) [https://perma.cc/K9SQ-8QYU].

[28] *See generally Critical Infrastructure Sectors*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/critical-infrastructure-sectors (last visited Nov. 21, 2018) [https://perma.cc/V55P-KP4T] [hereinafter *Critical Infrastructure Sectors*] (listing sixteen United States critical infrastructure sectors).

[29] In other words, a State is communicating to potential adversaries the importance of these particular assets and, consequently, the severe ramifications if attacked. While what exactly those ramifications may be is outside the scope of this Essay, it is important to note, "[t]he use of force threshold, wherever it may presently lie, will almost certainly drop in lock step with the increasing dependency of states on cyberspace." Michael N. Schmitt, The Law of Cyber Warfare: Quo Vadis?, 25 STAN. L. & POL'Y REV. 269, 281 (2014) [hereinafter *Law of Cyber Warfare*] ("In particular, operations that non-destructively target critical infrastructure may come to be viewed by states as presumptive uses of force.").

energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear, transportation systems, and water and wastewater systems.[30]

The failure of critical infrastructure, regardless of the reason, is potentially catastrophic. Although an August 2003 blackout was neither cyber-related nor did it occur during an armed conflict, the event's widespread disruption of power over parts of eight U.S. states illustrates the point.[31] On one afternoon in the middle of August, a power line in northern Ohio, softened by the heat of summer, brushed against some trees and triggered an automatic shutdown of the power line. Over the next few hours, as technicians tried to understand the nature and scope of the problem, three other power lines sagged into trees causing additional shutdowns.[32] Eventually, the entire electrical system was overtaxed.[33] Approximately 50 million people lost power, eleven individuals died, and economic damages escalated into the billions.[34] Additionally, the power outage stranded thousands of commuters, disrupted air traffic across the United States, flooded hospitals with patients complaining of heat injuries, and required mandatory evacuations of buildings, tunnels, and other public areas.[35]

As the 2003 blackout shows, critical infrastructure is interconnected and interdependent — an outwardly insignificant incident in northern Ohio triggered not only the massive loss of electrical power in one town, but severely disrupted power systems throughout the United States. Yet, vulnerabilities in systems as important as the electric "grid" continue to exist and are numerous and obvious. The entire system consists of miles of high-voltage and low-voltage power lines, distribution transformers,

---

[30] *See* U.S. DEP'T OF HOMELAND SEC., *Critical Infrastructure Sectors*, *supra* note 28.

[31] *See* James Barron, *The Blackout of 2003: The Overview; Power Surge Blacks Out Northeast, Hitting Cities in 8 States and Canada; Midday Shutdowns Disrupt Millions*, N.Y. TIMES (Aug. 15, 2003), https://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html [https://perma.cc/ZHX4-KJNC]. The blackout affected the U.S. states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, and New Jersey, and the Canadian province of Ontario. *See id.*

[32] *See* JR Minkel, *The 2003 Northeast Blackout — Five Years Later*, SCI. AM. (Aug. 13, 2008), https://www.scientificamerican.com/article/2003-blackout-five-years-later [https://perma.cc/M72K-SSTN].

[33] *See id.* An April 2004 report on the incident found that systemic problems with the grid, and the cascading nature of the event, caused the blackout. *See generally* U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS (2004).

[34] *See* Minkel, *supra* note 32. Estimates of the damage from the blackout were estimated at $6 billion. *See id.*

[35] *See* Barron, *supra* note 31.

and connections between thousands of power plants to hundreds of millions of electricity customers.[36] What becomes apparent is that any damage, disruption, or even delay along the electricity grid continuum is potentially devastating and could have a cascading negative effect on the economic and security well-being of an affected State.

The United States became acutely aware of such risks to critical infrastructure following the terrorist attacks of September 11, 2001. In February 2003, the United States government released *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* in an effort to reduce America's vulnerabilities to acts of terrorism.[37] The report observed that the facilities, systems, and functions that comprise an advanced society's critical infrastructure are highly sophisticated and complex.[38] Additionally, the report found that "our most critical infrastructures typically interconnect and, therefore, depend on the continued availability and operation of other dynamic systems and functions."[39] E-commerce, for example, depends on electricity (as well as information and technology), and protecting and maintaining these ancillary systems is a necessity for internet trade.[40] The report thus concludes: "[g]iven the dynamic nature of these interdependent infrastructures and the extent to which our daily lives rely on them, a successful terrorist attack to disrupt or destroy them could have tremendous impact beyond the immediate target and continue to reverberate long after the immediate damage is done."[41]

The report's logic applies equally to a cyber-attack against critical infrastructure, and its warning about the potential for such an incident is ever more prescient. For example, in 2013, an Iranian hacker named Hamid Firoozi — most likely working on behalf of the Iranian government[42] — gained remote access to the Bowman Avenue Dam in

---

[36] *See Electricity Explained: How Electricity Is Delivered to Consumers*, U.S. ENERGY INFO. ADMIN., https://www.eia.gov/Energyexplained/index.cfm?page=electricity_delivery (last updated Oct. 11, 2019) [https://perma.cc/T6JS-K9KE].

[37] *See* U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS (2003), https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf [https://perma.cc/G62A-MY6W].

[38] *See id.* at 6.

[39] *Id.*

[40] *See id.* (noting that, similarly, transportation and distribution systems are necessary to assure the delivery of fuel to generate power).

[41] *Id.* at 7.

[42] *See* Sealed Indictment at 1-2, United States of America v. Ahmad Fathi et al., No. 16CR00048, 2016 WL 1291521 (S.D.N.Y. Jan. 21, 2016) [hereinafter Sealed Indictment].

Rye Brook, New York (fifteen miles north of New York City).[43] Access to the dam gave Firoozi the ability to remotely operate and manipulate the sluice gate, which is responsible for controlling water levels and flow rates.[44] Fortunately, the dam operators had manually disconnected the sluice gate for maintenance prior to the hack.[45] While Firoozi seemingly failed, he may have in fact been extremely successful, as he was likely conducting "a dry run for a more disruptive invasion of, say, a major hydroelectric generator or some other grand and indispensable element of the nation's power grid."[46]

The strategic importance of critical infrastructure coupled with the numerous vulnerabilities found within these assets and systems make cyber-attacks increasingly attractive to potential adversaries of any advanced State. This is especially true during a period of armed conflict. The United States, in its Department of Defense 2015 Cyber Strategy, recognizes this fact by noting "[d]uring a conflict, the Defense Department assumes that a potential adversary will seek to target U.S. or allied critical infrastructure and military networks to gain a strategic advantage."[47] The report goes on to assume that all critical

[43] *See* Tom Ball, *Top 5 Critical Infrastructure Cyber Attacks*, COMPUTER BUS. REV. (July 18, 2017), https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks [https://perma.cc/HT9N-ZMAQ].

[44] *See* Sealed Indictment, *supra* note 42, at 14-15.

[45] *See id.* at 15.

[46] Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*, N.Y. TIMES (Mar. 25, 2016), https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html [https://perma.cc/9EAC-AXGD]. Since the incident at the Bowman Avenue Dam, cyber intrusions attempting to affect the American water supply have continued with increasing effectiveness. *See, e.g.*, Ari Mahairas & Peter J. Beshar, Opinion, *A Perfect Target for Cybercriminals*, N.Y. TIMES (Nov. 19, 2018), https://www.nytimes.com/2018/11/19/opinion/water-security-vulnerability-hacking.html [https://perma.cc/L7WW-8GZ2] (discussing recent examples of cyber-attacks on water and sewer utilities). The authors assert, "[t]he concept of damaging a society by attacking its water supply is as old as warfare itself. . . . These days, the threat is more pernicious than ever: Destruction and disruption that once required explosives can be achieved with keystrokes." *Id.*

[47] U.S. DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 2 (2015), https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf [hereinafter DOD CYBER STRATEGY]. The Department of Defense released an updated version of the Cyber Strategy document in September of 2018. *See* Mark Pomerleau, *DoD Releases First New Cyber Strategy in Three Years*, FIFTH DOMAIN (Sept. 18, 2018), https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy [https://perma.cc/4QUV-6ED7]. While the updated strategy supersedes the 2015 document, it re-emphasizes the importance of protecting critical infrastructure. *See* U.S. DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 2 (2018), https://media.defense.gov/2018/sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf [https://perma.cc/NZZ5-UL8C]

infrastructure is targetable and gives examples of an adversary attacking "an industrial control system (ICS) on a public utility to affect public safety" or entering "a network to manipulate health records to affect an individual's well-being."[48] The Cyber Strategy concludes that the purpose of any such attack is to undercut the United States' economic and national security — despite the inevitable death and destruction that will ensue — and therefore protecting critical infrastructure is of paramount interest.[49] The following Part discusses how the law currently protects such assets during a period of armed conflict.

