Classification of cyber capabilities and operations as weapons, means, or methods of warfare

INTERNATIONAL LAW STUDIES

Published Since 1895

Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare

Jeffrey T. Biller and Michael N. Schmitt

95 INT'L L. STUD. 179 (2019)

Volume 95

2019

Published by the Stockton Center for International Law

ISSN 2375-2831

Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare

Jeffrey T. Biller and Michael N. Schmitt***

CONTENTS

* Lieutenant Colonel, Judge Advocate General's Corps, U.S. Air Force; Military Professor and Director for the Law of Armed Conflict, Stockton Center for International Law, U.S. Naval War College.

** Howard S. Levie Professor, Stockton Center for International Law, U.S. Naval War College; Professor of Public International Law, University of Exeter; Francis Lieber Distinguished Scholar, U.S. Military Academy at West Point; Visiting Professor, University of Texas Law School; Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence.

The thoughts and opinions expressed are those of the authors and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

The development of cyber capabilities with the potential for operational use on the battlefield predates consideration as to how international law applies to this new form of warfare. Indeed, the first government assessment of cyber operations in armed conflict came in a 1999 analysis by the Office of the General Counsel at the U.S. Department of Defense, which warned, "[i]t will not be . . . easy to apply existing international law principles to information attack, a term used to describe the use of electronic means to gain access to or change information in a targeted information system without necessarily damaging its physical components."[1] In particular, the assessment pointed to "computer network attack, or in today's vernacular, the 'hacking' of another nation's computer systems."[2]

By then, strategists and operators had been thinking about "information warfare" for some time, with many heralding a "revolution in military affairs."[3] In 1998, the Joint Chiefs of Staff published *Joint Doctrine for Information Operations*, which began the complex process of developing a doctrinal framework for such operations.[4] As military structures and operations integrated cyber capabilities, the tendency was, and remains, "normalization," where practitioners incorporate terms and doctrine from existing military parlance and practice into the cyber context.[5]

---

1. OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 5 (1999), http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.

2. *Id.*

3. *See, e.g.*, CYBERWAR 2.0: MYTHS, MYSTERIES AND REALITY (Alan Campen & Douglas Dearth eds., 1998); CYBER WAR: SECURITY, STRATEGY, AND CONFLICT IN THE INFORMATION AGE (Alan Campen ed., 1996); MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE? (1995); MARTIN C. LIBICKI, THE MESH AND THE NET: SPECULATIONS ON ARMED CONFLICT IN A TIME OF FREE SILICON (1994); WINN SCHWARTAU, INFORMATION WARFARE: CHAOS ON THE ELECTRONIC SUPERHIGHWAY (1994); THE INFORMATION AGE: AN ANTHOLOGY ON ITS IMPACT AND CONSEQUENCES (David S. Alberts & Daniel S. Papp eds., 1977).

4. The term was defined as "[o]perations to disrupt, deny, degrade, or destroy information resident in computer and computer networks, or the computers and networks themselves." Joint Chiefs of Staff, Joint Pub 3–13, Joint Doctrine for Information Operations, at GL–5 (1998).

5. For example, U.S. military doctrine states, "Cyberspace attack actions are a form of fires, are taken as part of an OCO [offensive cyber operation] or DCO–RA [defensive cyber

The international legal community struggled, rather unsuccessfully, to maintain pace with both doctrinal development and technological advances. To lighten their load, most international lawyers also attempted to normalize their work, primarily through reasoning by analogy.[6] In particular, they tended to directly apply terms, concepts, and applications already resident in international humanitarian law (IHL), much as their operational brethren were doing with respect to operational concepts.

In most cases, this process generated acceptable results. However, certain concepts proved difficult to apply cleanly in the cyber context. For instance, the meaning of the word "attack" in IHL's conduct of hostilities rules remains unsettled when applied to cyber operations. Most significant in this regard is the prohibition on directing "attacks" against civilian objects that is found in Article 52(1) of Additional Protocol I to the 1949 Geneva Conventions[7] and relevant customary law,[8] for unless a cyber operation qualifies as an attack (or the targeted cyber infrastructure enjoys special protection), it arguably may be directed against civilian cyber infrastructure.[9] A related debate revolves around whether data is an "object" in IHL, such that a cyber operation that intentionally alters or deletes civilian data is unlawful and

operation-response action] mission, are coordinated with other USG departments and agencies, and are carefully synchronized with planned fires in the physical domain." Joint Chiefs of Staff, Joint Publication 3–12, Cyberspace Operations, at II–7 (2018) [hereinafter Joint Chiefs of Staff, Cyberspace Operations]. The *Department of Defense Dictionary of Military and Associated Terms* defines fires as "The use of weapon systems or other actions to create specific lethal or nonlethal effects on a target." DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 84 (As of June 2019), https:// www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2019–04–25–095717–503.

6. See, for example, the articles in 76 INTERNATIONAL LAW STUDIES (2002) resulting from the first major conference on the subject, Computer Network Attack and International Law, which was held at the U.S. Naval War College in 1999.

7. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 52(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

8. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW r. 7, at 25–29 (Jean–Marie Henckaerts & Louise Doswald–Beck eds., 2005) [hereinafter CIHL].

9. See the discussion in Michael N. Schmitt, *Rewired Warfare: Rethinking the Law of Cyber Attack*, 96 INTERNATIONAL REVIEW OF THE RED CROSS 189 (2014); *see also* Michael N. Schmitt, *Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations*, 102 INTERNATIONAL REVIEW OF THE RED CROSS (forthcoming 2019) [hereinafter Schmitt, *Wired Warfare 3.0*].

harm to civilian data in an otherwise lawful attack against a military objective would factor into proportionality and precautions in attack assessments.[10]

Further complicating matters is the fact that beyond the international law community terms may be used colloquially, or even described in official publications in ways that deviate from their legal meaning. For instance, "cyber attack" is defined in U.S. military doctrine as "actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires."[11] This definition is so broad that it would encompass some cyber operations that do not qualify as an "attack" as that term is defined by treaty in IHL—"an act of violence, whether in offence or defence."[12] Such disparities regularly generate confusion in discussions between the lay and legal communities regarding the law governing cyber operations.

This article examines three terms drawn from classic IHL—weapons, means, and methods of warfare—that are also being applied to cyber operations. The three terms are of particular significance with respect to the use of cyber capabilities during an armed conflict because they are integral to the various IHL prohibitions and obligations cataloged below. Whether those prohibitions and obligations apply depends on whether a cyber capability or cyber operation falls within the ambit of the term in question.

Interestingly, there has been little analysis of the terms as applied to cyber operations, at least among legal academics. We are of the view, however, that the tendency to normalize through reasoning by analogy, coupled with a lack of understanding of cyber operations from a technical perspective, may inadvertently have resulted in a flawed understanding of how the IHL governing weapons, means, and methods of warfare applies in the cyber context. To explain our concern, we begin by identifying those IHL rules with normative significance vis-à-vis weapons, means, and methods. We then assess the prevailing understandings as to the meaning of the terms when applied

10. *See, e.g.*, Heather A. Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISRAEL LAW REVIEW 39 (2015); Kubo Mačák, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law,* 48 ISRAEL LAW REVIEW 55 (2015); Michael N. Schmitt, *The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive Precision*, 48 ISRAEL LAW REVIEW 81 (2015); Schmitt, *Wired Warfare 3.0*, *supra* note 9.

11. Joint Chiefs of Staff, Cyberspace Operations, *supra* note 5, at GL–4.

12. AP I, *supra* note 7, art. 49(1).

to operations, including cyber operations, conducted during an armed conflict. Having laid this foundation, the core of the analysis follows, first with an examination of the defining characteristics of systems that scholars universally accept as weapons, means, and methods of warfare. Identifying a key commonality among these characteristics, we conclude that cyber capabilities cannot logically be categorized as weapons or means of cyber warfare. However, we find that in some circumstances cyber operations may qualify as a method of warfare. Finally, we apply our findings to the previously identified legal requirements to assess the extent to which they govern cyber capabilities and operations.

II. RELEVANT LAW

The determination of whether a cyber capability or operation qualifies as a weapon, means, or method of warfare bears on several key obligations that States shoulder under treaty and customary international law. First, certain requirements exist to review weapons, means, or methods of warfare for compliance with IHL and other legal regimes. Whether the "weapon review" obligations attach vis-à-vis cyber capabilities and operations depends on their legal characterization. Second, during an "attack," a term of art in IHL explained below, the attacking party is required to take precautions to minimize harm to civilians and civilian objects that includes choosing among means and methods of warfare. Again, the application of this obligation is tied to whether cyber capabilities and operations are means or methods of warfare. Finally, classification as a weapon, means, or method implicates prohibitions under the law of neutrality regarding the movement of munitions and supplies across the territory of neutral States.[13]

A. Legal Reviews of Weapons, Means, and Methods

It is a longstanding premise of international law that "[i]n any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited."[14] A key tool for operationalizing this premise is the re-

13. Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land art. 2, Oct. 18, 1907, 36 Stat. 2310, T.S. No. 540 [hereinafter 1907 Hague Convention No. V].

