American University National Security Law Brief

Volume 13 | Issue 1 Article 1

2023

The Tallinn Manual 2.0 on Nation-State Cyber Operations Affecting Critical Infrastructure

Terence Check

THE TALLINN MANUAL 2.0 ON NATION-STATE CYBER OPERATIONS AFFECTING CRITICAL INFRASTRUCTURE

TERENCE CHECK*

This article examines how public international law might apply to cyber-based operations against critical infrastructure, particularly by examining the Tallinn Manual 2.0, given the Manual's particular prominence in Western legal circles. Taking a sector-by-sector approach, this article shows how international law as restated in the Manual would permit a state actor to launch cyber operations against critical infrastructure in some circumstances, opening vulnerable and sensitive assets to sophisticated attacks from foreign adversaries. Nevertheless, many types of critical infrastructure are entitled to some manner of special legal protections under the law of armed conflict. Due to differing definitions and other factors, this article asserts that it may be difficult to make predictive judgments about what kind of critical infrastructure might be a permissible target of a cyber-attack. But it is clear that there is a significant risk that a hostile actor might lawfully target critical assets and systems during an armed conflict, though forecasting is prone to unpredictability. This article aims to create a better picture of the existing risk landscape for governments and the owners and operators of critical infrastructure, primarily through exploring the inherent risk to their society's sensitive assets under the current lex lata of the law of armed conflict. With a better understanding of the legal dimensions of cyber threats to critical infrastructure during armed conflict, relevant government and private stakeholders can begin to take steps to harden their systems and assets from cyber-attack and thereby better weather potential geopolitical storms.

* Senior Counsel, U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency; Adjunct Professor, Cleveland State University Law School; LL.M, American University; J.D., Cleveland State University. This article and the opinions stated therein are solely the author's and do not represent the views or positions of the United States government or the Department of Homeland Security, or CISA. The author would like to thank his colleagues, including Brian Eschels, for excellent feedback in the course of developing this article.

TABLE OF CONTENTS

"You can be sure of succeeding in your attacks if you only attack places which are undefended."[1]

I. Introduction

Protecting critical infrastructure from cyber threats is difficult and complex. News headlines abound with reports that show how critical infrastructure—ranging from voting machines to steel mills—have become increasingly vulnerable to cyber operations from state and sophisticated non-state actors. As critical infrastructure becomes increasingly entangled with the Internet and as new tactics, techniques, and procedures rapidly proliferate and evolve, governments and businesses alike must contend with a mutating threat environment that may put sensitive and highly important critical infrastructure assets in serious jeopardy. The vulnerabilities of critical infrastructure, which provide vital services and functions to societies, may pose a particularly tempting way for states to asymmetrically project power during an armed conflict or other crisis. Recent tensions between Russia and Ukraine have provided a useful test bed to consider how cyber-threat actors could couple cyber-based operations with movements of traditional military forces.[2]

In the United States, multiple state and federal legal regimes apply to different aspects of cybersecurity: state laws manage conduct within their own jurisdictions, federal law enforcement agencies address cyber crime and other unlawful conduct, regulatory agencies like the Federal Trade Commission and the Securities and Exchange Commission enforce their own cybersecurity rules. Reflecting Congress's judgment that critical infrastructure and cyber security reflects areas of particular concern to U.S. national security overall, federal law charges the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency with exercising primarily voluntary

[1] SUN TZU, THE ART OF WAR 96 (SAMUEL B. GRIFFITH TRANS., 1963).
[2] JOSEPH MARKS & AARON SCHAEFFER, *CYBER FEARS MOUNT AMID PROSPECT OF RUSSIAN INVASION OF UKRAINE*, WASH. POST (JAN. 25, 2022) https://www.washingtonpost.com/politics/2022/01/25/cyber-fears-mount-amid-prospect-russian-invasion-ukraine/.

authorities to provide cybersecurity and critical infrastructure security services to a wide range of critical infrastructure owners and operators.[3] International law—in particular the law of armed conflict—complicates matters further. The fact that most critical infrastructure assets are owned or operated by small or local businesses and governments does not shield those assets from international interest: security through obscurity is probably no longer a viable option for an interconnected world filled with sophisticated cyber threat actors with an eye to gain diplomatic, economic, or military advantages by targeting critical infrastructure.[4]

Understanding this fundamental fact, that predominately private entities must contend with a cybersecurity environment shaped by geopolitical trends and forces of the highest order, this essay examines the *Tallinn Manual 2.0 on the International Law Relating to Cyber Operations* and how the law of armed conflict may impact critical infrastructure assets in cyberspace, *especially during an armed conflict*.[5] Truly, these concepts discussed herein would warrant a fulsome discussion in their own right. In this respect, this article can only be considered a broad overview of the most basic ideas in this tremendously important area of the law. This author merely hopes to provide a better, if cursory, understanding of the *Manual's* examination of legal norms applicable to critical infrastructure; and to spot issues illuminated by the *Manual* to enable lawyers practicing in the area of cybersecurity to provide better advice to their clients (whether public or private) regarding operational risks that may arise from foreign state actors. This task takes on greater importance given the overall geopolitical

---

[3] *See* 6 U.S.C. § 652 (2021). The CISA Chemical Facility Anti-Terrorism Standards (CFATS) Program and the forthcoming cyber incident reporting regulations are among CISA's regulatory missions.

[4] *See, e.g.*, MARKS & SCHAEFFER, *supra* note 2 ("Cyberwarfare experts have warned for years that hacking will play an increasingly prominent role in conventional military conflicts. For example, nations may hack communications and energy systems to undermine their adversaries' ability to respond militarily or to scare their citizens and lower political support for the government."); *See also* CHRIS INGLIS AND HARRY KRESJA, *THE CYBER SOCIAL CONTRACT*, FOREIGN AFFAIRS (FEB. 21, 2022) https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract (commenting on the cyber vulnerabilities in the U.S. following a Russian attack on critical infrastructure, which had the ability to create gas shortages for millions of persons).

[5] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (MICHAEL N. SCHMITT ED., AND LIIS VIHUL ED., 2017) [hereinafter TALLINN MANUAL 2.0].

situation in 2022 and past examples of coupling cyber-intrusions with military action.[6] This article folds out in three parts. First, this article provides an overview of the *Tallinn Manual*, its structure, its background, and key definitions relevant to this kind of legal analysis. Second, this article takes a sector-by-sector approach to whether and how critical infrastructure may be lawfully targeted under the international law set forth in the *Manual*. Third, the article will discuss the obligations of government agencies to protect critical infrastructure under international law, with particular attention paid to the kind of tools the *Tallinn Manual* puts in the cybersecurity toolbox.[7]

Critical infrastructure owners/operators and government agencies will find that the *Manual's* unstated approach to critical infrastructure is a double-edged sword. Unfortunately, it appears that international law as restated in the *Manual* would permit a state actor to launch cyber operations against critical infrastructure in some circumstances, opening vulnerable and sensitive assets to sophisticated attacks from foreign adversaries.[8] The good news is that many types of critical infrastructure are entitled to some manner of special legal protections under the law of armed conflict.[9] Additionally, there are many tools at a government's disposal, as described in the *Manual*, to guard against and respond to cyber operations targeting critical infrastructure. With these concepts in mind, leaders in government and industry may be able to make more informed decisions

---

[6] *See, e.g.*, MARKS & SCHAEFFER, *supra* note 2 ("Russia has pioneered such hybrid campaigns, linking cyberattacks with military operations in its 2008 invasion of Georgia and the 2014 invasion of Crimea. Russia also launched the most serious known attack against an energy system when it interrupted power for thousands of Ukrainian citizens in 2015.").