II. AN OVERVIEW OF TARGETING UNDER THE LAW OF ARMED CONFLICT

The law of armed conflict regulates the targeting of both persons and objects, regardless of the means or methods used by the parties, in both international and non-international armed conflicts.[50] However, of importance to understanding the extant legal protections for critical infrastructure in armed conflict is the law of targeting[51] as it specifically relates to objects. While there are several law of armed conflict principles and rules applicable to the targeting of objects,[52] underlying each of these individual norms is a compromise between two diametrically opposed impulses: military necessity and humanitarian considerations.[53] Therefore, before delving into the specifics of the law

("[T]he Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident . . . .").

48 DOD CYBER STRATEGY, *supra* note 47, at 2.

49 *See id.*

50 TALLINN MANUAL 2.0, *supra* note 21, at 414.

51 The term "targeting" is broadly understood as using violence against people or objects in the context of an armed conflict. *See* Gary P. Corn et al., *Targeting and the Law of Armed Conflict*, *in* U.S. MILITARY OPERATIONS: LAW, POLICY, AND PRACTICE 167, 172, 173 (Geoffrey S. Corn et al. eds., 2016). The law of targeting is therefore that subset of the law of armed conflict that regulates how that violence is conducted. *See id.* at 172-73 ("[I]t is universally recognized that during *any* armed conflict, the warring parties' discretion to employ violence is not legally unfettered."); *see also* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 126 (1st ed. 2004) (stating that targeting is "the selection of appropriate targets from a list of military objectives — as well as the choice of weapons and ordnance").

52 *See* WILLIAM H. BOOTHBY, THE LAW OF TARGETING 60-64 (2012) [hereinafter LAW OF TARGETING].

53 *See* Kjetil Mujezinovi Larsen et al., *Introduction by the Editors: Is There a 'Principle of Humanity' in International Humanitarian Law?*, *in* SEARCHING FOR A 'PRINCIPLE OF HUMANITY' IN INTERNATIONAL HUMANITARIAN LAW 1, 9 (Kjetil Mujezinovi Larsen et al. eds., 2013).

of targeting, a brief discussion on the military necessity-humanity balance is necessary.[54]

A. The Foundation for the Law of Targeting: Military Necessity Versus Humanity

Military necessity[55] is best understood as a broad "attempt to realize the purpose of armed conflict, gaining military advantage," whereas humanitarian considerations are intent on "minimizing human suffering and physical destruction" in warfare.[56] These two broad, often times called "meta," principles[57] are weighed against each other throughout the entirety of the law of armed conflict with every rule or norm — whether treaty- or custom-based — considering both military necessity and the dictates of humanitarian aims.[58] In other words, "it

[54] *See id.*

[55] Francis Lieber stated, "[m]ilitary necessity, as understood by modern civilized nations, consists in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war." FRANCIS LIEBER, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD: GENERAL ORDERS NO. 100, at art. 14 (1863), *reprinted in* THE LAWS OF ARMED CONFLICTS 3, 6 (Dietrich Schindler & Ji í Toman eds., 3d ed. 1988) [hereinafter LIEBER CODE]. This definition of military necessity has remained mostly intact in current U.S. doctrine. *See, e.g.*, U.S. DEP'T OF THE ARMY, FIELD MANUAL NO. 27-10, THE LAW OF LAND WARFARE at ¶ 3.a (1956), https://www.loc.gov/rr/frd/Military_Law/pdf/law_warfare-1956.pdf [https://perma.cc/74KQ-ELS6] (defining military necessity as "those measures not forbidden by international law which are indispensable for securing the complete submission of the enemy as soon as possible"). The definition has also survived in academic writing. *See, e.g.*, WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 72 (2009) (citing LIEBER CODE, *supra* note 55, at art. 14).

[56] GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 278 (2d ed. 2016).

[57] *See* Brian J. Bill, *The Rendulic 'Rule': Military Necessity, Commander's Knowledge, and Methods of Warfare*, *in* 12 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 119, 131 (2009) ("Military necessity is a meta-principle of the law of war . . . in the sense that it justifies destruction in war. It permeates all subsidiary rules."); *see also* DINSTEIN, *supra* note 51, at 16 (comparing the principles at their extremes).

[58] *See* Christopher Greenwood, *Humanitarian Requirements and Military Necessity*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 35, 37-38 (Dieter Fleck ed., 2d ed. 2008) (discussing generally how the principles of military necessity and humanity check and balance each other throughout the law of armed conflict); Shane R. Reeves & Jeffrey S. Thurnher, *Are We Reaching a Tipping Point? How Contemporary Challenges Are Affecting the Military Necessity-Humanity Balance*, HARV. NAT'L SECURITY J. FEATURES ONLINE (2013), http://harvardnsj.org/2013/06/are-we-reaching-a-tipping-point-how-contemporary-challenges-are-affecting-the-military-necessity-humanity-balance [https://perma.cc/CG27-CSJM] (explaining that humanity and military necessity must be simultaneously considered in the law of armed conflict).

can be stated categorically that no part" of the law of armed conflict "overlooks military requirements, just as no part . . . loses sight of humanitarian considerations."[59]

This equilibrium is not new to the law of armed conflict. The 1868 St. Petersburg Declaration, which is considered the first major international agreement prohibiting the use of a particular weapon,[60] outlined the relationship, and inherent tension, between military necessity and humanity in renouncing the use of explosive projectiles.[61] A similar check and balance which exists in all subsequent law of armed conflict provisions ensures that "force is applied on the battlefield in a manner allowing for the accomplishment of the mission while simultaneously taking appropriate humanitarian considerations into account."[62] Otherwise, "[i]f military necessity were to prevail completely, no limitation of any kind would [be] imposed on the freedom of action of belligerent States. . . . Conversely, if benevolent humanitarianism were the only beacon to guide the path of the armed forces, war would . . . entail[] no bloodshed, no destruction and no human suffering; in short, war would not [be] war."[63]

The law of armed conflict therefore is a series of "prohibitions, restrictions, and obligations designed to balance a State's interest in effectively prosecuting the war (military necessity) with its interest in minimizing harm to those involved in a conflict."[64] With the law of targeting conceptually best thought of as a subset of the law of armed conflict, the underlying objective of both is the same. Accordingly, the

---

[59] DINSTEIN, *supra* note 51, at 17. Professor Dinstein notes that the law of armed conflict is "predicated on a subtle equilibrium between two diametrically opposed impulses: military necessity and humanitarian considerations." *Id.* at 16.

[60] *See* ADAM ROBERTS & RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 53 (3d ed. 2000). This treaty renounced the employment of any projectile of a weight below 400 grams, which was either explosive or charged with fulminating or inflammable substances. *See* Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Dec. 11, 1868, 138 C.T.S. 297 [hereinafter 1868 St. Petersburg Declaration], https://ihl-databases.icrc.org/ihl/full/declaration1868 [https://perma.cc/PP3T-ZSFH].

[61] *See* 1868 St. Petersburg Declaration, *supra* note 60; *see also* ROBERTS & GUELFF, *supra* note 60, at 53.

[62] Reeves & Thurnher, *supra* note 58, at 1.