14. AP I, *supra* note 7, art. 35(1); *see also* Regulations annexed to Convention No. II with Respect to the Laws and Customs of War on Land art. 22, July 29, 1899, 32 Stat. 1803, T.S.

quirement to review weapons or means (or methods for some States) of warfare for compliance with IHL and other international law norms. Never has that obligation loomed larger, for as one commentator has observed, "the duty to systematically review the legality of weapons is of particular importance today in light of the rapid development of new weapons technologies, such as remote-controlled drones and increasingly autonomous robots, cyber capabilities, nanotechnology, and the militarization of space."[15]

In treaty law, the duty to conduct a legal review is set forth in Article 36 of Additional Protocol I. That provision provides,

> [i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[16]

It is unclear to what extent, if at all, Article 36 reflects customary international law. The voluminous International Committee of the Red Cross (ICRC) study on customary IHL contains no such obligation.[17] However,

---

No. 403 [hereinafter 1899 Hague Convention No. II Regulations]; Regulations annexed to Convention No. IV Respecting the Laws and Customs of War on Land art. 22, Oct. 18, 1907, 36 Stat. 2227, T.S. No. 539 [hereinafter 1907 Hague Convention No. IV Regulations]; Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects pmbl., Oct. 10, 1980, 1342 U.N.T.S. 137 [hereinafter Conventional Weapons Convention]; Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti–Personnel Mines and on Their Destruction pmbl., Sept. 17, 1997, 2056 U.N.T.S. 211; Convention on Cluster Munitions, pmbl., May 30, 2008, 2688 U.N.T.S. 39; Treaty on the Prohibition of Nuclear Weapons pmbl., *opened for signature* Sept. 20, 2017 (adopted July 7, 2017, not yet in force), 52 INTERNATIONAL LEGAL MATERIALS 350 (2018).

15. NILS MELZER, INTERNATIONAL HUMANITARIAN LAW: A COMPREHENSIVE INTRODUCTION 299 (2016). For general guidance on the reviews, see INTERNATIONAL COMMITTEE OF THE RED CROSS, A GUIDE TO THE LEGAL REVIEW OF NEW WEAPONS, MEANS AND METHODS OF WARFARE (2006).

16. AP I, *supra* note 7, art. 36.

17. CIHL, *supra* note 8. It has been suggested that the obligation to conduct a legal review of new weapons may derive from the Martens Clause, which first appeared in the preamble to 1899 Hague Convention No. II and was subsequently reaffirmed in 1907 Hague Convention No. IV, as well as Additional Protocol I and Additional Protocol II. *See* MELZER, *supra* note 15, at 299; *see also* Convention No. II with Respect to the Laws and Customs of War on Land pmbl., July 29, 1899, 32 Stat. 1803, T.S. No. 403 [hereinafter 1899 Hague Convention No. II]; Convention No. IV Respecting the Laws and Customs of War

the experts who prepared the 2013 *HPCR Manual on International Law Applicable to Air and Missile Warfare* took the position that the requirement to conduct a legal review of weapons (which they classified as a category of means of warfare) before fielding them is customary in nature.[18] However, they found there to be insufficient State practice to conclude that an analogous customary law obligation applies to methods of warfare or that the duty to conduct reviews attaches during the "study, development, acquisition or adoption" of the weapons.[19]

As to cyber capabilities and operations, the International Group of Experts (IGE) that prepared *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* came to similar conclusions. It drew upon both Article 1 of the 1907 Hague Convention IV and Common Article 1 of the 1949 Geneva Conventions to find a customary law requirement to "ensure that the cyber means of warfare that they acquire or use comply with the rules of the law of armed conflict that bind them."[20] The former requires Parties to issue instructions to its land forces that are consistent with "the laws and customs of war,"[21] whereas the latter requires that the High Contracting Parties to the

---

on Land pmbl., Oct. 18, 1907, 36 Stat. 2227, T.S. No. 539 [hereinafter 1907 Hague Convention No. IV]; AP I, *supra* note 7, art. 1(2) ("In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience."); Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non–International Armed Conflicts pmbl., June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II]. The International Court of Justice opined in its *Nuclear Weapons* advisory opinion that the Martens Clause reflects customary international law and that it "has proved to be an effective means of addressing the rapid evolution of military technology." Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 226, ¶ 78 (July 8). However, in our view, deriving a distinct obligation to review means and methods of warfare where no specific treaty obligation exists is questionable, even in light of the Martens Clause.

18. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH AT HARVARD UNIVERSITY, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE 84 (2013) [hereinafter AMW MANUAL].

19. *Id.* With regard to the customary nature of the weapon review obligation, the experts noted that the requirement to assess their legality prior to fielding was "longstanding," pointing to Article 1 of 1899 Hague Convention No. II, which references Article 23(e) of its accompanying Regulations. *Id.* Likewise, they note the identically numbered provisions of 1907 Hague Convention No. IV and its accompanying Regulations. *Id.*

20. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS r. 110(a), at 464–67 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

21. 1907 Hague Convention No. IV, *supra* note 17, art. 1.

four 1949 Geneva Conventions "respect and ensure respect" for the Conventions.[22] For the IGE, this necessarily meant that the legality of "cyber weapons" must be reviewed prior to acquisition or use. The group was divided over whether the obligation stretches further in the direction of Article 36, and specifically, whether it applies to cyber methods of warfare and whether the obligation attaches during the cyber weapon acquisition or development phase.[23]

It appears, then, that the contemporary prevailing view is that the customary law legal review obligation applies to at least means of warfare and attaches before they are fielded.[24] States Party to Additional Protocol I are obligated beyond these requirements by the terms of Article 36. Note that States not a Party to the Protocol may adopt policy requirements more demanding than customary law.

Significant in this regard is the United States, especially considering its advanced cyber capabilities. The U.S. approach to weapon reviews is set forth in the Department of Defense (DoD) *Law of War Manual*.[25] It requires a review of weapons or weapons systems before acquisition or procurement for compliance with IHL obligations, other international law obligations of the United States, and any applicable domestic law.[26] Regulatory guidance issued by the DoD to the individual services implements this requirement.[27]

---

22. Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 1, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 1, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention (III) Relative to the Treatment of Prisoners of War art. 1, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 1, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

23. TALLINN MANUAL 2.0, *supra* note 20, at 465.

24. *But see* Natalia Jevglevskaja, *Weapons Review Obligation under Customary International Law*, 94 INTERNATIONAL LAW STUDIES 186 (2018).

25. OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL § 6.2 (rev. ed., Dec. 2016) [hereinafter DOD LAW OF WAR MANUAL].

26. *Id.*

27. U.S. Department of Defense, Directive 5000.1, The Defense Acquisition System ¶ E1.1.15, at 7 (2018)

> The acquisition and procurement of DoD weapons and weapon systems shall be consistent with all applicable domestic law and treaties and international agreements . . . . An attorney authorized to conduct such legal reviews in the Department shall conduct the legal review of the intended acquisition of weapons or weapons systems.

For service regulations, see Headquarters, Department of the Army, Army Regulation 27-53, Review of Legality of Weapons Under International Law (1979) [hereinafter Army

In its manual, the DoD states that the policy extends to "weapons that employ cyber capabilities to ensure that they are not per se prohibited by the laws of war," but cautions that "[n]ot all cyber capabilities . . . constitute a weapon or a weapon system."[28] To illustrate the requirement, the *Law of War Manual* cites a legal review during acquisition or procurement of a weapon employing cyber capabilities to ensure it is not indiscriminate. It then observes, "a destructive computer virus that was programmed to spread and destroy uncontrollably within civilian Internet systems would be prohibited as an inherently indiscriminate weapon."[29]

Note the use of the term "weapon," which suggests that, for the DoD, a destructive cyber capability is a weapon, whereas a non-destructive or non-injurious capability is not. Unfortunately, the *Manual* fails to describe the type of "destruction" conceived of in the provision.[30] As a result, this distinction and the criteria driving it are far from apparent. Moreover, it must be emphasized that the legal review requirement reflected in the *Manual* is set forth as a matter of policy, not law.

Of particular relevance to "cyber capabilities" is the U.S. Air Force's 2018 regulation, *The Law of War*. It requires the Air Force to "conduct[] legal reviews of all weapons, weapon systems and relevant cyber capabilities, acquired or modified by the Air Force to ensure compliance with the law of war, domestic law, and international law at the earliest stage possible in development (prior to procurement or acquisition)."[31] Interestingly, the Air Force addresses weapons and cyber capabilities separately throughout the document, which further states, "[c]yber capabilities are neither weapons nor nonlethal weapons, as defined and stated in DoD Directive 3000.03E."[32]

Regulation 27-53]; Secretary of the Navy, SECNAV Instruction 5000.2E, Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System (2011); Secretary of the Air Force, Air Force Instruction 51-401 (2018) [hereinafter Air Force Instruction 51-401].