[7] Importantly, this article only discusses the international law as re-stated by the Tallinn Manual: There are additional legal requirements that may bind the action of government and private actors in any given situation. Just because the Tallinn Manual's restatement may deem a particular action permissible under the international law of armed conflict does not give an entity immunity from domestic laws. A good example of this can be found in Rule 20 on countermeasures: "hacking back" might be allowable under the Tallinn Manual, but that does not give any actor immunity from prosecution under the Computer Fraud and Abuse Act. *See* TALLINN MANUAL 2.0, *supra* note 5, at 111-116; *See* 18 U.S.C. § 1030. The contours of the CFAA may contain lack of clarity which might yield unexpected legal results, as it did in a recent Supreme Court opinion that cast serious doubt on "exceeds access" prosecutions under the Act; *See Van Buren V. United States*, 141 S. CT. 1648 (2021).

[8] *See* TALLINN MANUAL 2.0, *supra* note 5, at 552-62. (discussing various prospective scenarios in which one state could lawfully target the civilian infrastructure of another state).

[9] *See id.* at 301-72 (discussing the series of legal protections afforded to civilians and civilian objects during cyber operations or general armed conflict).

regarding cybersecurity risks to critical infrastructure, especially during heightened geopolitical tensions.

II. Background

A. Overview of the Tallinn Manual 2.0

The *Tallinn Manual 2.0* (the "Manual") is a treatise that restates the *lex lata*—the international law as it currently is—regarding cyber operations.[10] Both versions[11] of the Manual were developed by two groups of pre-eminent legal scholars in the area of the law of armed conflict and international law more generally, known as the International Group of Experts ("Group of Experts" or "Experts").[12] This version of the Manual sets forth the law regarding cyber operations in peacetime and incorporates the 2013 *Manual*'s work on wartime norms in 154 black letter rules with accompanying commentary.[13] This is no easy feat: few treaties pertain to this subject matter, *opinio*

---

[10] *Id.* at 3.

[11] The first version of the *Tallinn Manual* was developed in response to the widespread institutional as well as international confusion on how to understand cyber operations within the paradigms of the law of armed conflict. This first version was published in 2013. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael Schmitt ed., 2013). The reader should assume that this article is discussing the *Tallinn Manual 2.0* even if the text says merely "Tallinn Manual," except where specifically denoted that the discussion is referring to the 2013 version.

[12] *See* TALLINN MANUAL 2.0, *supra* note 5, at XII-XXII. The drafters of the Tallinn Manual constitute a group of well-qualified experts hailing from many nations, including the United States, Canada, Australia, Belgium, the Netherlands, the United Kingdom, and Sweden. Collectively, these experts are referred to in the Manual as the "International Group of Experts." For the *Tallinn Manual 2.0*, a new group of experts convened to articulate the rules regarding peacetime norms. In a way, the *Tallinn Manual 2.0* represents the vision of two distinct groups of legal scholars. Because each group was responsible for its own portions of the *Manual* and its own portion alone, it is not clear whether, and to what extent, there are differences of opinion between the different groups of experts. Perhaps this is an area of opportunity for clarification in a future *Tallinn Manual 3.0*.

[13] *See generally Tallinn Manual 2.0*. The original 2013 iteration of the *Tallinn Manual,* divided into two parts: Part A (a discussion of international cyber security law, but really pertaining to jus ad bellum), and Part B (a discussion of the law of cyber armed conflict or jus in bello). Between the two parts, there are seven chapters that pertain to subjects such as state acts in cyberspace, the protection of specific classes of persons, and the applicability of the law of armed conflict to acts within cyberspace. It is important to note that the Rules and the accompanying commentary highlight where there are majority and minority positions among the Group of Experts. Therefore, many of the rules and statements provided in the Manual are subject to disagreement among the Experts, and should be treated as guidelines rather than definitive statements of legality. *See Id. at* 4.

juris is sparse, and most state practice in this area cannot be readily examined.[14] Additionally, state practice in this area is not always even available to the public eye.[15] As a result, these black letter rules represent a Herculean effort by the Manual's drafters—the International Group of Experts[16]—to separate the legal "wheat from the chaff" in the face of the near-constant churn of international cyber operations. A word of caution, however: the ability of decision-makers must temper their expectations and reliance on what type of conduct the Manual proscribes because the Group of Experts reflects a largely Western legal perspective. While customary international law would bind all states, we cannot predict how non-Western governments might apply these legal rules to the still-developing field of cyber operations, so much remains uncertain.

B. *Definitions of* Key Te*rms*

As a threshold matter, there is some need to clarify a few relevant terms of art, if for no other reason that imprecise use of language tends to complicate legal analysis and policy discussion.[17] News media in particular have a tendency to make errors in using legal terms of art in the area of the law of armed conflict, which unnecessarily muddies the waters of this complex subject area.[18] For

---

[14] *See Id. at* 3-4; *See also* Scott Shackelford, *The Law of Cyber Peace*,18 CHI. J. INT'L L. 4 (2017) (utilizing various authorities, legal and otherwise, to apply international law in cyberspace, specifically below the threshold of an armed attack).
[15] *See* TALLINN MANUAL 2.0, *supra* note 5, at 3-4 (noting that the majority of state cyber practices and cyber operations are classified).
[16] *See Id.* at 5-6 (explaining that one of the Experts' goals was to articulate clearer rules applicable to cyber operations that were drawn from existing sources of international law).
[17] *See* JERROLD TANNENBAUM, *What is Animal Law*?, 61 CLEV. ST. L. REV. 891, 920 (2013) ("A shared definition of a word can make it possible for people to communicate about the thing, to learn about it, and to argue about what is or is not factually true about it, or about what ought or ought not to be done with it. However, although a good definition can allow such inquiry and argument, it is almost always the inquiry and argument about which people are primarily interested.")
[18] *See, e.g.*, TARA SIEGEL BERNARD, ET. AL., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, New York Times (Sept. 7, 2017) https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=3 (using the term "cyber attack" to characterize what happened to Equifax, even though there was no observable physical property damage, injury, or loss of life resulting from that attack.)

the purposes of this Article, two definitions are of the utmost importance: the definitions of "cyber attack" and "critical infrastructure."