[63] DINSTEIN, *supra* note 51, at 16. The balance between military necessity and humanitarian consideration is the very essence of the law of armed conflict. You see this balance not only at the macro-level, but it permeates down to particular rules and provisions. It is what makes the body of law workable considering what is being regulated — i.e., the worst of human conditions. *See id.*

[64] Michael N. Schmitt & Jeffrey S. Thurnher, "*Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict*, 4 HARV. NAT'L SEC. J. 231, 232 (2013).

particular provisions or rules, discussed below, that regulate the targeting of objects will always carefully weigh the violence necessary to accomplish a mission with the need to minimize human suffering and physical destruction during warfare.[65]

B. Targeting and the Law: Distinction, Proportionality, and Precautions in the Attack

The military necessity-humanity balance establishes the foundation for the general principles that regulate hostilities and, more specifically, those relevant to the targeting of an object.[66] Undoubtedly, the most important of these principles is distinction — at times characterized as fundamental or "intransgressible."[67] Since the sole legitimate aim of belligerent hostilities is to weaken and defeat an adversary's military forces,[68] protecting both the civilian population and objects during an armed conflict is important.[69] Referenced in early law of armed conflict provisions, such as the Lieber Code[70] and the St. Petersburg

[65] *See* DINSTEIN, *supra* note 51, at 17; *see also* Shane R. Reeves & David Lai, *A Broad Overview of the Law of Armed Conflict in the Age of Terror*, *in* THE FUNDAMENTALS OF COUNTERTERRORISM LAW 139, 147-49 (Lynne Zusman ed., 2014) ("[M]ilitary necessity is 'discounted in the rules' that comprise the Law of Armed Conflict, with the particular provisions of the law either allowing for violence and destruction or forbidding such conduct out of deference to humanitarian considerations."); Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, 50 VA. J. INT'L L. 795, 799 (2010) [hereinafter *Military Necessity*].

[66] *See* Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, HARV. NAT'L SEC. J. FEATURES ONLINE 9-10 (2013) [hereinafter *Autonomous Weapon Systems*], https://harvardnsj.org/wp-content/uploads/sites/13/2013/02/Schmitt-Autonomous-Weapon-Systems-and-IHL-Final.pdf [https://perma.cc/DK85-537J] (discussing how the rules act as a safeguard).

[67] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257. The opinion also stated that distinction is one of two "cardinal" principles in the law of armed conflict. *See id.*

[68] *See* Nils Melzer, *The Principle of Distinction Between Civilians and Combatants*, *in* THE OXFORD HANDBOOK OF INTERNATIONAL LAW IN ARMED CONFLICT 296, 297 (Andrew Clapham & Paola Gaeta eds., 2014). The 1868 St. Petersburg Declaration makes a similar statement. *See* 1868 St. Petersburg Declaration, *supra* note 60.

[69] *See* COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 at ¶ 1863 (Yves Sandoz et al. eds., 1987) [hereinafter COMMENTARY] (footnotes omitted) ("It is the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected . . . . The entire system established in The Hague in 1899 and 1907 and in Geneva from 1864 to 1977 is founded on this rule . . . .").

[70] *See* LIEBER CODE, *supra* note 55, at art. 22 ("Nevertheless, as civilization has advanced during the last centuries, so has likewise steadily advanced, especially in war on land, the distinction between the private individual belonging to a hostile country

Declaration,[71] distinction is a norm of customary international law.[72] Additional Protocol I provides a contemporary definition of the principle of distinction by stating:

> [I]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[73]

Additional Protocol I further clarifies this legal obligation in regards to objects by requiring any attack — defined as any act of "violence against the adversary, whether in the offence or defence"[74] — to be "limited strictly to military objectives."[75] Military objectives are those "which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[76] This broad definitional framework allows for command discretion in interpretation. Ultimately, combatants must make judgments, often in very difficult and time-sensitive circumstances, in applying this definition. For example, when an object's "total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage"

and the hostile country itself, with its men in arms. The principle has been more and more acknowledged that the unarmed citizen is to be spared in person, property, and honor as much as the exigencies of war will admit.").

[71] 1868 St. Petersburg Declaration, *supra* note 60 ("[T]he only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy . . . .").

[72] *E.g.*, Schmitt, *Autonomous Weapon Systems*, *supra* note 66, at 10; *see also* JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, INTERNATIONAL COMMITTEE OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW VOLUME I: RULES 25, 40 (2005).

[73] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]. It is important to note that the United States has not ratified Protocol I or Protocol II but finds many portions of the protocols to be customary international law. *See generally* Michael J. Matheson, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419 (1987).

[74] AP I, *supra* note 73, at art. 49(1). An "attack" includes both large and small-scale combat actions by either party to the hostilities. *See* COMMENTARY, *supra* note 69, at ¶ 1880; DINSTEIN, *supra* note 51, at 84.

[75] AP I, *supra* note 73, at art. 52(2). This definition is widely recognized as reflecting customary international law. *See* HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 25.

[76] AP I, *supra* note 73, at art. 52(2).

depends upon the facts of a specific situation.[77] An otherwise civilian building may thus become targetable because it is being used by a party to the conflict. However, the protocol also provides clarity on what constitutes a "military objective" by requiring such objects to be only those that "by their nature, location, purpose, or use make an effective contribution to military action."[78]

Objects that by their nature make an effective contribution to military action include, but are not limited to, all those items directly used by armed forces such as: weapons, equipment, transports, fortifications, depots, buildings occupied by armed forces, staff headquarters, and communications facilities.[79] Other objects that may not have a military function may still directly contribute to military action simply due to their geography and location.[80] Natural land areas like beaches, mountain passes, and ridges or constructed items such as bridges or roads may therefore qualify as a military objective.[81] The future intended purpose of an object also determines whether it has an effective contribution to military action — for example, a civilian luxury liner that can easily transform into a method of troop transport.[82] Finally, the current use of a traditionally civilian object — like a hotel or church acting as headquarters for a military's staff — also determines if it is a military objective.[83]

---

[77] *Id.*; *see* LAURIE R. BLANK & GREGORY P. NOONE, INTERNATIONAL LAW AND ARMED CONFLICT: FUNDAMENTAL PRINCIPLES AND CONTEMPORARY CHALLENGES IN THE LAW OF WAR 399 (2013) (noting that a civilian object would not offer a definite military advantage at one moment but could if converted into a command post, a weapon storage facility, or a location to launch attacks). The reference to "military advantage" in the definition of military objective is positive expression of the broader concept of "military necessity." *See generally* Schmitt, *Autonomous Weapon Systems*, *supra* note 66, at 22.

[78] AP I, *supra* note 73, at art. 52(2); *see also* BLANK & NOONE, *supra* note 77, at 397 (discussing how "nature, location, use [and] purpose" are separate and definable criteria for determining a military objective).

[79] *See* COMMENTARY, *supra* note 69, at ¶ 2020.

[80] *See* BLANK & NOONE, *supra* note 77, at 398-99.

[81] *See* COMMENTARY, *supra* note 69, at ¶ 2021 ("[A] site which is of special importance for military operations in view of its location, either because it is a site that must be seized or because it is important to prevent the enemy from seizing it, or otherwise because it is a matter of forcing the enemy to retreat from it.").

[82] SOLIS, *supra* note 56, at 511-12. Professor Solis notes that converting luxury liners into troop transports was a regular practice during World War II and the Korean Conflict. *Id.* at 511. In fact, as late as 1982, during the United Kingdom-Argentina Falklands conflict, "the P&O Cruise Line's forty-five-thousand-ton *Canberra* was requisitioned by the British Ministry of Defense, hastily converted to troop use, and used to transport two thousand combatants to the Falklands." *Id.* at 511-12.

[83] *See* COMMENTARY, *supra* note 69, at ¶ 2022.

Many objects have dual military and civilian functions. Additionally, even in those circumstances where an object is exclusively a military objective, surrounding civilian objects may be at risk during targeting. Pursuant to the principle of proportionality,[84] parties to the conflict are obligated to minimize "collateral damage" or, in other words, the effects of the attack on the civilian population.[85] However, damage to civilian property does not necessarily indicate a violation of the principle of distinction.[86] Rather, launching an attack that may be expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian objects is prohibited if the death, injury, or damage to civilian life and property is excessive in relation to the direct and concrete military advantaged gained.[87] For example, the presence of a soldier on leave cannot justify the destruction of an entire village. By contrast, if the destruction of a bridge is vitally important to the success of a military operation, it is understood that some nearby civilians' buildings may be hit in the attack of the bridge.[88] Similar to the definition of military objective, commanders have discretion in the proportionality analysis as the military advantage gained is circumstance-specific and the incidental loss to civilian life and property is typically only an estimate.[89] While this analysis is therefore always contextual, at a minimum the principle of proportionality acts as a protective threshold by ensuring the unintended civilian harm is not on a scale such that it is tantamount to being indiscriminate.[90]

---

[84] The principle of proportionality is a norm of customary international law. *See generally* HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 46.