28. DOD LAW OF WAR MANUAL, *supra* note 25, § 16.6.

29. *Id.*

30. *Tallinn Manual 2.0* includes certain losses of functionality in the notion of damage. TALLINN MANUAL 2.0, *supra* note 20, at 417.

31. Air Force Instruction 51-401, *supra* note 27, ¶ 5.

32. *Id.*, attachment 1. The Instruction provides, "An Air Force cyber capability requiring a legal review prior to development or acquisition is any device, computer program or computer script, including any combination of software, firmware or hardware intended to deny, disrupt, degrade, destroy or manipulate adversarial target information, information systems, or networks." *Id.*

Although the exact meaning of this comment is unclear, it raises the possibility that, at least for the U.S. Air Force, cyber capabilities are not coextensive with weapons and therefore would not necessarily be subject to the same legal requirements and limitations that apply to the latter.

It is not our purpose to resolve the issue of the scope of the legal review requirement. Rather, our question is more fundamental. Given the nature of cyber capabilities and operations, do they legally qualify as a weapon, means, or method of warfare under IHL such that they are subject to review in the first place, whatever position a State might take on the scope issue? If so, and depending on the scope of the obligation, an assessment against numerous prohibitions, the violation of which would render the capability or operation unlawful in certain situations or even per se, is necessary.

Although a detailed discussion of these prohibitions is beyond the scope of this article, a degree of context is useful. A long-standing IHL rule prohibits the employment of "weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering."[33] The prohibition traces its lineage to the 1868 St. Petersburg Declaration,[34] recurs in numerous early IHL treaties,[35] and finds contemporary expression in Article 35(2) of Additional Protocol I. It is a prohibition that has unquestionably acquired customary status.[36] Of more modern vintage is the prohibition on methods or means of warfare that "are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment." Found in Article 35(3) of Additional Protocol I,[37] this rule is not accepted as customary by a number of key States, including the United States,[38] although the ICRC considers it as such.[39] Should cyber capabilities or operations qualify as a weapon, means, or method of warfare, they would

33. AP I, *supra* note 7, art. 35(2).

34. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Nov. 29/Dec. 11, 1868, 138 Consol. T.S. 297, 18 MARTENS NOUVEAU RECUEIL (ser. 1) 474.

35. *See, e.g.*, 1899 Hague Convention No. II Regulations, *supra* note 14, art. 23(e); 1907 Hague Convention No. IV Regulations, *supra* note 14, art. 23(e).

36. CIHL, *supra* note 8, r. 70, at 237–44.

37. AP I, *supra* note 7, art. 35(3).

38. DOD LAW OF WAR MANUAL, *supra* note 25, § 6.10.3.1 (citing Mark Simonoff, Minister Counselor, U.S. Mission to the United Nations, Remarks at the 70th U.N. General Assembly, Sixth Committee on the Report of the International Law Commission on the Work of its 67th Session (Nov. 11, 2015)); 2015 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW ch. 7, §D(2), at 287; United States, Statement on Ratification of the CCW, Accepting Protocols I & II, Mar. 24, 1995, 1861 U.N.T.S. 482, 483.

39. CIHL, *supra* note 8, r. 45, at 151–58.

be subject to these prohibitions, which States would optimally identify during the afore-mentioned legal review process.

For cyber capabilities, the more likely obstacle is the prohibition on indiscriminate weapons, a ban residing in both treaty and customary international law. Weapons can be unlawful on this basis in two ways. First, a method or means of warfare is prohibited by Article 57(4)(b) of Additional Protocol I and customary law if it "cannot be directed at a specific military objective."[40] In other words, the system cannot be aimed at a military objective with sufficient confidence that it will strike the target. The classic example is the German V-2 rocket of World War II, for its guidance system was so rudimentary that hitting a military objective was almost a matter of luck. Second, a method or means of warfare is unlawful under Article 57(4)(c) of Additional Protocol I and customary law if it generates uncontrollable effects that do not sufficiently discriminate between lawful military objectives and civilian objects or the civilian population.[41] Here, an illustration would be an air-delivered persistent chemical, for its spread would be subject to wind currents and other meteorological phenomena, and thus place the civilian population at uncontrollable risk.

These prohibitions must be distinguished from those that encompass the unlawful *use* of a lawful means or method of warfare. For instance, the most basic IHL prohibition is on the use of otherwise lawful weapons, means, or method of warfare to target civilians, civilian objects, and other protected persons and objects.[42] Similarly, it would be unlawful to fail to aim them at a military objective.[43] An example would be the dropping of bombs or firing of artillery into an area without regard for whether protected persons or objects will be harmed. We are not concerned here with these prohibitions, for they are dependent upon the consequences that manifest from the use of the cyber capability or operation rather than their qualification as a weapon, means, or method of warfare.

B. The Requirement of Feasible Precautions in Choice of Means and Methods

The second IHL rule potentially implicated by categorization as a weapon, means, or method is the Additional Protocol I, Article 57(2)(a)(ii) requirement that an attacker "[t]ake all feasible precautions in the choice of means

40. AP I, *supra* note 7, art. 51(4)(b); CIHL, *supra* note 8, r. 12, at 40–43.
41. AP I, *supra* note 7, art. 51(4)(c); CIHL, *supra* note 8, r. 12, at 40–43.
42. AP I, *supra* note 7, arts. 51(2), 52(1); CIHL, *supra* note 8, rr. 1, 7, at 3–8, 25–29.
43. AP I, *supra* note 7, art. 51(4)(a); CIHL, *supra* note 8, rr. 11, 12(a), at 37–43.

and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects,"[44] an obligation that is customary in nature.[45] In other words, an attacker must consider the various alternatives for achieving a desired effect in the battlespace and select the one that results in the least collateral damage from among those yielding the same or similar effect. "Feasible" options are widely understood as referring to those measures that are "practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations."[46] Textually, it is clear that the requirement to take this precaution only applies in situations causing the type of harm set forth in the rule itself and not, for example, inconvenience, irritation, or fear. All such situations qualify as "attacks" under IHL,[47] and therefore the reference to means or methods "of attack" as distinct from means or methods "of warfare" does not bear on the rule's applicability.

The DoD *Law of War Manual* illustrates the taking of feasible precautions to avoid civilian harm by citing "weaponeering (e.g., selecting appropriate weapons, aim points)."[48] Although the *Manual* does not employ the terms means or methods, its reference to "appropriate weapons" implicates the requirement to select from among alternative means of warfare, whereas aim point selection implicates methods of warfare. Thus, it is apparent that, at least by the DoD interpretation, the requirement of choice includes weapons, means, and methods.

Cyber operations offer an alternative to a kinetic attack that can sometimes reduce the potential for injury to civilians or damage to civilian objects. However, because the rule only applies to means and methods of attack,

---

44. AP I, *supra* note 7, art. 57(2)(a)(ii).

45. CIHL, *supra* note 8, r. 17, at 56–58; *see also* DOD LAW OF WAR MANUAL, *supra* note 25, § 5.11. The *Law of War Manual* notes that the obligation is legal in character. *Id.* at 250 n.336 (citing Exec. Order No. 13,732, 3 C.F.R. 13,732 (July 1, 2016)).

46. Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as Amended on 3 May 1996 art. 3(10), May 3, 1996, 2048 U.N.T.S. 93, 133; United Kingdom Statement made upon Ratification of Additional Protocols I and II ¶ (b) (July 2, 2002), *reprinted in* DOCUMENTS ON THE LAW OF WAR 510 (Adam Roberts & Richard Guelf eds., 3d ed. 2000); CIHL, *supra* note 8, at 54.

47. For the definition of attack in IHL, see AP I, *supra* note 7 art. 49. On attacks in the cyber context, see TALLINN MANUAL 2.0, *supra* note 20, r. 92, at 415–20. Note that even if no qualifying damage occurs to the target of a cyber operation, any indirect or collateral damage resulting from the cyber operation will qualify it as an attack subject to the requirement to take precautions. *Id.* at 418–19.

48. DOD LAW OF WAR MANUAL, *supra* note 25, § 5.11.

qualification of a cyber capability or operation as such is a condition precedent to its application in the cyber context. Note that even if they fail to qualify, the Additional Protocol I requirement to take "constant care . . . to spare the civilian population"[49] would compel States Party to use an available cyber option if doing so minimizes harm to civilians and civilian objects, does not require the sacrifice of military advantage, and turning to that option is feasible in the circumstances. Even though these obligations overlap in practice, a party to the conflict will not be in breach of its obligation to choose among means and methods of warfare to avoid civilian harm unless the cyber capability or operation qualifies as a means or method; otherwise, its use will only violate the broader constant care requirement.