First, the term "cyber attack", as used by the *Tallinn Manual*, specifically means any cyber operation[19] that is "reasonably expected to cause injury or death to persons or damage or destruction to objects."[20] Therefore, this definition requires at least some risk of injury, death, or property damage. As a result, the *Manual* indicates that data breaches—even massive ones like the recent Equifax hack[21]—are not by definition a cyber-attack under the *Manual's* interpretation of the law of armed conflict. In other words, financial or informational losses alone, no matter how grievous, are not enough to make a cyber operation into a cyber attack. Importantly, under this rule, the cyber attack itself—being comprised merely of ones and zeros traveling through cables—does not need to directly cause injury, death, or property damage. Ultimately, the definition of a cyber attack is fairly straightforward: the definition of an attack in cyberspace is functionally similar to an attack in the traditional three-dimensional kinetic space: both require violence of action.[22]

The definition of "critical infrastructure" is more complicated. *Tallinn Manual* defines 'critical infrastructure' as:

> Physical or virtual systems and assets of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment.[23]

---

[19] *See* TALLINN MANUAL 2.0, *supra* note 5, at 564 (stating that a "cyber operation" is defined as "the employment of cyber capabilities to achieve objectives in or through cyberspace").
[20] *Id.* at 415.
[21] *See* BERNARD, *supra* note 18, at 3-4.
[22] TALLINN MANUAL 2.0, supra note 5, at 415. *See also* GENEVA CONVENTIONS OF 1949, ADDITIONAL PROTOCOL I art. 49, JUNE 8, 1977, 1125 U.N.T.S. 27 (stating the original agreement for sovereignty as a rule of international law, although not all states are party to the agreement).
[23] TALLINN MANUAL 2.0, supra note 5, at 564. It is worth noting that the Experts did not convene *sua sponte*. Rather, the Cooperative Cyber Defense Center of Excellence of the North Atlantic Treaty Organization (NATO CCDCOE) invited both Groups of Experts to develop the *Tallinn Manual*. Importantly, the *Manual* does not reflect the official positions of NATO, NATO CCDCOE, or any other government involved with either body. *See Id.* at 1-2.

For comparison purposes, the United States' Defense Production Act of 1950 (or "DPA"), as amended, defines "critical infrastructure" as:

> [A]ny systems and assets, whether physical or cyber-based, so vital to the United States that the degradation or destruction of such systems and assets would have a debilitating impact on national security, including, but not limited to, national economic security and national public health or safety.[24]

There are a couple notable points of departure between these definitions. It is unclear, however, if these differences are significant. First, the *Tallinn Manual* definition indicates that critical infrastructure includes "physical and virtual" systems and assets, while the DPA definition uses "cyber-based" instead of "virtual." Second, the *Tallinn Manual* definition characterizes the requisite type of harm as "incapacitation or destruction" while the DPA definition uses "degradation or destruction." Perhaps this means that the definition under the DPA is somewhat broader, as assets could be degraded without necessarily being incapacitated: perhaps a loss of capacity, if severe enough in its effects, is enough to come within the DPA definition. Third, the scope of adverse harms differs slightly as well: the *Tallinn Manual* definition of critical infrastructure states that debilitation to a nation's "security, economy, public health or safety, or the environment" is required for an asset or system to be critical infrastructure. The DPA definition is substantially narrower: destruction or degradation of assets or systems must be debilitating to "national security" which includes "national economic security" and "national public health and safety." Additionally, other U.S. laws hew to the DPA definition, but vary slightly around the edges.[25]

---

[24] *See* 50 U.S.C. § 4552(2) (2020) ("The term "critical infrastructure" means any systems and assets, whether physical or cyber-based, so vital to the United States that the degradation or destruction of such systems and assets would have a debilitating impact on national security, including, but not limited to, national economic security and national public health or safety.").

[25] For example, the statutes governing the scope of the Committee on Foreign Investment in the United States (CFIUS) state use the DPA definition, except the type of harm to be avoided is limited to a "debilitating impact on national security," to include homeland security as well. *See* 50 U.S.C. § 2170(5-6). *See also* 42 U.S.C. § 5195c(e) (defining critical infrastructure for the purpose of public health and welfare in the United States). Of note, and certainly beyond the scope of this article, the Department of Defense Law of War Manual does not contain a discussion, much less a definition, of critical infrastructure. The DoD Manual adopts several approaches that differ from the Tallinn Manual in several respects, but a fulsome analysis is best deferred to others. *See* DEP'T OF DEF. LAW OF WAR MANUAL (2016).

Looking across the pond, the government of the United Kingdom defines critical infrastructure as:

> Critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.[26]

These definitions are united by a few key features: critical infrastructure are (1) objects that are so important that (2) some sort of damage would cause some level of (3) adverse consequences to (4) a valuable state interest. It is unclear if these are distinctions without differences, but this author contends that this is cause for further consideration outside the scope of this article.[27] For the purposes of the foregoing discussion in Part 3, this article uses the *Tallinn Manual* definition of critical infrastructure as a baseline.[28]

In any case, critical infrastructure, which by definition must provide vital services to society writ large, to both civilian and military efforts, forms the central focus of the analysis in Part 3 below, which seeks to answer the key question: 'what legal rules apply to cyber attacks against critical infrastructure?' This analysis mirrors the approach of US law, taking a sector-by-sector approach where the *Tallinn Manual* provides specific rules for a given sector.

---

[26] CTR FOR THE PROT. OF NAT'L INFRASTRUCTURE, CRITICAL NAT'L INFRASTRUCTURE (APRIL 20, 2021) https://www.cpni.gov.uk/critical-national-infrastructure-0 (last accessed March 17, 2018).

[27] This subject has been the topic of some discussion among the "Five Eyes" of Australia, Canada, New Zealand, the United Kingdom, and the United States. *See* CYBERSECURITY & INFRASTRUCTURE AGENCY., CRITICAL 5: FORGING A COMMON UNDERSTANDING FOR CRITICAL INFRASTRUCTURE (2014) *available at:* https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf. (last accessed March 18, 2018); By way of example, the United States recognizes sixteen (perhaps seventeen) critical infrastructure sectors, Australia recognizes seven, Canada recognizes ten, New Zealand recognizes five, and the United Kingdom recognizes thirteen. *See Id.* at 8-14; *see also* 6 U.S.C. § 601 (2020) (recognizing a seventeenth critical infrastructure sector, postal and shipping, for the United States).

[28] *See* TALLINN MANUAL 2.0, *supra* note 5, at 564 (defining "critical infrastructure" as "[p]hysical or virtual systems and assets of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment"); The *Tallinn Manual* definition, however, may not be authoritative. *See* TALLINN MANUAL 2.0, *supra* note 5, at 2 (stating that their work is not the official position of any one government).

III. Rules on Targeting Critical Infrastructure–a Sector-by-Sector Approach

With this understanding of the bounds of critical terminology, this Article now considers how the *Tallinn Manual's* restatement of the law of armed conflict may impact critical infrastructure.