[85] *See* DINSTEIN, *supra* note 51, at 155.

[86] *See* SOLIS, *supra* note 56, at 292 (quoting Yoram Dinstein, *Discussion: Reasonable Military Commanders and Reasonable Civilians*, 78 INT'L L. STUD. 173, 219 (2002)) ("Nevertheless, the realistic goal is to minimize civilian casualties, not to eliminate them altogether. There is no way to eliminate civilian deaths and injuries due to collateral damage, mistake, accident and just sheer bad luck."). In fact, extensive civilian casualties or destruction of property is acceptable if it is not excessive in relation to the direct and concrete military advantage gained. *Id.* at 292-93 (discussing proportionality).

[87] *See* AP I, *supra* note 73, at arts. 51(5)(b), 57(2)(a)(iii). Other treaties express the principle of proportionality as well. *See, e.g.*, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflict (Protocol II) art. 14, June 8, 1977, 1125 U.N.T.S. 313 [hereinafter AP II]; Rome Statute of the International Criminal Court, art. 8(2)(b)(iv), July 17, 1998, 2187 U.N.T.S. 90.

[88] *See* COMMENTARY, *supra* note 69, at ¶¶ 2213-14.

[89] *See* Schmitt, *Autonomous Weapon Systems*, *supra* note 66, at 24 (stating that the proportionality analysis is contextual).

[90] *See* Corn et al., *supra* note 51, at 182.

Further supplementing the principle of distinction is the well-understood customary international norm that "in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[91] This mandate imposes, on both the attacking and defending parties in the hostilities, a number of precautionary legal obligations. For the attacking party, these obligations include: doing everything feasible[92] to identify military objectives and direct attacks only at those targets;[93] taking all feasible precautions in the choice of the means and methods of warfare;[94] refraining or canceling any attack that violates the principle of proportionality;[95] providing advanced warning to civilians if circumstances permit;[96] and targeting the military objective, when possible, that is "expected to cause the least danger to civilian lives and to civilian objects."[97] The defending party, for their part, must take feasible measures to protect the civilian population, individual civilians, and civilian objects from the dangers resulting from military operations.[98]

C. Specially Protected Objects — Works and Installations Containing Dangerous Forces

Certain types and classes of objects receive protections in addition to those provided by the general legal framework described above. A non-

[91] AP I, *supra* note 73, at art. 57(1); *see also* BOOTHBY, LAW OF TARGETING, *supra* note 52, at 119 (discussing how the general rules of precautions in the attack can reasonably be regarded as supplementing the principle of distinction). Precautions in the attack were first codified in Article 2 of the 1907 Hague IX Regulations. *See* Convention Between the United States and Other Powers Concerning Bombardment by Naval Forces in Time of War, art. 2, Oct. 18, 1907, 36 Stat. 2351. The obligation to take precautions in the attack is customary international law. *See* HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 51.

[92] "Feasible" is that which is "practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations." Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II), art. 3(10), as amended May 3, 1996, 2048 U.N.T.S. 93.

[93] *See* AP I, *supra* note 73, at art. 57(2)(a)(i).

[94] *See id.* at art. 57(2)(a)(ii); *see also* A. P. V. ROGERS, LAW ON THE BATTLEFIELD 96 (2d ed. 2004) (noting that the means and methods of warfare chosen must be likely to hit the target).

[95] *See* AP I, *supra* note 73, at arts. 57(2)(a)(iii), (b).

[96] *See id.* at art. 57(2)(c).

[97] *Id.* at art. 57(3).

[98] *See id.* at art. 58.

exhaustive list of examples includes medically-related objects,[99] the natural environment,[100] cultural property,[101] and objects indispensable to the survival of the civilian population.[102] However, of particular relevance to the potential targeting of critical infrastructure is the special protections provided for works and installations containing dangerous forces.

Additional Protocol I, Article 56 prohibits "dams, dykes and nuclear electrical generating stations" from being the "object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."[103] Further, the rule provides that other military objectives located at, or near, these works or installations "shall not be made the object of attack if such attack may cause the release of dangerous forces . . . and consequent severe losses among the civilian population."[104] The rule also requires attackers to take all practical precautions to avoid the release of the dangerous forces if the structure loses special status[105] and prohibits making dams, dykes, and nuclear electrical generating stations the object of reprisals.[106] Finally, although the rule appears largely focused on attacking forces, it also applies to military operations in the defense stating "[t]he Parties to the conflict shall endeavour to avoid locating any military objectives in the vicinity of the works or installations . . . ."[107]

As justification for these special protections, the Commentary to the rule offers several historical incidents where catastrophic collateral damage resulted from attacks on works or installations containing dangerous forces. For example, in 1938 Chinese Nationalists destroyed

[99] *See, e.g.*, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, arts. 33-37, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31.

[100] *See, e.g.*, AP I, *supra* note 73, at arts. 35(3), 55.

[101] *See, e.g.*, Convention for the Protection of Cultural Property in the Event of Armed Conflict, arts. 2-4, May 14, 1954, 249 U.N.T.S. 240.

[102] *See, e.g.*, AP I, *supra* note 73, at art. 54.

[103] *Id.* at art. 56(1). Similar protections also apply in a non-international armed conflict. *See* AP II, *supra* note 87, at art. 15.

[104] AP I, *supra* note 73, at art. 56(1).

[105] The terminology "special status" refers to heightened protections under the law of international armed conflict. As noted in the commentary to Article 56, "[i]t seemed appropriate to specify that in any attack directed against a dam, dyke or nuclear electrical generating station which had ceased to enjoy special protection, all other rules protecting the civilian population must be respected." COMMENTARY, *supra* note 69, at ¶ 2168.

[106] *See* AP I, *supra* note 73, at art. 56(4).

[107] *Id.* at art. 56(5).

the dykes of the Yellow River near Chang-Chow to stop advancing Japanese troops, resulting in extraordinary civilian death and property damage.[108] However, the protections described in the article are not absolute and are limited in two circumstances. First, these special protections only applies to dams, dykes, and nuclear electrical generating stations, which, if attacked, would release dangerous forces causing severe civilian losses.[109] Accordingly, if the structure is away from areas of civilian habitation, and is a military objective, there is no prohibition on such an attack.[110] Second, the special protections under the rule cease if the structure "is used for other than its normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support."[111]

Article 56 is not without controversy. The United States categorically denied the applicability of the rule to its military operations.[112] Similarly, on ratification of Additional Protocol I, the United Kingdom stated it could not "undertake to grant absolute protection to installations which may contribute to the opposing party's war effort, or to the defenders of such installations" but would "take all due precautions in military operations" based on known facts.[113] France also agreed absolute protections for works or installations was not possible.[114] As a result, a more limited set of prohibitions on targeting works and installations containing dangerous forces is arguably also customary international law.[115]

---

[108] *See* COMMENTARY, *supra* note 69, at ¶ 2142. Other historic examples discussed in the Commentary include German troops flooding thousands of hectares of farmland in the Netherlands with seawater in 1944 and numerous deliberate attacks in 1943 against hydroelectric dams in Germany. *See id.* at ¶¶ 2142-43.

[109] *See* AP I, *supra* note 73, at art. 56(1).

[110] *See* DINSTEIN, *supra* note 51, at 174.

[111] AP I, *supra* note 73, at art. 56(2); *see also* DINSTEIN, *supra* note 51, at 174.

[112] *See* Matheson, *supra* note 73, at 427 ("[W]e do not support the provisions of [A]rticle 56, concerning dams, dykes, and nuclear power stations . . . ."). The United States stressed that the proportionality analysis was appropriate for assessing the legality of an attack against such works or installations. *See* BOOTHBY, LAW OF TARGETING, *supra* note 52, at 247 n.81. Whether this is still the position of the United States is unclear.