C. The Prohibition on Movement of Munitions across Neutral Territory

The third area of law potentially implicated by categorization as a weapon, means, or method is the law of neutrality. This body of law serves to balance the interests of belligerents in effectively prosecuting an armed conflict with those of States that are not a party to the conflict in minimizing the conflict's impact upon their real and legal persons, their activities, and their territory. In doing so, it imposes corresponding rights and obligations on both belligerents and neutrals. For instance, it prohibits belligerents from using neutral territory as a base of operations against their adversary, thereby respecting the right of neutrals to exclusive control over their territory, as well as the right to be free from the effects of hostilities.[50] Neutral States have an obligation to put an end to any activities related to the conflict (belligerent rights) occurring on their territory.[51] Should a neutral State fail to comply with this duty, the aggrieved party to the conflict may take action to do so itself.[52]

---

49. AP I, *supra* note 7, art. 57(1); CIHL, *supra* note 8, r. 15, at 51–55. On the nature of the obligation, see Michael N. Schmitt & Michael Schauss, *Uncertainty in the Law of Targeting: Towards a Cognitive Framework,* 10 HARVARD NATIONAL SECURITY JOURNAL 148, 178–80 (2019).

50. 1907 Hague Convention No. V, *supra* note 13, art. 1; Convention No. XIII Concerning the Rights and Duties of Neutral Powers in Naval War arts. 1–2, Oct. 18, 1907, 36 Stat. 2415, T.S. No. 545 [hereinafter 1907 Hague Convention No. XIII]; *see also* DOD LAW OF WAR MANUAL, *supra* note 25, § 15.5.

51. 1907 Hague Convention No. V, *supra* note 13, art. 5; TALLINN MANUAL 2.0, *supra* note 20, r. 152, at 558–60; *see also* DOD LAW OF WAR MANUAL, *supra* note 25, § 15.5.

52. *See* DOD LAW OF WAR MANUAL, *supra* note 25, ¶ 15.4.2; UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 1.43(a) (2004) [hereinafter UK LOAC MANUAL]; TALLINN MANUAL 2.0, *supra* note 20, r. 153, at 560–61.

In treaty law, the rules of neutrality are set forth in the 1907 Hague (V) Convention for land conflict and the 1907 Hague (XIII) Convention for maritime warfare.[53] They are generally considered reflective of customary international law.[54] In the context of qualification as a weapon, means, or method of warfare, the relevant provision of the former is Article 2, by which "[b]elligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power."[55] Because, as explained below, the term "munitions" logically includes the terms "weapons" and "means" in the contemporary context, the question is whether this prohibition extends to the transmission of cyber capabilities through the cyber infrastructure of a neutral country.[56]

The fact that there is no analogous position in Hague Convention XIII should not be interpreted as suggesting that there is no maritime context to the prohibition. Assuming solely for the sake of analysis that Article 2 encompasses the transmission of malware across neutral territory, there is no reason to exclude its applicability to submarine communication cables passing through the territorial sea of a neutral coastal State for use in land warfare. Nor should it be presumed that the prohibition applies only to the transit of weapons for use in land combat merely because Hague Convention V is limited to that domain. The customary law analog to Article 2 is best interpreted as prohibiting the transit of weapons across neutral territory irrespective of domain. This understanding is consistent with the object and purpose of the prohibition, especially since air warfare did not exist at the time, and maritime weapons would typically have been transported by sea outside the territorial sea of coastal states, which then extended only three

53. 1907 Hague Convention No. V, *supra* note 13; 1907 Hague Convention No. XIII, *supra* note 50.

54. Eric Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INTERNATIONAL LAW JOURNAL 816, 819–20 (2012).

55. 1907 Hague Convention No. V, *supra* note 13, art. 2; *see also* DOD LAW OF WAR MANUAL, *supra* note 25, § 15.5.

56. On the law of neutrality in the cyber context, see Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INTERNATIONAL LAW STUDIES 123 (2013); Allison Gaul, *Neutrality in the Digital Battle Space: Applications of the Principle of Neutrality in Information Warfare*, 29 SYRACUSE SCIENCE AND TECHNOLOGY LAW REPORTER 51 (2013); Jensen, *supra* note 54; Wolff Heintschel von Heinegg, *Neutrality in Cyberspace*, *in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 35 (Christian Czosseck, Rain Ottis & Katherina Ziolkowski eds., 2012).

nautical miles seaward.[57] This narrows the issue to whether States may transmit malware through cyber infrastructure located in the maritime or land territory of a neutral State.

The DoD raised "[t]he issue of the legality of transporting cyber 'weapons' across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of 'overflight rights'" in its 2011 Defense Cyberspace Policy Report to Congress.[58] It accepted the applicability of the prohibition, noting that "[t]he law of armed conflict and customary international law, however, provide a strong basis to apply such norms to cyberspace governing responsible state behavior" and "the development of norms for state conduct does not require a reinvention of customary international law nor render existing norms obsolete." [59] The DoD acknowledged that "[t]he interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains" and observed that "[t]here is currently no international consensus regarding the definition of a "cyber weapon."[60] Thus, it concluded, "DoD, in conjunction with other U.S. Government departments and agencies, will continue to work with our partners and Allies to build consensus on the applicability of norms in cyberspace to develop customary international law further."[61] Although leaving open the question of the legality of transmitting cyber capabilities across neutral territory, the report accurately identified the problems: determining whether cyber capabilities are weapons and, if so, the applicability of the prohibition thereto.

There are two camps, both of which were represented within the *Tallinn Manual 2.0* IGE. By the first view, embraced by a majority of the experts, Article 2 prohibits the transmission of "cyber weapons" through neutral territory. As explained below, all of the experts characterized malware as a weapon, and thus those experts in the majority reasoned that the prohibition necessarily applies to malware, whether carried intact (for example, on a memory stick) or transmitted in a communication across neutral cyber infrastructure.

---

57. 2 UNITED NATIONS CONVENTION ON THE LAW OF THE SEA 1982: A COMMENTARY ¶ 3.2, at 77 (Satya N. Nandan & Shabtai Rosenne eds., 1993).

58. U.S. DEPARTMENT OF DEFENSE, DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT 8 (2011).

59. *Id.* at 8–9 (citing WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011)).

60. *Id.* at 8.

61. *Id.* at 9.

These experts noted that malware is typically broken into packets upon transmission, such that the cyber weapons are not intact when transmitted. Indeed, only a portion of packets might cross neutral territory on their way to reassembly at the targeted infrastructure. For proponents of the approach, this technical reality posed no obstacle to the application of Article 2. They pointed out that the prohibition would unquestionably apply to the transport of individual components of a weapon across neutral territory and could identify no reason to treat "components" (packets of data) of a cyber weapon differently.

Should Article 2 apply to cyber capabilities, the neutral State would bear a corresponding obligation to put an end to their transit across its territory. Of course, this obligation would be conditioned on that State having constructive or actual knowledge of the transmission and possessing feasible means to terminate it.[62] If the State were either unwilling or unable to terminate the wrongful transmission of the malware through its cyber infrastructure, the aggrieved belligerent would have the right to take those actions necessary to terminate it, including through the use of force.[63]

Concerned that this interpretation of neutrality law would effectively prohibit many military cyber operations that States would be likely to deem necessary and therefore inappropriately skew the balance between neutral and belligerent rights and obligations, a minority of the *Tallinn Manual 2.0* IGE adopted a different understanding of the law. These experts pointed to Article 8 of Hague Convention V, which states, "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[64] Note that the provision is not limited to belligerent communications lacking military value. They reasoned, therefore, that malware is best analogized to a communication (Article 8) rather than a tangible weapon (Article 2). It might be a communication of great military value, but Article 8 provides a specific exception for all belligerent communications.

In our estimation, the latter approach is a better fit to the reality of cyber hostilities. An attacker may not have full control over the path taken by the malware packets to the intended target, and in most circumstances, the neutral State is unlikely to effectively identify those packets passing through its

62. TALLINN MANUAL 2.0, *supra* note 20, at 559.

63. *Id.*

64. 1907 Hague Convention No. V, *supra* note 13, art. 8; *see also* DOD LAW OF WAR MANUAL, *supra* note 25, § 16.4.1; TALLINN MANUAL 2.0, *supra* note 20, at 558–59.

cyber infrastructure, at least in the current state of the technology. This understanding comports with the premise that an interpretation of law logically should allow for its enforcement. The 2016 U.S. *Law of War Manual* endorsed this approach, thereby resolving the question DoD had raised in its 2011 *Cyberspace Policy Report*.[65]

It must be cautioned, however, that the aforementioned rights and obligations, whatever their scope, depend on qualification of the cyber capability transmitted across neutral territory as a weapon or means of warfare. As will become apparent, that qualification is not a foregone conclusion.