A. Threshold Matters: Sovereignty, Civilian Status, and General Targeting Rules

The Manual provides some black letter rules about key aspects of the law of armed conflict as relevant to cyber operations, such as violations of sovereignty, the civilian status of objects and individuals. Rule 4 provides that international law prohibits states from violating the sovereignty of other states.[29] Importantly, cyber operations directed against privately-owned infrastructure can be considered a violation of state sovereignty, regardless of whether or not those cyber operations result in any effect on government-owned infrastructure.[30] This is significant because in the United States, the majority of critical infrastructure assets are owned or operated by private persons. But there is no bright threshold demarcating whether a given operation is a violation of sovereignty. Regardless of where that threshold lies, all of the Experts agreed that a cyber operation that "necessitat[es] repair or replacement of physical components of cyber infrastructure" or those operations that result in "physical damage or injury" would qualify as violations of state sovereignty.[31] Therefore, it is clear that a cyber operation that, for example, renders a computer hard-drive useless or that causes a printer to catch fire, even if such assets are privately owned, is a violation of sovereignty, whereas a distributed denial of service attack that causes an interruption or degradation of a network-based service might not be. While this area is unclear, the Group of

---

[29] *See* TALLINN MANUAL 2.0, *supra* note 5, at 17-27 (outlining states' international obligation not to violate the sovereignty of one another); The notion of sovereignty is as old as international law itself; *see also* UN CHARTER ART 2, PARA 1 (establishing that all states are equal for legal or juridical purposes and requiring that all states respect the territorial integrity and political independence of other states).
[30] *Id.* at 18 ¶ 5.
[31] *Id.* at 20-21.

Experts noted that many states are becoming increasingly concerned about cyber operations that result in "severe economic loss or that affect critical infrastructure."[32] Does this mean that critical infrastructure assets will receive different treatment from other assets *as a general rule* under the applicable international law? Possibly, but observers must wait and see how state practice and *opinio juris* develops on this issue. Critical infrastructure may be a different sort of target, but it is not quite clear whether that will change anything going forward. Still, this much is certain: under Rule 4, cyber operations conducted by states[33] against private entities and privately-owned assets can violate their state's national sovereignty and invoke the *Tallinn Manual*. The remedies available to respond to such a violation would depend upon the severity of the cyber operation and whether that level of severity would entitle the state on the receiving end to take some sort of action permissible under international law.[34] Nevertheless, the implications of Rule 4 are clear: if a state targets private critical infrastructure within another state, that is a violation of sovereignty and the target's national government would be entitled to respond accordingly.

Furthermore, Rules 94 and 99 provide—as a general rule—that targeting civilians and "civilian objects" is impermissible under the law of armed conflict.[35] According to Article 52 of the Additional Protocol I of the Geneva Conventions, civilian objects are those objects that are not military objectives, which are defined in turn as objects that, by their "nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization . . . offers a definite military advantage."[36] Therefore, under this formulation, some

---

[32] *Id.* at 25-26.
[33] Though there is a view that attacks conducted by non-state actors are violations of sovereignty, that view was not adopted by any of the Experts. *See id.* at 18 ¶ 3 (noting that none of the Experts believed that a non-state actor could violate the sovereignty of a state). As the Group of Experts formulates it, there is no violation of sovereignty unless a cyber operation is attributable to a State.
[34] For a discussion of some of these remedies, *see infra § 4.1*; *See Id.* at 312-330 (providing a general discussion of the principles of non-intervention and other prohibitions on interference in the affairs of another state in Rules 66-68).
[35] *Id.* at 422-23, 425-28.
[36] Additional Protocol I, Article 52.

critical infrastructure assets could be considered military objects. For example, a factory that manufactures cell phone batteries and serves both military and civilian customers could qualify as a military objective.[37] But if a given critical infrastructure asset does not make an "effective contribution" to the military effort, it may not be targeted. These are the general rules, to which there are exceptions.[38]

One exception to this general rule arises when targeting civilian infrastructure would fulfill a military objective and the loss of civilian life or property is proportional to the military advantage to be gained.[39] To illustrate this concept of proportionality with a general example, it would likely be impermissible under the law of armed conflict to conduct an air raid designed to bomb a small military garage if that attack would also destroy an adjoining apartment building that houses thousands of people. Similar rules could apply in cyberspace: for example, it could be impermissible to launch a cyber attack against a power plant in order to deprive a small military outpost of electricity if it would also cause a total black out in a wide geographic radius around the power plant.

The nature of information technology and communications infrastructure often means that the same wires, cables, and transmitters may serve both civilian and military customers, and it may be hard to tell what network traffic belongs to the military versus what traffic comes from grandmothers checking their social media accounts. Given this uncertainty and the high degree of damage that may result from indiscriminately targeting IT and communications infrastructure

---

[37] *See* TALLINN MANUAL 2.0, *supra* note 5, at 439 ("All of the Experts agreed that a factory that produces computer hardware or software under contract to the enemy's armed forces is a military objective by use, even if it also produces items for other than military purposes.").

[38] Additionally, even though critical infrastructure might be a valid military objective because its destruction or degradation may provide a military advantage, other rules included in the Tallinn Manual may provide additional protections for certain types of infrastructure. *See infra* §§ 3.3-3.5.

[39] *See* TALLINN MANUAL 2.0, *supra* note 5, at 470-76 (providing the parameters of a proportionality analysis, as required by Rule 113, and further stating that cyber attacks are prohibited if the attack would be expected to cause "incidental loss of civilian life, injury, or property damage" that is excessive in proportion to the military advantage to be gained).

wholesale, this author contends that the burden[40] is on the *attacker* to carefully assess the tactical situation in order to determine whether a given civilian object has become a permissible military target. But this is not a high bar under the rule: the Experts point out that certainty is not required, and so long as a commander has reasonable grounds to conclude that a civilian object has been converted for military use, it is a permissible target. Obviously, the civilian status of many potential targets of cyber operations may be unclear, especially in the heat of battle. Rule 102 of the *Tallinn Manual* requires that an attacker do "everything feasible to verify" that their objective is not a civilian object or otherwise subject to special protection.[41] Additionally, customary international law[42] directs commanders to "take feasible precautions" to minimize collateral damage when attacking military targets,[43] but doubts remain as to how far this obligation goes. For example, Rule 118 directs attackers to use methods that cause the least amount of damage to civilian infrastructure when considering several different military operations with the goal of achieving the same result.[44] But a sizable minority of the Group of Experts took the position that Rule 118 is not yet customary international law—therefore, states need only comply if they are parties to Additional Protocol I. Furthermore, a commander's obligation to "do the least harm" under Rule 118 does not require a commander to actually forgo attacking a valid target—even if it causes more collateral damage than attacking an alternative target—if attacking the alternate target would not achieve the same military advantage.[45] Consider a situation where a commander can choose to conduct a cyber attack either