[113] BOOTHBY, LAW OF TARGETING, *supra* note 52, at 248; *see also* HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 140.

[114] HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 140.

[115] *See id.* at 139; *see also* TALLINN MANUAL 2.0, *supra* note 21, at 529. The International Group of Experts that drafted the Tallinn Manual generally agreed that neither Article 56 nor Additional Protocol II, Article 15, were customary international law. *See id.* The Tallinn authors therefore drafted a more limited rule to reflect customary international law than that found in the Additional Protocols by drawing from Rule 42 of the International Committee of the Red Cross's Customary

Regardless of the outcome of this debate, Article 56 provides a legal framework for considering how best to protect important objects.[116] Determining whether critical infrastructure requires heightened protections from cyber-attacks during an armed conflict depends on whether the existing law of targeting provides adequate legal safeguards. Application of the law of armed conflict's general principles and rules to critical infrastructure in cyberspace is therefore necessary to make this determination.

III. APPLYING THE EXISTING RULES TO CRITICAL INFRASTRUCTURE IN CYBERSPACE

Understanding how the existing law of targeting regulates cyber-attacks against critical infrastructure during an armed conflict is not merely an abstract academic pursuit. This exercise is of utmost importance as advanced States rely heavily on critical infrastructure to perform essential societal functions. Consequently, as the threat posed by cyber means and methods increases, so does the relevance of this analysis.[117]

A. Law of Armed Conflict Applies to Cyberspace

As a preliminary matter, it is important to establish that the law of armed conflict applies in cyberspace. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence ("NATO CCD COE"), a cyber think tank in Tallinn, Estonia, convened a group of international law experts to develop a practical manual on cyber conflict.[118] This group of legal scholars and practitioners, referred to as the International Group of Experts, analyzed and then articulated how extant legal norms

International Humanitarian Law Study, which states "[p]articular care must be taken if works and installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, and other installations located at or in their vicinity are attacked, in order to avoid the release of dangerous forces and consequent severe losses among the civilian population." *Id.* (citing HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 139).

116 In fact, Article 56 appears to recognize the need for protecting future, unanticipated works or installations by including a provision urging the High Contracting Parties and the Parties to the conflict "to conclude further agreements among themselves to provide additional protections for objects containing dangerous forces." AP I, *supra* note 73, at art. 56(6).

117 For a comprehensive approach to emerging technology and the law of armed conflict, see generally THE IMPACT OF EMERGING TECHNOLOGIES ON THE LAW OF ARMED CONFLICT (Eric Talbot Jensen & Ronald T.P. Alcala eds., 2019).

118 *See* TALLINN MANUAL 2.0, *supra* note 21, at 1.

apply to cyber warfare.[119] Their efforts resulted in the *Tallinn Manual on International Law Applicable to Cyber Warfare* in 2013.[120] In its nearly 600 pages, the manual addresses vital issues spanning public international law and in particular the law governing cyber warfare. In light of the success of the first manual, the NATO CCD COE initiated a subsequent effort to enlarge the scope of coverage with an updated Tallinn Manual to include the international law governing cyber activities during peacetime. As part of the follow-on effort, the NATO CCD COE again assembled a group of international law experts, which led to the creation and publication of *Tallinn Manual 2.0* in February 2017. *Tallinn Manual 2.0* not only incorporated and updated the materials from the first *Tallinn Manual*, but also included coverage of peacetime international legal regimes and frameworks.[121] Importantly, the *Tallinn Manual 2.0* experts limited the manual to an objective restatement of the *lex lata* and avoided including statements reflecting the *lex ferenda*.[122]

Tallinn Manual 2.0 expressly states that the current law of armed conflict applies to cyberspace and cyber-attacks during armed conflict.[123] While, to date, there are no cyber-specific law of armed conflict treaties, the Martens Clause, found in the preamble to the 1899

---

[119] *See id.*; *see also* Jeremy Kirk, *Manual Examines How International Law Applies to Cyberwarfare*, CIO (Sept. 3, 2012, 7:00 AM), https://www.cio.com/article/2392610/manual-examines-how-international-law-applies-to-cyberwarfare.html [https://perma.cc/YEK5-SHUL] (noting that the Cooperative Cyber Defense Center of Excellence, which "assists NATO with technical and legal issues associated with cyberwarfare-related issues," created the Tallinn Manual to examine "existing international law that allows countries to legally use force against other nations, as well as laws governing the conduct of armed conflict").

[120] *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 1 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL 1.0].

[121] *See* TALLINN MANUAL 2.0, *supra* note 21, at 1.

[122] *See id.* at 3.

[123] *See id.* An "armed conflict" triggers the law of armed conflict. *See* ADVISORY SERV. ON INT'L HUMANITARIAN LAW, *supra* note 22 ("International humanitarian law applies only to [international or non-international] armed conflict; it does not cover internal tensions or disturbances such as isolated acts of violence. The law applies only once a conflict has begun, and then equally to all sides regardless of who started the fighting."). While there is not a conclusive definition of the term "armed conflict," it is generally understood to "exist[] whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State." Prosecutor v. Tadi , Case No. IT-94-1-l, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

Hague Convention (II),[124] reflects customary international law and remains applicable even in novel cyber situations.[125] Therefore, the lack of cyber-specific treaties does not equate to a legal lacuna regarding the application of the law of armed conflict to cyberspace and cyber-attacks[126] as the Martens Clause extends existing principles and rules to fill any gaps in legal regulations caused by emerging technologies and, specifically, cyber capabilities.

While the *Tallinn Manual 2.0* experts were unanimous in their conclusion that the law of armed conflict applies to both international and non-international armed conflicts,[127] this determination has recently come into question. In 2015, the United Nations General Assembly requested a body of experts to form a group officially titled the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, or more simply, the UN Group of Government Experts ("UN GGE"). The task of the UN GGE was to build upon the conclusions of four previous experts' reports in order to promote common understandings on various technology related matters including "how international law applies to the use of information and communications technologies by States."[128] Despite adopting an uncontroversial

---

[124] *See* Preamble, Convention Between the United States and Certain Powers, with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803 [hereinafter Hague Convention II]. Specifically, the Martens Clause states:

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

Id.

[125] The Martens Clause is often invoked in the interpretation of law of armed conflict treaties "both to rule out that what is not expressly prohibited is permitted and as a presumption that favours humanitarian considerations whenever doubts exist on the meaning of certain provisions." MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 22 (2014).

[126] The Martens Clause is the subject of a great deal of controversy with some arguing that it represents an enforceable legal principle and others arguing the clause is more general guidance. For a more detailed discussion, see Dave Wallace & Shane R. Reeves, *Modern Weapons and the Law of Armed Conflict*, *in* U.S. MILITARY OPERATIONS: LAW, POLICY, AND PRACTICE 41, 62-63 (Geoffrey S. Corn et al. eds., 2016).

[127] TALLINN MANUAL 2.0, *supra* note 21, at 375.

[128] G.A. Res. 70/237, Developments in the Field of Information and Telecommunications in the Context of International Security (Dec. 23, 2015).

approach to the applicability of international law to cyberspace, a number of States rejected the final report in 2017.[129]

By rejecting the report, some legal questions remain unsettled.[130] However, the States' non-concurrence with the report was seemingly more of a political decision than a rejection of the understanding that international law applies in cyberspace.[131] In fact, whether the law of armed conflict applies in the cyber context is seemingly a resolved issue "[s]ince no international lawyer can . . . deny their applicability to cyber activities, [so] the failure of the GGE can only be interpreted as the intentional politicization in the cyber context of well-accepted international law norms."[132]

B. What Is a "Cyber Armed Attack?"

Since the law of armed conflict applies fully to cyberspace, the meaning of "cyber-attack" is critical it serves as the basis for numerous limitations and prohibitions under the international law.[133] Rule 92 of *Tallinn Manual 2.0* provides that a cyber-attack is "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects," whereas

---

[129] *See* Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SECURITY (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms [https://perma.cc/337F-DD8V]. While only Cuba issued a formal declaration of non-concurrence with the report, Russia and China also reportedly rejected the group's final product. *See id.*

[130] *See id.* ("The real legal challenge lies in determining when and how the aforementioned rights and legal regimes apply in the unique cyber context, questions Russia, China and the other recalcitrant States have deftly sidestepped.").