III. DEFINITIONS OF WEAPONS, MEANS, AND METHODS

Given that the involvement of a weapon, means, or method is the *sine qua non* element in the rules above, one might expect the terms to be well defined in international law. This is far from the case. Despite persistent claims that determination of what constitutes a weapon, means, or method is a "relatively straightforward process,"[66] divergent views and approaches exist. These differences are examined below in an attempt to distill the key criteria for qualification as one of the categories in the contexts set out above.

A. Treaty Definitions

As noted, references to weapons, means, and methods appear in Article 35 and Article 36 of Additional Protocol I. However, the drafters were somewhat inconsistent, for Article 35 refers to "methods or means of warfare," as well as "weapons, projectiles and material and methods of warfare,"[67] while Article 36 uses the phrase "weapon, means or method of warfare."[68] In any event, the treaty defines none of these terms. Nor are the *travaux préparatoires* on the provisions of much help. They note that "[n]o effort was made . . . to define either term, and the choice of words should, perhaps, be considered further by a drafting committee."[69] Instead, the delegates to the

65. DOD LAW OF WAR MANUAL, *supra* note 25, § 16.4.1.

66. Justin McClelland, *The Review of Weapons in Accordance with Article 36 of Additional Protocol I*, 85 INTERNATIONAL REVIEW OF THE RED CROSS 397, 404 (2003).

67. AP I, *supra* note 7, art. 35.

68. *Id.* art. 36.

69. 15 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS, GENEVA (1974–1979), at 369 (1978) [hereinafter OFFICIAL RECORDS].

Conference discussed whether to include the word "methods" in the treaty articles, for they realized doing so "would make an important change in the law and that this should not be done without further careful consideration."[70] Although this finding supports the proposition that the customary law requirement for legal reviews does not extend to methods of warfare, it has no bearing on the question at hand—the meaning of the terms.

Article 2 of Hague Convention V does not use the terms weapons or means, but rather the phrase "munitions of war" and the term "supplies."[71] Both are undefined. Article 7, which deals with export and transportation by a neutral State, distinguishes arms from munitions of war, suggesting that munitions is a narrower concept that refers to the destructive aspect as distinct from the entity that launched it. However, the reference to supplies would render the distinction meaningless in terms of the substantive prohibition, as supplies would self-evidently encompass arms. This interpretation is supported by Article 14, which provides that neutral powers may permit the passage of the sick and wounded over their territory "on the condition that the trains carrying them shall carry neither personnel nor war material."[72] Again, the reference to war materials suggests a broad interpretation of the prohibition.[73] But, as with Additional Protocol I, Hague Convention V offers no assistance towards identifying any particular characteristics of the term munitions, a problem that did not arise in 1907 when the plain meaning of the term "arms" would include, for instance, rifles and artillery, whereas munitions would encompass, relatedly, bullets artillery shells.

No other treaties, including the Conventional Weapons Convention,[74] provide guidance on the meaning of the terms at hand. Therefore, it is useful to consider how States have interpreted them in practice, especially with respect to the guidance that they give to their armed forces.

B. State Definitions

State definitions of weapons, means, and methods, found primarily in military manuals, offer some help in understanding use of the terms. In its discussion of weapon reviews, the U.S. Navy, U.S. Marine Corps, and U.S.

---

70. *Id.*

71. 1907 Hague Convention No. V, *supra* note 13, art. 7.

72. *Id.* art. 14.

73. A. PEARCE HIGGINS, THE HAGUE PEACE CONFERENCE AND OTHER INTERNATIONAL CONFERENCES CONCERNING THE LAWS AND USAGES OF WAR 291 (1909).

74. Conventional Weapons Convention, *supra* note 14.

Coast Guard's *Commander's Handbook on the Law of Naval Operations* defines "weapons and weapons systems" to which it extends the requirement of a review, as "all arms, munitions, materiel, instruments, mechanisms, devices, and those components required for their operation, that are intended to have an effect of injuring, damaging, destroying, or disabling personnel or property, to include nonlethal weapons."[75] In the same context, the U.S. Air Force explains that a weapon is a "device designed to kill, injure, disable or temporarily incapacitate people or destroy, damage, disable or temporarily incapacitate property or materiel."[76] The U.S. Army similarly includes "[c]hemical weapons and all conventional arms, munitions, materiel, instruments, mechanisms, or devices which have an intended effect of injuring, destroying, or disabling enemy personnel, materiel, or property"[77] within the ambit of its weapon review requirement. As to the prohibition of transport across neutral territory, the *Commander's Handbook* does not use the words "munitions" or "weapons," opting instead for "troops or war materials and supplies."[78] Interestingly, the DoD's *Dictionary of Military and Associated Terms* includes no entry for weapon, means of warfare, or method of warfare.[79] While the latter two terms are legal terms of art, the inclusion of which might not be expected, the absence of a definition of weapon is noteworthy.

Among other States, Australia had previously defined weapons as "an offensive or defensive instrument of combat used to destroy, injure, defeat or threaten. It includes weapon systems, munitions, sub-munitions, ammunition, targeting devices, and other damaging or injuring mechanisms."[80] The explanation notes that a "computer expressly designed as a new weapon to offensively target enemy computer systems for destruction is covered."[81]

The Australian Defence Force replaced the instruction containing the above definition with interim guidance that refers to its *Defence Legal Review*

75. U.S. NAVY, U.S. MARINE CORPS & U.S. COAST GUARD, NWP 1-14M/MCTP 11-10B/COMDTPUB P5800.7A, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS § 9.1 (2017) [hereinafter THE COMMANDER'S HANDBOOK].

76. Air Force Instruction 51-401, *supra* note 27, ch. 1.

77. Army Regulation 27-53, *supra* note 27, ¶ 3(a).

78. THE COMMANDER'S HANDBOOK, *supra* note 75, § 7.3.1.

79. DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS, *supra* note 5.

80. Department of Defence, DI(G) OPS 44-1, Legal Review of New Weapons ¶ 3 (2005) (Austl.) [hereinafter Legal Review of New Weapons].

81. *Id.* ¶ 3 n.2.

of New Weapons Guide.[82] The *Guide* provides the following definitions, which are of particular significance because Australia is a Party to Additional Protocol I, and therefore the definitions represent that State's understanding of the meaning of the terms in Article 36. It defines weapon as, "[a] device, whether tangible or intangible, designed or intended to be used in warfare to cause: a. injury to, or death of, persons; or b. damage to, or destruction of, objects," and means of warfare as "[w]eapons or weapon systems."[83] Finally, it defines methods of warfare as "[t]he way or manner in which weapons and weapon systems are to be used."[84]

Denmark provides a definition similar to that of the United States, explaining that the term weapons refers to "inter alia, conventional weapons, chemical, biological, and bacteriological weapons, ammunition, weapons systems, delivery systems, platforms, and instruments designed to kill, destroy, injure, or in any other way incapacitate or render *hors de combat* personnel and equipment."[85] Notably, Denmark added incapacitation as an effect that qualifies an instrument as a weapon. However, it is unclear if the notion of incapacitation applies only to people or to equipment as well.

Canada merely discusses incendiaries, booby-traps, land mines, nuclear weapons, rockets, missiles, bombs, and torpedoes in its section on lawful weapons.[86] As to unlawful weapons, Canada includes poison, non-detectable fragments, environment altering weapons, gas, biological and chemical weapons, riot control agents, and blinding lasers.[87] Similarly, the United Kingdom does not define weapons, but rather provides an illustrative list that includes biological weapons, bayonets, swords, booby-traps, chemical weapons, dum-dum bullets, explosive bullets, fragmentation, incendiaries, landmines, lasers, nuclear weapons, non-lethal weapons, and poison.[88] There is no suggestion that the list is exhaustive.

---

82. Department of Defence, Interim Defence Instruction, DI Admin 44-1, Legal Review of New Weapons ¶ 3 (2018) (Austl.) (referring to Directorate of Operations and Security Law, Defence Legal Division, Australian Defence Force, Defence Legal Review of New Weapons Guide (n.d.)).

83. Directorate of Operations and Security Law, Defence Legal Division, Australian Defence Force, Defence Legal Review of New Weapons Guide 1 (n.d.).

84. *Id.*

85. DANISH MINISTRY OF DEFENCE, MILITARY MANUAL ON INTERNATIONAL LAW RELEVANT TO DANISH ARMED FORCES IN INTERNATIONAL OPERATIONS 336 (2016).

86. CHIEF OF THE GENERAL STAFF (CANADA), LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS, B-GJ-005-104/FP021, ¶¶ 520–29 (2001).

87. *Id.* ¶¶ 508–19.