---

[40] The question of who has the "burden" under Rule 102 was subject to some disagreement. *See id.* at (explaining that a majority of experts thought that a presumption of civilian use was customary international law, while others believed that such a position improperly shifted the burden from the defender to the attacker; *See id.* at 448-49 (discussing Additional Protocol I, Art. 52(2-3) and explaining the considerations made in determining which party has the "burden").
[41] *See* TALLINN MANUAL 2.0, *supra* note 5, at 449 ¶ 6 (referencing Rule 115, which states, "[attackers] must do everything feasible to verify that the objectives to be attacked are neither civilian objects nor subject to special protection").
[42] *Id.* at 480 (citing Additional Protocol I, Art. 57(2)(a)(ii)).
[43] *Id.* at 479-80.
[44] *Id.* at 481-82 (citing Additional Protocol I, Art. 57(3)).
[45] *Id.* at 482 ¶ 7.

against an enemy unit's communications system or against the electrical grid for the area in which the enemy unit is operating. Arguably, the military advantage conferred by attacking and disabling the electric grid is much more pervasive than just jamming the communications system. In the former case, the advantage may be fleeting—the unit could recover, or switch to an alternative or redundant backup system. In the latter case, the military advantage is near permanent—the enemy unit would be unable to restore communications without significant difficulty and would likely suffer from a persistently degraded quality of service.

The takeaway here is that critical infrastructure owners and operators and defending governments[46] should not assume that an attacker will refrain from attacking merely because there is significant doubt as to a target's civilian status.[47] Therefore, defenders should proceed under the assumption that when in doubt, an attacker will favor military expediency over certainty when resolving doubt as to status of objects,[48] and should assume that civilian infrastructure may be targeted if its status is unclear.

---

[46] This naturally raises questions about critical infrastructure that is part of a civilian government agency. For example, in the United States, several civilian agencies fulfill national security functions, such as the Department of Homeland Security or the Intelligence Community agencies. Civilian government infrastructure that can be used for military purposes can qualify as a military objective. *See id.* at 445-46 (stating that civilian infrastructure being used for both a military and civilian purpose will qualify as a permissible military objective). However, critical infrastructure that is part of a government's diplomatic mission is entitled to greater protection. States that host another state's diplomatic mission are required to "take all appropriate steps to protect the premises of a diplomatic mission against any intrusion." *Id.* at 213 ¶ 3 (referencing Rule 40, which states, "[a] receiving State must take all appropriate steps to protect cyber infrastructure on the premises of a sending State's diplomatic mission or consular post against intrusion or damage"). This duty extends far indeed under the Group of Experts' formulation: if the security services of a host state were to become aware of cyber operations directed against the diplomatic mission of a sending state, then the host state must "engage in all reasonable efforts to terminate the offending cyber operation." *Id.* at 217 ¶ 1.

[47] *See supra* note 46.

[48] A different calculus applies when targeting persons directly. *See generally* TALLINN MANUAL 2.0, *supra* note 5, at 424-32) (providing, *inter alia*, that civilians—including civilian employees of non-military government agencies—enjoy protected status unless they directly participate in hostilities); *See also* TALLINN MANUAL 2.0, *supra* note 5, at 406 § 14 (highlighting that even if cyber tools could qualify as "weapons" and thus be required to be carried openly under Rule 87, the rule would probably have "little application in the cyber context").

B. Specific Protections for Particular Types of Infrastructure

Even though these general rules apply to the targeting of critical infrastructure during an armed conflict, particular types of critical infrastructure may be entitled to additional protections under international humanitarian law.[49] This section explores these protections and analyzes the extent of their reach.

C. Distinctive Emblems and Unnecessary Suffering: Healthcare and Public Health Sectors

The protection of medical personnel and facilities ranks among the most fundamental and time-honored tenets of international humanitarian law.[50] The Group of Experts concludes that this customary norm applies in cyberspace as well: "medical . . . personnel, medical units, and medical transports . . . may not be made the object of a cyber attack."[51] But it is not enough for a combatant to merely refrain from attacking medical infrastructure, assuming that infrastructure is properly marked. International law requires combatants to "respect and protect" medical infrastructure and to avoid taking actions that would interfere with its function.[52] For example, the Group of Experts indicates that a cyber operation to misdirect a medical transport by altering GPS data would run afoul of the admonition to "respect" medical units.[53] A similar scenario could also include a ransomware attack on a hospital, depriving medical professionals access to patient information and essential computer systems. Such an operation might not rise to the level of an armed attack but

---

[49] *See id.* at 512-13 (providing that protections exist under international law for, inter alia, "[m]edical and religious personnel, medical units, and medical transports").
[50] *See Practice Relating to Rule 28* https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule28 (last visited August 2, 2018) (citing to the Hague Regulations, the Geneva Conventions, and dozens of national military manuals enshrining the principle of protecting medical units).
[51] TALLINN MANUAL 2.0 at 513.
[52] *Id.* at 514.
[53] *Id.* at 514 ¶ 5.

would still be unlawful under Rule 132 as identified in the *Manual*.[54] The Experts do identify one type of cyber-based intrusion that might be permissible: "cyber reconnaissance" that does not impair functionality of systems but is instead designed to gather information or intelligence.[55] Furthermore, in the case of a server that contains both military and protected medical data, such commingling of the data may mean that the server would lose its protected status. However, such commingling also becomes quite complicated for operators because many services, such as Software as a Service ("SaaS") providers support both military and civilian customers, so complex questions regarding the scope of permissible targets will persist. Nevertheless, an attacker would likely be required to issue due warning so the defender could take steps to ensure that the medical systems or data continue to receive protection under the law.[56]

In addition to these considerations, medical infrastructure is also covered by *Manual* Rule 104. Much like the requirement to protect medical units and transports, the rule against unnecessary injury, pain, and suffering has a long history in the law of armed conflict.[57] Humanitarianism undergirds this rule: while some death, injury and pain is inevitable in war—belligerent parties should nevertheless avoid making war worse than it needs to be by causing pain and suffering that otherwise serves no military purpose.[58] This principle has often taken the form of prohibitions on using certain types of weapons in war, such as blinding laser weapons and hollow point bullets.[59] In the context of cyber operations, the Group of Experts speculates that a cyberattack on an

---

[54] *See* Patrick Howell O'Neill, *Indiana Hospital Shuts Down Systems After Ransomware Attack*, Cyber Scoop (Jan. 15, 2018) https://www.cyberscoop.com/hancock-hospital-ransomware/ (describing a ransomware intrusion into a hospital's computer systems that caused disruption but neither shut down the entire hospital nor caused death or injury).
[55] TALLINN MANUAL 2.0, *supra* note 5, at 515 ¶ 2.
[56] *Id.* at 519 ¶ 5.
[57] *Id.* at 453 (citing the Hague Regulations, the Additional Protocol I and the Preamble to the 1868 St. Petersburg Declaration).
[58] *See generally* INTERNATIONAL COMMITTEE OF THE RED CROSS, *International Humanitarian Law Legal Fact Sheet* https://www.icrc.org/en/document/what-international-humanitarian-law (Apr. 6, 2022). ("International Humanitarian Law ("IHL") is a set of rules that seeks, for humanitarian reasons, to limit the injurious effects of armed conflict."
[59] *See generally* INTERNATIONAL COMMITTEE OF THE RED CROSS, *1980 Convention on Certain Conventional Weapons* https://www.icrc.org/en/document/1980-convention-certain-conventional-weapons.

individual's pacemaker inside the body may run afoul of the rule against unnecessary pain and suffering.[60] Thankfully, remotely targeting an individual's medical device through cyber means remains a mostly theoretical problem,[61] though one that may have lasting implications for the future of warfare.