[131] *See id.* (noting that "[r]educed to basics, the States concerned have put forward what are essentially political arguments that make little legal sense"). The United States has expressly stated that international law applies in cyberspace. *See* THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011) ("The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing norms obsolete. Long-standing international norms guiding state behavior — in times of peace and conflict — also apply in cyberspace."); *see also* Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013) (noting that the United States, as well as other important States such as China and Russia, agreed that "[i]nternational law, and in particular the Charter of the United Nations, is applicable" to cyberspace).

[132] Schmitt & Vihul, *supra* note 129.

[133] *See* Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 294. Again, an "attack" is defined as an act of "violence against the adversary, whether in the offence or in defence." AP I, *supra* note 73, at art. 49(1).

non-violent operations do not qualify as an attack.[134] However, "[c]yber operations have complicated matters in that they can be highly useful militarily without generating destructive or injurious effects."[135] Therefore,"[t]he violence must be understood in terms of the consequences of the act rather than the act itself; hence, violent acts may include cyber (computer network) attacks leading to mayhem and destruction."[136]

For example, a cyber operation against an electrical grid or a hydro-electrical plant that results in violent consequences is a cyber-attack,[137] and, as such, is subject to the law of targeting. In contrast, an act of cyber espionage having no violent effects is not a cyber-attack and, therefore, the principle of distinction and its supplementing provisions do not regulate that behavior. Yet, there is difficulty in determining whether the concept of "attack" extends to certain nondestructive or non-injurious cyber operations such as altering or destroying data.[138] The majority of the experts behind *Tallinn Manual 2.0* took the position that, under the current state of the law, the concept of "object" is not interpreted to include something as intangible as "data."[139] Noting that "data" does not fall under the ordinary meaning of the word "object" nor comports with how the Commentary to Additional Protocol I defines the term,[140] the majority of the experts were not willing to extend the concept of "attack" to damaging or destroying data. However, this position seems untenable going forward as Professor Michael N. Schmitt notes:

> Given the pervasive importance of cyber activities, an interpretation that limits the notion of attacks to acts generating physical effects cannot possibly survive. Suggestions that civilian activities may lawfully be seriously disrupted or that important data can be altered or destroyed because there is no resulting physical damage or injury will surely collide with

134 TALLINN MANUAL 2.0, *supra* note 21, at 415.

135 Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 294.

136 DINSTEIN, *supra* note 51, at 84; *see also* TALLINN MANUAL 2.0, *supra* note 21, at 415.

137 *See* TALLINN MANUAL 2.0, *supra* note 21, at 416.

138 *See id.* at 437.

139 *Id.*

140 *See* COMMENTARY, *supra* note 69, at ¶¶ 2007-08 (noting that the term "object" means something "visible and tangible" that can be "placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing").

> future assessments of the military necessity/humanitarian considerations balance.[141]

At a minimum, it appears that a cyber operation that interferes "with the functionality of an object" necessitating "repair of the target cyber infrastructure" qualifies as a cyber-attack.[142] Yet, while the existing law may limit a cyber-attack to those events causing physical harm,[143] it is worth again noting that any cyber-attack on critical infrastructure could potentially result in extreme, unanticipated consequences.[144] Deleting, corrupting, altering, or otherwise disrupting the computer network supporting critical infrastructure may result in the destruction or incapacitation of the structure or facility.[145] The effects of such an operation are not limited to simply causing damage to the computer networks of a given facility but may extend to large numbers of people through the loss of, for example, electrical power or water.[146] While physical damage to property, loss of life, and injury to persons may not be the intended purpose of the cyber-attack that targets critical infrastructure, this could be the result.[147] Therefore, while *de minimis* damage to critical infrastructure may not meet the cyber-attack definitional threshold, considering the expected secondary and tertiary effects of any such operation is necessary in applying the law of armed conflict.

C. The Law of Targeting Applied to Cyber-Attacks Against Critical Infrastructure During Armed Conflict

A cyber-attack occurring against critical infrastructure during an armed conflict triggers the law of targeting as it specifically relates to objects and, consequently, any concomitant protections.[148] The principle of distinction clearly prohibits a cyber-attack on critical

---

141 Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 295-96.

142 *Id.* at 295 (citing TALLINN MANUAL 1.0, *supra* note 120, at 93).

143 The likelihood that the concept of "cyber-attack" remains limited to causing physical harm to person and/or tangible objects is unlikely to remain static. Most likely, the notion of cyber-attack will expand to "include interference with essential civilian functions." *Id.* at 296. For a discussion on the difficulty in expanding the definition of "cyber-attack," see *id.*

144 *See supra* Part II (highlighting the potential devastating consequences of an attack on critical infrastructure).

145 *See* ROSCINI, *supra* note 125, at 52.

146 *See id.* at 52-53.

147 *See id.* at 53.

148 *See supra* Part III (highlighting what triggers the law of targeting).

infrastructure exclusively used for a civilian purpose.[149] However, critical infrastructure is generally dual use in nature — meaning it has both a military and civilian function — and therefore qualifies as military objective.[150] For example,

> military communications occur in part across cables and other media that are also used for civilian traffic. Weapons often rely on data generated by the Global Positioning Satellite (GPS) system, which serves civilian purposes such as navigation. Social media like Facebook and Twitter have been widely used during recent conflicts to transmit militarily important information. Militaries are also increasingly turning to 'off the shelf' equipment like commercial computer systems for their forces, thereby qualifying the factories which produce the products as military objectives.[151]

Certainly, if the military and civilian functions are distinguishable in dual-use critical infrastructure, any cyber-attack may only target the military function.[152] Still, most critical infrastructure is interconnected and interdependent, making such fine discernments extremely difficult. As a result, protections for critical infrastructure from a cyber-attack occurring during an armed conflict are primarily through the principle of proportionality and the requirement to take precautions in the attack.[153]

"[T]he principle of proportionality allows, in effect, an attacker to conduct an attack in the knowledge"[154] that civilian objects will be damaged or destroyed assuming such loss is incidental and not "excessive in relation to the concrete and direct military advantage

---

[149] *See* AP I, *supra* note 73, at art. 48; *see also* TALLINN MANUAL 2.0, *supra* note 21, at 420-21.

[150] *See* AP I, *supra* note 73, at art. 52(2); *see also* Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 298 ("The extent of military use is irrelevant; so long as the object is being employed militarily, it qualifies as a military object subject to attack." (citing TALLINN MANUAL 1.0, *supra* note 120, at 112)).

[151] Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 298.

[152] *See* AP I, *supra* note 73, at art. 51(5)(a) (defining an indiscriminate attack as "an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects"). The Tallinn Manual 2.0 updates and operationalizes this provision for cyber-attacks in Rule 112. *See* TALLINN MANUAL 2.0, *supra* note 21, at 469-70.

[153] *See supra* Part III.B. (discussing proportionality).

[154] Ian Henderson & Kate Reece, *Proportionality Under International Humanitarian Law: The "Reasonable Military Commander" Standard and Reverberating Effects,* 51 VAND. J. TRANSNAT'L L. 835, 854 (2018).

anticipated."[155] While calculating the expected collateral damage from a cyber-attack on critical infrastructure is difficult,[156] the importance of these assets to ongoing military operations[157] makes the anticipated "concrete and direct military advantage" gained from such an attack significant.[158] Further, those planning or approving a cyber-attack against critical infrastructure have discretion as terms like "expected," "excessive," and "anticipated" that are embedded within the proportionality principle allow for a "fairly broad margin of judgment."[159] Future applications of the principle of proportionality may become more difficult for those conducting cyber-attacks as "[t]he notion of damage in the proportionality context will probably expand beyond a strict limitation to physical effects" and the term "object" may include a broader understanding.[160] However, as currently applied, the proportionality principle legally allows for, if necessary, extensive collateral damage from a cyber-attack against critical infrastructure during armed conflict.[161] In other words, as long as such damage remains below the "excessive" threshold there is no prohibition against

[155] TALLINN MANUAL 2.0, *supra* note 21, at 470.