88. UK LOAC MANUAL, *supra* note 52, ch. 6.

Interesting, the United Kingdom has recently followed the U.S. Air Force example by using the term "cyber capabilities" instead of cyber weapon. In its 2018 Ministry of Defence doctrine publication *Cyber and Electromagnetic Activities*, there is only one mention of cyber weapons.[89] All other associated references are to cyber capabilities. The UK Concepts and Doctrine Centre likewise refers to cyber capabilities in its *Cyber Primer*.[90]

C. Unofficial Definitions

Unofficial treatment of the terms weapons, means of warfare and methods of warfare tend to mirror those proffered by States. The ICRC *Commentary on the Additional Protocols* distinguishes means and methods but does not address weapons separately. The commentary to Article 35, which addresses superfluous injury or unnecessary suffering, as well as the environment, provides, "[t]he words 'methods and means' include weapons in the widest sense, as well as the way in which they are used. The use that is made of a weapon can be unlawful in itself, or it can be unlawful only under certain conditions."[91] The commentary to Article 36, which contains the weapons review provision, provides no explanation of the terms "weapon, means or methods of warfare," although the text is framed primarily in terms of "weapons" and their "normal use."[92]

Similarly, the Article 57 commentary focuses on "weapons," despite requiring a choice among means and methods.[93] Finally, when discussing Article 51(4)(b) and Article 51(4)(c), which prohibit an attack that is indiscriminate either because the means or methods used cannot be directed or their effects are uncontrollable, the *Commentary* provides, "[t]he term 'means of combat' or 'means of warfare' . . . generally refers to the weapons being used, while the expression 'methods of combat' generally refers to the way in

89. DEVELOPMENT, CONCEPTS AND DOCTRINE CENTRE, UNITED KINGDOM MINISTRY OF DEFENCE, JDN 1/18, CYBER AND ELECTROMAGNETIC ACTIVITIES 35 (2018).

90. DEVELOPMENT, CONCEPTS AND DOCTRINE CENTRE, UNITED KINGDOM MINISTRY OF DEFENCE, CYBER PRIMER 5 (2d ed. 2016) ("Defence cyber capabilities can be a combination of hardware, firmware, software and operator action.").

91. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 1402 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) [COMMENTARY ON THE ADDITIONAL PROTOCOLS].

92. *See id.* ¶¶ 1463–82.

93. *Id.* ¶¶ 2200–02.

which such weapons are used."[94] Throughout the *Commentary*, it is clear that the term "means" includes "weapons."

Importantly, although the ICRC *Commentary* tends to speak of methods as the manner in which weapons are employed, the term is clearly broader. This is apparent in the Additional Protocol I Article 54 and customary law prohibition on using starvation as a method of warfare.[95] The commentary to Article 54 explains, "[s]tarvation is referred to here as a method of warfare, i.e., a weapon to annihilate or weaken the population."[96] Despite the term "weapon," the better interpretation of the provision is that annihilation or weakening of the civilian population by deprivation of food and other essentials refers to a method that does not depend on the use of a weapon. The significance of the point that methods of warfare do not require the use of a weapon is discussed below.

In 2013, the Geneva Academy of International Humanitarian Law and Human Rights launched its *Weapons Law Encyclopedia*, an online compilation of information on the regulation of weapons under public international law. Echoing the prevailing understanding, the *Encyclopedia* observes that while "[t]here is no definition of a weapon under international law,"[97] a working definition is that a

> weapon is a device that is constructed, adapted, or used to kill, injure, disorient, or threaten a person or to inflict damage on a physical object. A weapon may act through kinetic energy or by other means, such as transmission of electricity, diffusion of chemical substances or biological agents or sound, or direction of electromagnetic energy.[98]

The *Encyclopedia* suggests, "[t]he term 'means of warfare' generally describes the weapons being used by parties to an armed conflict in the conduct of hostilities."[99] By contrast, it suggests methods of warfare "generally describes the way in which weapons are used by parties to an armed conflict in

94. *Id.* ¶ 1957.

95. AP I, *supra* note 7, art. 54(1); AP II, *supra* note 17, art. 14. On starvation and cyber operations, see TALLINN MANUAL 2.0, *supra* note 20, r. 107, at 459–60.

96. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 91, ¶ 2090.

97. GENEVA ACADEMY OF INTERNATIONAL HUMANITARIAN LAW AND HUMAN RIGHTS, WEAPONS LAW ENCYCLOPEDIA, www.weaponslaw.org/glossary/weapon (last visited July 1, 2019) [hereinafter WEAPONS LAW ENCYCLOPEDIA].

98. *Id.*

99. *Id.*, Glossary, "means of warfare."

the conduct of hostilities."[100] The latter definition is overly restrictive, as it excludes methods, such as starvation, not requiring the use of weapons.

Another important collaborative project in the field of international humanitarian law, the *Manual on International Law Applicable to Air and Missile Warfare* (*AMW Manual*),[101] sets out its own set of definitions. According to the *AMW Manual*, a weapon is

> a means of warfare used in combat operations, including a gun, missile, bomb or other munitions, that is capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects."[102] Means of warfare is broader, for it also encompasses the platforms and equipment which make possible an attack.[103]

An additional note of consequence is that the *Manual* describes munitions as being "a narrower concept than 'weapon' and refers to the object that causes the injury, death, damage or destruction."[104] Thus, the *Manual* explains, some weapons are also munitions, such as bombs delivered from an aircraft.[105] If a munition requires an object to deliver the force necessary for delivery, such as a gun or artillery, then that component constitutes a weapon, but not the munition itself.[106] By contrast, "methods of warfare consist of the various general categories of operations, such as bombing, as well as the special tactics used for an attack, such as high altitude bombing."[107] They are not limited to the manner in which weapons, or other means of warfare, are employed.

Tallinn Manual 2.0 also addresses the terms. It explains that a weapon is "generally understood as that aspect of the system used to cause damage or destruction to objects or injury or death to persons," and characterizes both weapons and weapon systems as means of warfare.[108] For the Tallinn 2.0 experts, a "cyber means of warfare" encompasses "cyber weapons and their

100. *Id.*, Glossary, "method of warfare."
101. AMW MANUAL, *supra* note 18.
102. *Id.* r. 1(ff), at 49–50.
103. *Id.* r. 1(t), at 31–32.
104. *Id.* r. 1(ff), at 49–50.
105. *Id.* r. 1(ff), cmt. ¶ 4, at 50.
106. *Id.*
107. *Id.* r. 1(v), at 34–35.
108. TALLINN MANUAL 2.0, *supra* note 20, at 452.

associated cyber systems,"[109] including "any cyber device, material, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack."[110] Methods of cyber warfare are "the cyber tactics, techniques, and procedures by which hostilities are conducted."[111] The term "refers to how cyber operations are mounted, as distinct from the means used to mount them."[112]

IV. TOWARDS AN UNDERSTANDING OF THE TERMS

The imprecision and overlapping nature of the various explications of munitions, weapons, weapon systems, means, and methods set forth above render conclusive definitions of these terms elusive. Nevertheless, from the survey of the various treaties, commentaries, *travaux préparatoires*, State definitions and lists, and unofficial manuals, a taxonomy enabling the application of legal prohibitions and requirements to cyber capabilities and cyber operations emerges.

To begin, the interpretive situation is not as complex as it might initially appear, for the various terms can be divided into two broad categories. On the one hand, there are munitions, projectiles, weapons, weapons systems, and means of warfare. On the other hand, there are methods of warfare. This binary approach corresponds to that found in the ICRC *Commentary*.[113]

It is unlikely that the relevant treaties contemplated a distinction between the terms in the first category. Article 36 and Article 57 of Additional Protocol I, as well as Article 2 of Hague Convention V, were self-evidently meant to be read expansively, with the same legal prohibitions and obligations attaching to each of the terms. Secondary sources usefully attempt to establish logical delineations thereof. The various manuals, in particular, approach the issue by treating terms such as munitions and projectiles as a subcategory of weapons, which are themselves either equivalent to, or a subcategory of, means of warfare.[114] Doing so is logical and appropriate.

Weapon systems comprise military equipment that, while not weapons themselves, have functions that are integral to the operations of a weapon,

109. *Id.* r. 103(a), at 452–53.

110. *Id.* at 452.

111. *Id.* r. 103(b), at 452–53.

112. *Id.* at 453.

113. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 91, ¶ 1957.

114. AMW MANUAL, *supra* note 18, r. 1(ff), at 49–50; TALLINN MANUAL 2.0, *supra* note 20, at 452–53.

such as a radar that guides a weapon to the target or a missile transporter, erector, or launcher. They are systems specifically designed for effectuating an attack using the weapon in question. That being so, it would be logically impossible to have a weapon system that was not designed to employ a weapon. Weapon systems qualify as a means of warfare.[115] By contrast, a standard truck fitted with a rocket launcher or filled with explosives for a suicide attack is not a weapon system, as the truck was not designed to facilitate such attacks. In none of the sources surveyed were the terms substantively distinguished. Accordingly, it is appropriate to treat the term "means of warfare" as encompassing both weapons and weapon systems, therefore the terms will be used interchangeably.