D. Collateral Damage: Water & Wastewater Systems, Dams, Chemical Facilities, and Nuclear Sectors

Unlike medical infrastructure, other types of critical infrastructure could pose a tempting target to an attacker. For example, an attacker might try to damage a hydroelectric dam to deprive an enemy unit of electricity or to render a particular geographic location unusable or inaccessible due to flooding. Dams, dykes, and nuclear plants belong to a class of critical infrastructure assets to which special precautions apply under the law of armed conflict.[62] Experts disagree, however, as to how far these precautions extend. Article 56 of Additional Protocol I of the Geneva Conventions states that dams, dykes, and other critical infrastructure containing "dangerous forces" (such as large tanks of volatile, toxic chemicals) can never be attacked—no matter how vital the target—if it would cause

---

[60] TALLINN MANUAL 2.0, *supra* note 5, at 455. The question of whether a hackable pacemaker could be considered critical infrastructure is unsettled. An individual's medical device might not meet the definition of "critical infrastructure" under the *Manual's* formulation, but it might fall within other nations' definitions; The question of whether a given device or asset is critical infrastructure is not necessarily an idle inquiry. First, critical infrastructure assets may be eligible to receive specialized protection and other state services under a nation's domestic law. Second, the Group of Experts indicates that attacks on critical infrastructure might implicate other legal considerations. For example, they indicate that "temporarily suspending general access to the Internet may be permissible" in situations where there is a grave national security threat to critical infrastructure.

[61] *Cybersecurity*, U.S. Food and Drug Administration https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm (last visited August 10, 2018) (stating "[i]n each of the above cases, the FDA is not aware of any patient injuries or deaths associated with cybersecurity incidents, nor are we aware that any specific devices or systems in clinical use have been purposely targeted.").

[62] TALLINN MANUAL 2.0, *supra* note 5, at 529; *see also* Art. 56, Additional Protocol I. Interestingly, the Group of Experts does not believe that these special protections extend to other critical infrastructure assets that may release dangerous forces if attacked. In particular, the *Manual* calls out chemical plants and petroleum refineries as *not* within the bounds or Rule 140. It is unclear, however, why these precautions are limited to some types of critical infrastructure (dams) but not others (petroleum plants) even though "dangerous forces" can still be released in the latter case as well as the former. *See* AMW Manual, commentary accompanying Rule 36. For example, recent events have demonstrated that a loss of power or control over cooling units used in chemical facilities can lead to explosions. Jeff D. Colgan, *Harvey Caused a Chemical Plant Explosion. Is that the Next Face of Climate Change?*, Washington Post (Sept. 6, 2017) https://www.washingtonpost.com/news/monkey-cage/wp/2017/09/06/harvey-caused-a-chemical-plant-explosion-is-that-the-next-face-of-climate-change/?noredirect=on&utm_term=.b15e04f364bd.

"severe losses" among the civilian population; while the Group of Experts took a more limited position, requiring "particular care" when targeting such assets.[63] Because the introduction of malware into a computer system often involves some risk of unforeseeable or unanticipated consequences, Rule 140 of the *Manual* exhorts cyber-warriors to think long and hard before launching an attack that might have either some literal and figurative "downstream" effects. This is especially important given that malware has a way of spreading beyond its initial intended targets and impacting unrelated systems and assets.

E. Food and Agriculture Sectors

In addition to the heightened duty of care that belligerents must take in targeting civilian objects generally, an even more prescriptive rule applies to critical infrastructure that is "indispensable to the survival of the civilian population." Under *Manual* Rule 141, attacks on food and agricultural infrastructure and other critical items "indispensable to survival" are prohibited outright.[64] It may be difficult to think of circumstances under which a cyber attack might run afoul of this rule, but the Group of Experts state that cyber attacks that impair the function of critical infrastructure necessary for the maintenance of objects indispensable to the survival of the civilian population—like generators that keep vital food or medicine refrigerated—could run afoul of this Rule 141.[65] Perhaps this protection could extend to other circumstances as well—such as hacking into a motor vehicle's onboard computer so that its brakes fail and necessary shipments of food or medicine are destroyed in the resulting crash or are otherwise unable to reach their final

[63] GENEVA CONVENTIONS OF 1949, ADDITIONAL PROTOCOL I, Art. 56 ¶ 1.
[64] TALLINN MANUAL 2.0, *supra* note 5, at 531-32.
[65] *Id.* at 533.

destination.[66] Other consumables—such as those that may be found in the context of the U.S.'s "commercial facilities" civilian infrastructure sector—that are merely for the "comfort" of the civilian population would not enjoy this heightened protection but nevertheless receive all due protection as civilian objects under Rule 99.[67]

Furthermore, agricultural infrastructure might be entitled to some additional protections under the law of armed conflict. This is because the law of armed conflict prohibits cyber operations that are specifically designed to cause starvation to a civilian population, and the Manual incorporates this same principle into Rule 107.[68] While the Experts contend that it would take exceptional circumstances for cyber operations to violate Rule 107,[69] it is not difficult to envision a scenario where a cyber attack could result in the starvation of a civilian population, either through crippling the food supply chain[70] or by tampering with food processing equipment.[71]

Determining which types of critical infrastructure are entitled to which protections under international law is likely to depend on the facts of a particular scenario. Some relevant factors include the type of asset involved, how that asset is used, how the attacker will target the asset, and the type of effects arising from the actual cyber attack. Because of the factual complexities alluded to above and in the *Tallinn Manual* itself, it would be difficult to make predictive judgments about *in bello* cyber attacks against various categories of critical infrastructure beyond these broad

---

66 *Cf.* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired Magazine, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (July 21, 2015) (demonstrating the possibility for a malicious actor to remotely seize control of an automobile currently being driven).

67 TALLINN MANUAL 2.0, *supra* note 5, at 533 ¶ 4.

68 *See* Art. 54(1), Additional Protocol I; Art. 14, Additional Protocol II.

69 TALLINN MANUAL 2.0, *supra* note 5, at 460; *See generally* Food and Agriculture Sector-Specific Plan, U.S. Department of Homeland Security (2015) *available at*: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-food-ag-2015-508.pdf (providing only general details regarding cyber security risks to food and agriculture critical infrastructure and instead focusing primarily on cyber threats to federal agencies like the USDA or FDA).