[156] A cyber-attack may cause "what have been termed 'reverberating,' 'knock-on,' or 'indirect' effects." Henderson & Reece, *supra* note 154, at 847; *see also* TALLINN MANUAL 2.0, *supra* note 21, at 472 ("Collateral damage can consist of both direct and indirect effects."). However, the proportionality analysis considers only expected indirect effects in contrast to those that are remote possibilities. *See id.* at 475 ("The attacker either reasonably expects it or the possibility of collateral damage is merely speculative, in which case it would not be considered in assessing proportionality."). For a more detailed discussion on the difference between "expected" and "remote" indirect effects, see Henderson & Reece, *supra* note 154, at 846-54.

[157] *See supra* Part II (discussing the general importance of critical infrastructure).

[158] *See* AP I, *supra* note 73, at art. 51(5)(b).

[159] *See* COMMENTARY, *supra* note 69, at ¶ 2210. Of course, a commander must be "reasonable" when making a targeting decision. *See* TALLINN MANUAL 2.0, *supra* note 21, at 475 (citing Prosecutor v. Gali , Case No. IT-98-29-T, Judgement and Opinion, ¶ 58, (Int'l Crim. Trib. for the Former Yugoslavia Dec. 5, 2003) ("In determining whether an attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack.")). *See generally* Bill, *supra* note 57 (discussing the Rendulic Rule); Henderson & Reece, *supra* note 154, at 855 (arguing that the "appropriate standard for assessing a decision on the proportionality of attack is that of a 'reasonable military commander'").

[160] *See* Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 297.

[161] *See* TALLINN MANUAL 2.0, *supra* note 21, at 473 ("[T]he majority of the International Group of Experts took the position that extensive collateral damage may be legal if the anticipated concrete and direct military advantage is sufficiently great.").

a cyber-attack against critical infrastructure functioning as a military objective.

Those executing a cyber-attack against critical infrastructure are also required to "be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon."[162] Yet, similar to the principle of proportionality, in application the constant care obligation will most likely not prohibit a cyber-attack against critical infrastructure. The precautionary legal obligations — whether requiring a cyber-attacker to do everything feasible to verify the critical infrastructure is a military objective[163] or to take all feasible precautions in the choice of the cyber means and methods intended for the attack[164] — provide the decision-maker ample discretion to go forward with a cyber-attack. In fact, the term "feasible" is widely accepted as that which is "practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations."[165] The other express precautionary provisions also contain sufficiently ambiguous language to allow for a cyber-attack.[166] Consequently, the requirement to take precautions in the attack may shape how the cyber-attack occurs, but will not legally prohibit such action.[167]

Given the nature of critical infrastructure and the possible catastrophic consequences associated with cyber-attacks against such objects, the general protections provided by the law of targeting are insufficient.[168] Logically, this would seem to trigger the special

---

[162] *Id.* at 477 (citing U.K. MINISTRY OF DEFENCE, THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 5.32.1 (2004)).

[163] *See* AP I, *supra* note 73, at art. 57(2)(a)(i).

[164] *Id.* at art. 57(2)(a)(ii).

[165] *E.g.*, Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons (Protocol III), art. 1(5), Oct. 10, 1980, 1342 U.N.T.S. 171.

[166] For example, the attacker must provide advance warning to civilians if "circumstances permit," AP I, *supra* note 73, at art. 57(2)(c), and, when possible, only target the military objective that is "expected to cause the least danger to civilian lives and to civilian objects." *Id.* at art. 57(3).

[167] *See* Henderson & Reece, *supra* note 154, at 854 (noting that even if "all the appropriate precautions are taken, there will be some circumstances in which . . . civilian objects remain in danger of incidental harm from an attack").

[168] *See, e.g.*, Rob Taylor & Mayumi Negishi, *U.S. Allies Raise New Security Worries About China's Huawei*, WALL ST. J. (Dec. 7, 2018, 12:54 PM), https://www.wsj.com/articles/water-electricity-would-be-at-risk-in-attacks-on-5g-networks-australian-intelligence-chief-says-1544182836 [https://perma.cc/V6BQ-A6NJ]. "The head of Australia's top military cyber defense agency, Mike Burgess, said Chinese companies were blocked from the rollout of 5G mobile-phone capabilities in August because the new technology" would threaten critical infrastructure. *Id.* Mr. Burgess clarified the

protections extended for particular objects found within the law of armed conflict.[169] More specifically, the extra-legal safeguards provided for works and installations containing dangerous forces found in Additional Protocol I, Article 56[170] are relevant to regulating cyber-attacks during armed conflicts. Unfortunately, these provisions are limited to a narrow class of objects and do not comprehensively guard a State's entire critical infrastructure.[171] These provisions are therefore most helpful if viewed as a blueprint for how the law can evolve to provide heightened protections against cyber-attacks for critical infrastructure during armed conflicts.

IV. PROTECTING CRITICAL INFRASTRUCTURE IN AN ERA OF CYBER WARFARE

It is increasingly "inconceivable that the extant law of cyber warfare, which responds to cyber operations that are still in their relative technological infancy, will survive intact" in today's technological age.[172] This is especially true as "cyber activities become ever more central to the functioning of modern societies, the law is likely to adapt by affording them greater protection."[173] The trend therefore, is towards greater protections for those assets, including critical infrastructure, that are essential to civilian activities.[174] However, how these protections evolve, especially during an armed conflict, is currently unknown.[175]

reasoning by stating, "[i]f the 5G network of the future isn't there, there's a good chance electricity supply might be interrupted, water supply might be interrupted, the financial sector or elements of it might impacted." *Id.* Similarly, Japan is taking steps to lower the cyber-infiltration risk of its government agencies and critical infrastructure. *See id.*

169 *See supra* notes 103–111 and accompanying text (discussing the law of targeting's special protection provisions).

170 *See* AP I, *supra* note 73, at art. 56. Additional Protocol II, Article 15 offers a counterpart for these provisions for a non-international armed conflict. *See* AP II, *supra* note 87, at art. 15. The special protections of objects indispensable to the survival of the civilian population may also be salient when exploring the idea of how best to provide additional legal safeguards for critical infrastructure. *See* AP I, *supra* note 73, at art. 54.

171 For example, the special protections for dams, dykes, and nuclear electrical generating stations would only insulate a minor portion of the United States' critical infrastructure. *See supra* notes 28, 30 and accompanying text (listing the sixteen critical infrastructure sectors designated by the United States).

172 Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 271.

173 *Id.* at 299.

174 *See id.* at 296-99.

175 *See id.* at 296.

The legal framework contained in Additional Protocol I, Article 56 for protecting particularly important objects offers a possible solution to this problem. The special protections outlined in Article 56 expressly cover dams, dykes, and nuclear electrical generating stations.[176] These objects, a subset of any State's critical infrastructure, receive special protections because of the potentially catastrophic consequences of an attack. In contemporary warfare, a cyber-attack on critical infrastructure, whether it be a health care system, power grid, or transportation network, has the same possible devastating effects. Therefore, developing a legal provision similar to Article 56, albeit with broader understanding of what is a protected object seems to be a necessary expansion in this era of cyber warfare.

Perhaps more importantly, Additional Protocol I, Articles 56 provides a workable template for addressing cyber-attacks against critical infrastructure during armed conflict because of its pragmatic approach to targeting. While the extent of the protections described in Article 56 are debatable,[177] it is unquestioned that the article strives to strike the delicate balance between military necessity and humanitarian considerations required for a workable law of armed conflict legal provision.[178] For example, the article does not absolutely ban an attack on dams, dykes, and nuclear electrical generating stations but rather links a prohibition to attacks that "may cause the release of dangerous forces and consequent severe losses among the civilian population."[179] Moreover, the special protections afforded under Article 56 cease under specified conditions while also placing duties and obligations on both the attacker and the defender of the critical infrastructure.[180]

Given the operational reasons for targeting critical infrastructure, any future legal provision must address the military necessity-humanity balance. Otherwise, if viewed as less about fixing "the technical limits at which the necessities of war ought to yield to the requirements of humanity,"[181] and more about restricting all cyber-attacks on critical infrastructure,[182] the provision risks being ineffectual and ignored.