Means of warfare stand in contrast to methods of warfare. The latter do not comprise equipment, but rather the tactics, techniques, and procedures (TTP) for carrying out military operations involving the conduct of hostilities.[116] Indeed, starvation and the use of human shields are both methods of warfare prohibited by international law,[117] but neither necessarily requires the use of a means of warfare to be carried out. This distinction between means and methods in part explains the concern of some participants in the Additional Protocol I negotiations that the reference to methods in various provisions imposed legal requirements going beyond those attaching to means of warfare.[118]

A. A Survey of Damage Mechanisms

Having distinguished between methods and means, it remains necessary to identify the required characteristic(s) for qualification as a means of warfare and assess whether cyber capabilities can qualify, and be subject to the legal prohibitions and obligations that attach as a result. At surface level, it might appear that tangibility is the key. After all, tangibility is signaled by the terms typically used in discussions of means—weapon, device, equipment, material, arm, munition, instrument, mechanism, and so on.

Yet tangibility has been rejected by some commentators in the cyber context, most notably the *Tallinn Manual 2.0* experts. They included software

115. AMW MANUAL, *supra* note 18, r. 1(ff), cmt. ¶ 2, at 50; TALLINN MANUAL 2.0, *supra* note 20, at 452.

116. AMW MANUAL, *supra* note 18, r. 1(v), cmt. ¶ 2, at 34; TALLINN MANUAL 2.0, *supra* note 20, r. 103(b), at 452–53.

117. CIHL, *supra* note 8, rr. 53, 97, at 186–89, 337–40.

118. 15 OFFICIAL RECORDS, *supra* note 69, at 369.

that is designed to conduct a "cyber attack" in their illustration of the term means of warfare.[119] For them, the defining characteristic was not tangibility, but the consequences that are incident to the use of a means of warfare. If those consequences qualify use of the cyber capability as a "cyber attack," as IHL employs that term, the "device, material, instrument, mechanism, equipment, or software" under consideration is a means.[120] In that regard, the experts understood a cyber attack as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[121] They treated a loss of functionality that requires repair of the system or is permanent as damage, although the experts were unable to achieve further consensus on the classification of other types of consequences.[122]

This leads to a second possible distinguisher of means of warfare: direct causation. Here, examples include a direct causal connection between the means of warfare and physical damage to objects, the permanent loss of functionality of an object, or injury to persons.[123] Design intent is essential in this regard. Consider a rock used to strike an enemy soldier during hand-to-hand combat. The rock causes the qualifying consequences, but it is not designed to do so. As a result, it is not a weapon (means of warfare) in the IHL sense. By contrast, a small club crafted with the specific intent of use for striking someone is a weapon. Absent this requirement of design intent, the notion of means of warfare would become so overbroad as to preclude meaningful application of the relevant legal prohibitions and requirements.

The condition of design intent to injure, kill, damage, or destroy necessitates that the instrument of harm has some damage mechanism that causes the requisite consequence. Damage mechanisms need not be complex, or even mechanical (as with poison), but their intended use must be to cause harm. Mechanisms of definitively categorized weaponry include blunt force, penetration, blast, fragmentation, heat, fire, electrical, electromagnetic,

119. TALLINN MANUAL 2.0, *supra* note 20, r. 92, at 415–20.

120. *Id.* at 452–53.

121. *Id.* at 415.

122. *Id.* at 417–18.

123. The exception is the outdated Australian definition, which includes an "instrument of combat" used to "defeat or threaten" the enemy. *See* Legal Review of New Weapons, *supra* note 80, ¶ 3.

sound, radiation, chemical, and biological.[124] By identifying the characteristic(s) common to all damage mechanisms utilized by instruments accepted as weapons, it is possible to tease loose the essence of a means of warfare. To do so, key damage mechanisms are reviewed below.

Blunt force: In all likelihood, the earliest tools used by humans to engage in combat were blunt-force objects. Whether the first weapon was a branch, rock, or another type of blunt-force tool, the purpose of its use was to inflict greater damage than the attacker's body could achieve through striking, kicking, biting, and the like. Modern examples of blunt-force weapons include the baton and truncheon.

Blunt-force damage results from the transfer of mechanical energy, which is a form of kinetic energy, from the weapon to the target when the weapon accelerates toward the target. When the weapon and the target come into contact, energy transfers to the weaker of the two entities.[125] This transfer of kinetic energy from the object to its target is "terminal" in the sense that the damage mechanism is capable of directly causing the damage without an intermediary mechanism or action.

Penetration: Some damage mechanisms are intended to penetrate or perforate their target, as with a bayonet or a bullet. Penetration weapons are effective because the force employed is so concentrated that the weapon enters the target, as opposed to simply contacting it. However, like blunt force weapons, the transfer of mechanical energy produces the damage. Penetration weapons can be combined with other damage mechanisms to cause additional harm after penetration of the protective layer. For example, "bunker busting" bombs are designed to cause damage first by penetrating a protective layer, the bunker, and then producing blast and fragmentation effects inside it.[126] As with blunt force, the penetration damage mechanism itself delivers a terminal effect, that is, it causes the actual harm with no intermediary necessary.

---

124. STUART CASEY-MASLEN & STEVEN HAINES, HAGUE LAW INTERPRETED 18 (2018). See also the explanations of various weapons in the *Weapons Law Encyclopedia*. WEAPONS LAW ENCYCLOPEDIA, *supra* note 97.

125. *See* MCGRAW HILL ENCYCLOPEDIA OF PHYSICS 523 (Sybil P. Parker ed., 1983) (discussing Newton's third law of motion).

126. Although developed as far back as World War Two, the bunker buster achieved prominence during Operation Desert Storm with the GBU-28. This weapon and its progeny use a short-delay time fuse to allow the weapon to penetrate the target before detonating.

Blast/fragmentation: The third type of damage mechanism that employs the transfer of kinetic energy is blast/fragmentation. Although blast and fragmentation are separate mechanisms, they typically occur in tandem. Blast damage is the result of a shock wave produced by overpressure resulting from the detonation of an explosive. The shock wave consists of highly compressed air particles moving at a high rate of velocity.[127] Kinetic energy stored in the shockwave is then transferred to the targeted person or object. Damage may also be caused by the movement of air that floods into the vacuum created by the initial blast and from the heat given off as a byproduct of the explosion.

The shell casing or objects within the shell inflict fragmentation damage when they are propelled outward by the force of the explosion. Secondary fragmentation results as objects unassociated with the device are struck by the blast wave or initial fragmentation and then carried along behind the blast wave, causing additional damage. The detonation of the shell directly causes all these effects; they are therefore, terminal effects.

Heat/fire: Damage from heat results from the transfer of thermal energy, which is also a kinetic energy damage mechanism. Thermal energy is the movement of particles within a system and is transferred when two systems of differing temperatures contact one another. Transfer occurs because the systems attempt to achieve thermal energy equilibrium.[128] Damage occurs when the target system cannot cope with the increased thermal energy, as with the burning of the skin.

In weapons, the thermal energy typically transfers through thermal radiation, as opposed to direct contact, convection, or conduction. Thermal radiation, commonly referred to as heat, consists of electromagnetic waves emitted from the heat source.[129] Battlefield damage from heat is typically produced by an explosive, with a rise in temperature occurring along the flow direction of a shock wave.[130] However, certain weapons, such as the flamethrower and munitions containing napalm use heat as the primary damage mechanism. In these cases, the ignited flammable liquid spreads out over the target, causing a direct transfer of thermal energy, as opposed to radiated

127. MCGRAW HILL ENCYCLOPEDIA OF PHYSICS, *supra* note 125, at 1047.
128. *Id.* at 422.
129. *Id.* at 424
130. *Id.* at 1047.

energy. Whatever the method of heat transfer, it is the thermal energy produced by the weapon and transmitted to the target through thermal radiation that directly produces the terminal effect.

Electrical: Some weapons employ electricity as the damage mechanism, as with a "Taser,"[131] which delivers an electric current through electrodes fired at the target. The current disrupts voluntary control of muscle systems, with the intended effect of temporarily incapacitating the target. Like the previously described damage mechanisms, the passage of electrical current involves the transfer of energy.[132] The primary effect on the body is involuntary muscle contractions, resulting from the electricity overwhelming the nervous system's natural electrical impulses.[133] Although most often designed as nonlethal weapons, some can deliver a lethal dose of electricity. As with the previously described damage mechanisms, the electricity causes the terminal effect, which is the loss of muscle system control.

Electromagnetic and sound: In 1962, the Atomic Energy Commission launched a PGM-17 Thor that detonated a 1.45-megaton thermonuclear warhead at an altitude of two hundred fifty miles.[134] The detonation generated an electromagnetic pulse (EMP) that, in addition to disrupting electrical and phone service in Hawaii one thousand miles away, damaged orbiting communications satellites.[135] The EMP occurred when the flux of gamma radiation from the nuclear explosion produced high-energy free electrons that became trapped in the Earth's geomagnetic field.[136] The interaction of the free electrons with the magnetic field caused a short burst, or pulse, of electromagnetic energy.