70 *See* Thomas Fox-Brewster, *There's A Windows PC Helping Control Fleet Trucks -- Any Idiot Can Start Hacking It In 30 Seconds*, Forbes (Aug. 5, 2016) *available at:* https://www.forbes.com/sites/thomasbrewster/2016/08/05/windows-pc-truck-telematics-hack-def-con/#2bb948de4ab9 (explaining how a cyber attack directed at trucking could deprive an area of food for a significant period of time).

71 Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 Cal. L. Rev. 1079, 1110 (2013).

observations. In summary, the international law applicable to cyber operations makes clear that some types of critical infrastructure can be validly targeted, while other types of infrastructure are entitled to some higher level of protection that would require additional caution or due diligence on the part of an attacker. Hopefully this overview can assist owners and operators of critical infrastructure in better understanding the cybersecurity threat landscape and the conditions that may give rise to cyber attacks.

IV. Remedies for Cyber Operations: Tools in the Toolbox during Armed Conflict

Understanding that the *Tallinn Manual's* rules on *jus in bello* apply to critical infrastructure, this Part examines what tools may be available to the operators of critical infrastructure and the governments that defend them in order to counter a cyber attack. A close reading of the *Tallinn Manual* reveals a few courses of action that may be of use to decision-makers before, during, and after a cyber attack on critical infrastructure.

A. Precautionary Responsibilities of a Defending Party During an Armed Conflict

Considering what the *Manual* requires of defenders may be a helpful place to begin. As discussed above, the law of armed conflict subjects an attacking party to several obligations regarding the targeting of civilian infrastructure. But Rule 121 of the *Manual* sets forth what precautions are required to protect civilian populations and objects from the "dangers resulting from cyber attacks."[72] During armed conflict, defenders must take these precautions in order to protect civilian objects under their control from cyber attacks "to the maximum extent feasible."[73] This

[72] TALLINN MANUAL 2.0, *supra* note 5, at 487.
[73] *Id.*; Interestingly, some of the Group of Experts think that these defenders' duties apply to all cyber operations, and not just cyber attacks that rise to the level of a use of force. *see id.* at 488 ¶ 5.

indicates that the Group of Experts believe that defending governments cannot simply leave large swaths of civilian infrastructure unprotected during an armed conflict.[74]

Rule 121 also raises the issue of systems segregation. The Group of Experts suggests that segregating civilian and military systems and segregating *critical* systems from the Internet entirely are types of "passive precautions."[75] The *Tallinn Manual's* commentary, however, also recognizes that segregating critical infrastructure into critical and non-critical or civilian and military categories is a matter of nuance: a power plant might provide electricity to a military base as well as the town nearby.[76] In such circumstances, the Experts conclude that defending governments must still use other precautions to protect civilian objects. Ultimately, this course of mitigation confirms the thesis of this article: wartime targeting of civilian critical infrastructure is not only a possibility; it might be unavoidable in a world of commingled military and civilian infrastructure, especially if the belligerents are careless, aggressive, or patently cruel.

B. Distinctive Markings—Warning Potential Attackers of Protected Infrastructure

There is another type of precaution that defenders should consider under Rule 102. As noted above, civilian infrastructure can be lawfully targeted in several circumstances, including where the enemy suspects that a given civilian object has been converted to military use.[77] The standard for resolving a commander's doubt as to an object's status is not a high one: as noted above, a commander only needs to have "reasonable grounds to conclude" that a civilian objective has been converted to military use.[78] Because this analysis is conducted *ex ante*, one could assume that most

---

[74] *Id.* at 487 ¶ 1 (citing Article 58(c) of Additional Protocol I); According to the Group of Experts however, this obligation does not extend to a garden variety cyber operation, such as a Distributed Denial of Service (DDoS) attack or temporary alterations to or defacement of a company's website. *see id.* at 489-9 ¶ 9.
[75] *Id.* at 488 ¶ 3.
[76] *Id.* at 489 ¶ 7.
[77] *Id.* at 438-39.
[78] *Id.* at 449 ¶ 8; *see also supra* § 3.1.

commanders will resolve questions regarding status of objects in the interest of military expediency. The Experts exhort governments defending against cyber attacks to make this analysis more straightforward, reasoning that if an attacker can readily identify a civilian object, then there is a greater chance that the object may be spared from attack.[79] As a result, the Experts state that "defenders must facilitate an attacker's efforts to resolve the status [of] . . . hospitals, and places where the sick and wounded are 'collected' by means of distinctive markings or by notifying the attacker beforehand."[80] Perhaps these distinctive markings could take the form of a notice or banner that sits on the perimeter of critical infrastructure facilities' networks, warning all who would seek to penetrate those networks that doing so may run afoul of international law as restated in Rule 102. Obviously, such a banner is unlikely to deter the attack of a terrorist group or other non-state actor, but it might give pause to military commanders who seek to comply with the law of armed conflict.

Importantly, the use of these distinctive markings or "protective indicators"—whatever form they might take—must be done in good faith.[81] Defending governments should only use distinctive markings as preventative or precautionary measures and not to disguise permissible targets.[82] It is not permissible, under the law of armed conflict, to display the indicators, emblems, or insignia of protected organizations, neutral parties, or enemy parties for any use—including deception—other than which the indicator or insignia is designed.[83]

---

[79] *See id.* at 450 ¶ 9 (stating that certainty in targeting is not necessarily required, but rather, an attacker must conduct a careful assessment to determine whether there are reasonable grounds to conclude, based on reliable facts, that a specific infrastructure target is eligible for attack).
[80] *Id.* 451 ¶ 12.
[81] *See id.* at 496-98 (describing various examples of what the Experts refer to as "improper use" of protective indicators or markings). The specific rules on certain indicators apply to all activities and uses of indicators, whereas perfidy prohibits only causing injury or death.
[82] *Id.* at 496-504.
[83] *Id.* at 451-52.

C. Hitting Back in Peace and War: Stopping Communications, Necessity, and Self-Defense

This next section examines the more offensive capabilities that governments might employ if the precautionary measures taken above should fall short in the face of a cyber attack. These types of capabilities can be categorized and justified under several different labels: countermeasures (also known as "peacetime reprisals"), operations taken pursuant to a plea of necessity, operations suspending or stopping harmful communications, and operations taken under the self-defense. Each category is briefly discussed below, with an emphasis on its relevance to critical infrastructure.