---

[176] *See* AP I, *supra* note 73, at art. 56(2).

[177] *See supra* notes 112–115 and accompanying text (noting the debate over Article 56 customary status and applicability).

[178] *See supra* Part III.A–B (discussing the military necessity-humanity balance).

[179] AP I, *supra* note 73, at art. 56(1).

[180] *See id.* at art. 56(2).

[181] 1868 St. Petersburg Declaration, *supra* note 61.

[182] *See* Reeves & Thurnher, *supra* note 57, at 12 ("It is incumbent upon states to maintain the balance between military necessity and humanity, as the primacy of the Law of Armed Conflict is dependent upon this equilibrium.").

Therefore, any new norm must look to Article 56 as a model for how to weigh military necessity with the dictates of humanitarian aims in order to be an effective regulatory provision. While States may resist joining a cyber-specific treaty protecting critical infrastructure during armed conflict, there may be incentives for States to sign and ratify such a treaty, tempered by a realistic skepticism that pervades compliance with and enforcement of the law of armed conflict generally.

First, States have an enlightened self-interest in protecting their own critical infrastructure. Given the increased capability of States to use digital combat power offensively, the vulnerabilities of and threats to advanced States' critical infrastructure are outpacing their ability to defend their networked computer systems.[183] A cyber-specific treaty establishing norms of behavior for protecting critical infrastructure during armed conflict is not and will never be a panacea. But, such an international agreement would be underpinned by notions of reciprocity. Once States bind themselves to such a treaty, the continued force of that treaty could be contingent on reciprocal observation by other States.[184] Notwithstanding the challenges associated with attribution in the cyber domain, if a State is found to be abusing the treaty, the attacking State would risk losing the protections associated with entering into the treaty.

A second, and related reason is that, at a minimum, such a cyber-specific treaty provides a special emphasis on the protection of critical infrastructure. As a general matter, civilian objects are protected under the law of armed conflict. There are some objects that receive special or heightened protections under the law of armed conflict "because of their particular importance for the protection of victims of armed conflicts, the civilian population or mankind in general or because of their particular vulnerability to destruction and damage in times of armed conflict."[185] In that regard, critical infrastructure is like other types of objects that the law of armed conflict identifies for heightened protections such as cultural property, medical facilitates, the natural environment and, most specifically, works or installations containing dangerous forces as represented by Additional Protocol I, Article 56.

---

[183] *See, e.g.*, DAVID E. SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE 300-01 (2018) (discussing the actions of the United States and other nations to defend their networked computer systems from a potential Chinese threat).

[184] Sean Watts, *Reciprocity and the Law of War*, 50 HARV. INT'L L. REV. 365, 375 (2009).

[185] *What Objects Are Specially Protected Under IHL?*, INT'L COMM. RED CROSS BLOG (Aug. 14, 2017), https://blogs.icrc.org/ilot/2017/08/14/objects-specially-protected-ihl/ [https://perma.cc/8YJW-EDF3].

Finally, adopting narrowly scoped international agreements to avoid potentially catastrophic consequences of armed conflict is not without precedent. For example, the 1976 *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques* ("ENMOD Convention") prohibits the use of "environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party."[186] The ENMOD Convention defines "environmental modification techniques" as "any technique for changing — through the deliberate manipulation of natural processes — the dynamics, composition or structure of the Earth, including its biota, lithosphere, hydrosphere and atmosphere, or of outer space."[187] The ENMOD Convention was negotiated during a period of heightened international concern about the protection of the environment during armed conflict.[188] Namely, by the 1970s, the international community became increasingly aware that the toll of modern armed conflicts went far beyond human suffering and damage to physical property. It also led to extensive destruction and degradation to the natural environment.[189] Most notably, the widespread use of the defoliant Agent Orange during the Vietnam War resulted in environmental contamination and related human suffering and led to significant international criticism and concern.[190] The roots of the ENMOD Convention represent a reaction to State parties using environmental modification techniques as weapons of war. Some commentators have referred to these means and methods as "geophysical warfare."[191] Such environmental modification techniques include, but are not limited to, provoking earthquakes, tsunamis or changing weather patterns.[192]

Like the 1976 ENMOD Convention, a cyber-specific treaty protecting critical infrastructure would represent a meaningful and realistic effort

---

[186] *See* Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, art. I, Dec. 10, 1976, 1108 U.N.T.S. 151 [hereinafter ENMOD Convention]. The treaty is commonly referred to as the "ENMOD Convention." *See, e.g.*, *1976 Convention on the Prohibition of Military or any Hostile Use of Environmental Modification Techniques*, INT'L COMM. RED CROSS (Jan. 2003), https://www.icrc.org/en/download/file/1055/1976-enmod-icrc-factsheet.pdf.

[187] ENMOD Convention, *supra* note 186, at art. II.

[188] *See* ROBERTS & GUELFF, *supra* note 60, at 407.

[189] *See* U.N. ENV'T PROGRAMME, PROTECTING THE ENVIRONMENT DURING ARMED CONFLICT: AN INVENTORY AND ANALYSIS OF INTERNATIONAL LAW 8 (2009).

[190] *See* KAREN HULME, WAR TORN ENVIRONMENT: INTERPRETING THE LEGAL THRESHOLD 5-6 (2004).

[191] *See* U.N. ENV'T PROGRAMME, *supra* note 189, at 12.

[192] *Id.*

by States to reassert themselves in shaping the normative infrastructure of the law of armed conflict in response to an emerging technology that could cripple the backbone of modern societies — critical infrastructure. Similar to the effects of a disaster like starting earthquakes or creating hurricanes, cyber-attacks against a State's critical infrastructure will precipitate reverberating negative consequences that will permeate throughout that society. Intuitively, the more advanced and interconnected a State, the more devastating the effects will be. To complete the analogy between the ENMOD Convention and a cyber-specific treaty protecting critical infrastructure, it is reasonable to conclude that for both types of attacks — that is, those involving environmental modification techniques and those involving cyber capabilities — the outcomes simply cannot be predicted and controlled. For example, if a belligerent party creates a hurricane that hits Florida, the consequences may vary considerably depending on its strength and where it precisely lands. Likewise, a cyber-attack against a power grid or nuclear power plant could create many unforeseeable and catastrophic effects.

CONCLUSION

In October 2012, in a speech at the Intrepid Sea, Air & Space Museum in New York, United States Secretary of Defense Leon E. Panetta sounded an alarm that the United States was increasingly vulnerable to a "cyber-Pearl Harbor" that could dismantle the nation's critical infrastructure, including power grids, transportation systems, and financial networks.[193] According to Secretary Panetta, the most destructive possibilities involve hostile parties launching cyber operations against multiple critical infrastructure targets simultaneously in concert with a conventional attack.[194] Secretary Panetta's warning is not exclusive to the United States, but applies to any advanced State.

Therefore, the urgent need to protect critical infrastructure from cyber-attacks during armed conflict appears to provide an opportunity for the creation of the first cyber-specific law of armed conflict treaty. This treaty, built upon the legal blueprint found in Additional Protocol I, Article 56, would offer special protections to critical infrastructure from cyber-attacks during an armed conflict. Of course, promulgating a

[193] *See* Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES (Oct. 11, 2012), https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html [https://perma.cc/32UD-5N3U].

[194] *See id.*

new treaty is difficult. For example, even the definition of "critical infrastructure" would likely be a controversial topic requiring significant deliberation.[195] Yet, the very real threat to these assets during an armed conflict, coupled with the common cause shared by advanced States to protect critical infrastructure may provide the incentive necessary to develop a new conventional norm. Otherwise, States are left with the law of targeting's basic protections which, increasingly, are inadequate for protecting assets of such significant importance.

[195] Creation of a new conventional norm is the exclusive responsibility of States. *See* Schmitt, *Military Necessity*, *supra* note 65, at 799 (highlighting that only States can "reject, revise, or supplement" the Law of Armed Conflict or "craft new norms").