Rules 20-26 govern how governments may be able to take countermeasures (either cyber or physical) in response to internationally wrongful acts committed against it by another state.[84] Countermeasures are actions that would otherwise be unlawful under international law, but are justified as a response to internationally wrongful acts.[85] These countermeasures fall between "belligerent reprisals," which ordinarily violate the law of armed conflict during peacetime (such as an armed attack) save some prior unlawful act by the attacking party, and acts constituting "retorsion," which are actions that are still lawful under international law but could be considered "unfriendly."[86] An example of a "belligerent reprisal" could be a commando raid on the source of a cyber attack, whereas a "countermeasure" could be a Distributed Denial of Service ("DDoS") attack against an attacking government's systems, while retorsion could be a suspension of communications by blocking certain IP addresses from accessing a network or website.[87] In circumstances where the offending cyber operation originates from non-state actors, Rule 26 of the *Manual* provides perhaps the only avenue for a defending government to use countermeasures in

---

[84] *See generally id.* at 111-42 (delineating the general rules of countermeasures, their specific parameters, and also the areas of disagreement both among the Experts and among states regarding the rules or parameters).
[85] *Id.* at 111 ¶ 1 (citing *Gabčikovo-Nagymoros judgment*, 1997 ICJ 7, ¶ 82-83 (25 September)).
[86] TALLINN MANUAL 2.0, *supra* note 5, at 112 ¶ 2-4.
[87] *Id.* at 112 ¶ 4.

response to a cyber operation falling short of an armed attack.[88] Rule 26 authorizes the use of countermeasures under a plea of necessity. Pleading necessity is difficult, but in a situation where a widespread cyber operation places critical infrastructure assets in imminent peril, a defending state may be able to invoke necessity in order to respond with countermeasures: such as a cyber operation against the network of a terrorist group that is located on another state's cyber infrastructure.[89]

States may also suspend or stop communications—seemingly any communications or the internet itself—that are contrary to its "national interest."[90] As a result, Rule 62 would support a government, when faced with a cyber attack on its own critical infrastructure, in suspending access to the internet in order to abate the possibility of a cyber attack coming from abroad. Other domestic and international laws, such as the First Amendment of the U.S. Constitution, might provide roadblocks to this course of action–at least in the United States.

Finally, and somewhat obviously, if a cyber operation rises to the level of an armed attack (a "cyber attack") and thereby shifting from peacetime to wartime norms, defending governments may employ the last resort: armed attacks undertaken in self-defense.[91] While self-defense in response to a cyber attack deserves its own full consideration,[92] there are a few observations worth making. First, even though an armed attack may come through cyberspace, there is no *per se* requirement that an

---

[88] *Id.* at 138 ¶ 11.

[89] *Id.* at 136-37 ¶ 4-6; Critical infrastructure, like power grids, banking systems, and air traffic control systems, are the type of "essential interests" that States are permitted to protect by undertaking operations under the plea of necessity.

[90] *Id.* at 293 (stating "[a] State's authority to suspend an international cyber communication service was illustrated by the Egyptian government's blocking of the international Internet and mobile telephony connections for several days in 2011 due to civil unrest").

[91] *Id.* at 339.

[92] *See, e.g.*, Oona A. Hathaway, Rebecca Crootof, William Perdue, and Philip Levitz, *The Law of Cyber-Attack*, 100 Calif. L. Rev. 817 (2012) (noting one argument that a cyber attack only evokes self-defense when it its severity is akin to an armed attack and its foreseeably causes physical injury or death); Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 Air Force L. Rev. 65 (2009) *Conflict* (explaining that employing self-defense is an effective response to a cyber attack and therefore can increase the deterrence of international law); Priyanka R. Dev, *"Use of Force" and "Armed Attack" Thresholds in Cyber*: *The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, 50 Tex. J. Int'l L. 379, 381, 389, 395 (2015) (noting that a state's lawful of self-defense is still governed by necessity and proportionality constraints); Terence Check, *Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict, a NATO-Centric Approach*, 63 Clev. St. L. Rev. 495, 507-08, 511 (2015) (noting several factors to be considered in determining if a state has the right to invoke self-defense).

armed response must also come through the other end of a fiber optic cable.[93] Additionally, the uncertainty of whether a given cyber operation is an armed attack is likely to be a limiting factor in a practical sense: If a state cannot easily determine when the remedy of self-defense becomes available due to difficulties in ascertaining whether a cyber attack has actually happened, states that are risk-averse will decline to engage in self-defense in borderline cases.[94] It is also worth noting that self-defense operations must otherwise conform to all other applicable legal requirements, such as necessity and proportionality.[95]

D. After the Fight and Before the Next One: Reparations and Special Agreements

After the dust settles, defending governments might seek to repair the damage suffered and to take steps to ensure that it does not happen again. Rules 28 and 29 of the *Manual* provide for some manner of reparations.[96] While reparations would likely be hard to enforce, in theory, states are liable for full reparation for injuries (public and private) suffered from a wrongful cyber operation, but only injuries that are foreseeable.[97]

Could governments agree, notwithstanding other international law, that certain types of targets—such as critical infrastructure—are off limits from cyber attack? The *Tallinn Manual* contemplates that the advent of specialized agreements that extend additional protections to particular types of infrastructure could increase the amount of protection beyond what is provided

---

[93] TALLINN MANUAL 2.0, *supra* note 5, at 340 ¶ 4.
[94] This fundamental uncertainty deserves fuller examination outside the confines of this essay, especially its impact on the decision-maker charged with determining how and when to launch an armed response.
[95] TALLINN MANUAL 2.0 at 348; *see also* TALLINN MANUAL 2.0, *supra* note 5, at 457 (requiring that when responding to an attack, a defending government must avoid countermeasures that are cyber-booby traps, or could be characterized as such).
[96] *Id.* at 144-152.
[97] *Id.* at 145-46, ¶¶ 5-7.

for under existing international humanitarian law.[98] However, so long as the prospect of targeting critical infrastructure through cyber space remains a strategically or tactically useful option, states might resist giving it up this capability.

V. Conclusion

Largely, the question of whether a given type of critical infrastructure is entitled to protection—in other words, whether cyber attacks directed at that piece of critical infrastructure may violate the law of armed conflict or other international law—is primarily based on two considerations: 1) the ultimate actual effects of that attack on the civilian population and 2) whether the critical infrastructure asset in question falls into one of the specific prescribed categories of specially protected infrastructure. As the *Tallinn Manual* shows, the *lex lata* of the law of armed conflict certainly indicates that critical infrastructure—including civilian critical infrastructure—can certainly become a target of a belligerent party during the conduct of hostilities. Nevertheless, the law of armed conflict places limits and prohibitions on attacks on some types of critical infrastructure. As this Article shows, it is difficult to make predictive judgments about what kind of critical infrastructure might be a permissible target of a cyber-attack, as definitions pose an interpretive challenge. Still, it is clear that there is some significant risk that a hostile actor might lawfully target critical assets and systems during an armed conflict. As noted above, the unpredictability of what might be "off limits" increases if additional perspectives are considered beyond just those of the primarily Western Group of Experts who composed the *Tallinn Manual*. Once governments and the owners or operators of critical infrastructure understand this inherent

[98] *Id.* at 512, (citing Claude Bruderlein, *Harvard Program on Humanitarian Policy and Conflict Research Manual on International Law Applicable to Air and Missile Warfare with Commentary* (2010), Art. 99); *see also* GENEVA CONVENTION OF 1949 Common Article 3, Aug. 12, 1949, 75 U.N.T.S. 86-88.

risk to their society's sensitive assets, the sooner they can begin to take steps to harden their systems and assets from cyber -attack and to weather potential geopolitical storms.