In addition to the shorter, concentrated pulses, such as those resulting from nuclear detonations, accelerating, or oscillating electrical charges may produce disturbances in the form of continuous waves. When strong

131. Taser is actually the brand name of a device produced by Axon. *See TASER Smart Weapons*, AXON, https://www.axon.com/solutions/law-enforcement/in-the-field#smart-weapons (last visited July 1, 2019).

132. MCGRAW HILL ENCYCLOPEDIA OF PHYSICS, *supra* note 125, at 268.

133. *Physiological Effects of Electricity*, ALL ABOUT CIRCUITS, www.allaboutcircuits.com/textbook/direct-current/chpt-3/physiological-effects-electricity/ (last visited July 1, 2019).

134. Gilbert King, *Going Nuclear over the Pacific*, SMITHSONIAN (Aug. 15, 2012), https://www.smithsonianmag.com/history/going-nuclear-over-the-pacific-24428997/.

135. *Id.*

136. R. EVERETT LANGFORD, INTRODUCTION TO WEAPONS OF MASS DESTRUCTION: RADIOLOGICAL, CHEMICAL, AND BIOLOGICAL 104 (2004).

enough, these waves can result in varying harmful effects. Weapons employing concentrated waves of energy as the damage mechanism are often referred to as directed-energy weapons, the most recognizable variant being the laser.[137] Electromagnetic energy of a certain intensity, whether transmitted through pulses or continuous waves, directly causes the terminal effect upon the target.

Sound waves, such as ultra-high frequency sonic waves, are related to electromagnetic waves, but unlike the latter, which can transmit in empty space, they require a medium, such as air, water, or solids to transmit energy. However, like electromagnetic waves, they carry energy, producing damage by causing the target to vibrate excessively. A common, non-weaponized example of damage caused by sound is a hearing loss caused by prolonged exposure to loud noises, such as construction work. In addition to sonic weapons, sound damage can also occur from the detonation of explosive weapons. In both examples, the direct transfer of sonic wave energy from a weapon to its target causes the damaging terminal effect.

Radiological: Radiation damage mechanisms are designed to cause radiation poisoning or contamination of an area with a radiological source. Although radiological damage, together with blast, fragmentation, heat, and electromagnetic, is a key damage mechanism of nuclear weapons, simpler lower-level devices such as "dirty bombs" (conventional explosives to which a radiological source is attached) also employ this mechanism.

The release of energy from an unstable atomic nucleus as it attempts to achieve stability causes radiological harm. In certain elements, like uranium, the release can occur naturally over a period known as a half-life. Thus, even after the employment of a radiological weapon, potential long-term damage may not be immediately manifest. Release can be the product of a human-engineered forcing mechanism, such as an explosion, that triggers the spread of radiation.

When alpha, beta, gamma, and neutron forms of radiation, or a combination thereof, are released, the energy transfers from that radiation to the matter into which it comes in contact. In living organisms, this damages the deoxyribonucleic acid (DNA), an effect that interferes with cellular reproduction. If the energy contained in the particle is strong enough, it can kill cells and cause relatively immediate death. However, when weaker particles

137. Laser is an acronym for "light amplification by stimulated emission of radiation." *See* SPENCER TUCKER, INSTRUMENTS OF WAR 353 (2015).

damage the DNA severely enough, long-term effects such as cancer and birth defects can occur. [138] Although this damage may not manifest itself for long periods and other factors can exacerbate it, immediate harm directly results from the terminal effect of the radiological damage mechanism.

Chemical: Many weapons rely upon chemicals to function, but not all of these weapons qualify as chemical weapons. For example, explosives work on chemical principles but they are not regulated as chemical weapons. The distinction is clear in the 1993 Chemical Weapons Convention, which defines a chemical weapon as "toxic chemicals and their precursors," as well as the "[m]unitions and devices, specifically designed to cause death or other harm through the toxic properties of those toxic chemicals."[139] Under the Convention, a toxic chemical is "[a]ny chemical which through its chemical action can cause death, temporary incapacitation or permanent harm to humans or animals."[140]

Chemical weapons are unique in that they include both agents that act through a transfer of energy, as with a burning agent, and agents utilizing a non-organic toxin that causes damage by interfering with organic functions, as opposed to the transfer of energy. Examples of chemical weapons include blister agents, blood agents, choking agents, nerve agents, lacrimators (tear gas), vomiting agents, irritants, and psychotropic compounds. They generally work through contact or inhalation, and while some agents are designed to produce temporary incapacitation, others can cause permanent damage or death.[141] In both cases, they directly inflict damage on their target with no required intermediary.

Biological: The 1972 Biological Weapons Convention prohibits States Party from developing, producing, stockpiling, or otherwise acquiring or retaining "microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes" in addition to their

138. The body's cellular repair mechanisms are capable of fixing broken single strands of DNA. However, when the radiation breaks both strands of the DNA molecule, the body is generally unable to repair the strand. This type of damage is more common with the larger alpha particles. *See* LANGFORD, *supra* note 136, at 38–44.

139. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction art. II(1), Jan. 13, 1993, 1974 U.N.T.S. 45.

140. *Id.* art. II(2).

141. LANGFORD, *supra* note 136, at 225–30.

delivery mechanisms.[142] Their harm mechanism is biological in character, as opposed to chemical, because organic pathogens or other microorganisms produce the toxin that causes the disease.[143] Typical biological toxins include bacteria, rickettsia, fungi, and viruses. Like some chemical toxins, biological weapons do not inflict harm through the transfer of energy; instead, they interfere with natural biological functions.[144] Although there is no transfer of energy, the damage mechanism is nonetheless terminal as the toxin's interaction with the target directly inflicts the harm.

B. Determinative Characteristic of a Means of Warfare

From the survey of damage mechanisms, it is possible to identify common characteristics, thereby allowing cyber capabilities to be assessed against them to determine their qualification as means of warfare that are subject to the legal obligations and prohibitions set forth earlier. As discussed below, while some of the damage mechanisms share several characteristics, the sole common, and therefore determinative, trait is the ability to deliver a terminal effect directly on a target. Before turning to that feature, it is helpful to rule out other potential commonalities.

The characteristic that is perhaps most likely to be viewed as defining a means of warfare is the transfer of energy, as with mechanical, thermal, radiological, and electromagnetic damage mechanisms. Yet, some chemical—and all biological—weapons do not involve the transfer of energy. Since their status as a means of warfare is beyond question, energy transfer cannot serve as a required qualification.

Another shared characteristic of many weapons is that the harm triggered by the damage mechanism manifests in an immediate and discernable manner, as in the case of being shot. However, not all damage mechanisms generate an immediate effect. A number of mechanisms, like radiological, inflict harm internally, sometimes only at the cellular level, which may not surface for years. A low-yield radiological device, for instance, is unlikely to

142. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction art. 1, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163.

143. The United States defined toxins during the treaty negotiations as "poisonous substances produced by biological organisms, including microbes, animals, and plants." United States, Policy on Toxins: Working Paper Submitted to the Conference of the Committee on Disarmament ¶ 2, U.N. Doc. CCD/286 (Apr. 21, 1970).

144. LANGFORD, *supra* note 136, at 152–53.

achieve any immediate effect against personnel or equipment but is certainly a weapon in light of the foreseeable likelihood that it will cause severe health problems, even if sometimes only over the longer term. Even the blast damage from an explosive device may not be apparent until long after its use, as in the case of traumatic brain injuries.[145] Accordingly, the ability to immediately recognize or measure harm cannot be considered a condition precedent to qualification as a means of warfare. And while the harm that eventually results from use of a weapon is usually discernable, that is not universally the case. For instance, an electromagnetic pulse device may never result in visually identifiable harm, other than the fact that an electronic system permanently ceases to function.

In contrast, there are two defining characteristics common to all means of warfare damage mechanisms. First, the effect must be to injure or kill persons or damage or destroy objects. As noted above, IHL provides protections against such consequences during an attack. Devices and systems that do not produce these effects are generally not considered as means of warfare. For example, a system such as an EA-6B Prowler aircraft that jams enemy radar and communications is not a weapon,[146] nor is an aircraft that merely monitors enemy signals like the EP-3E Aires.[147]

Second, means of warfare are designed to directly produce a terminal effect. An effect is terminal when no intermediary or intervening device or action beyond the weapon itself is required for the harm to occur. The harm may be visible or not, immediate or not, or kinetic or not, but it always directly results from the damage mechanism associated with the weapon. In other words, the weapon itself causes harm. Reflecting this commonality, Bill Boothby has observed, "[m]eans of warfare consist of all weapons, weapons platforms and associated equipment used directly to deliver force during hostilities."[148]

Combining these factors, we suggest that having a damage mechanism with the ability to directly inflict the damaging or injurious terminal effect on

---

145. *See generally* Michael Schmitt & Chad Highfill, *Invisible Injuries: Concussive Effects and International Humanitarian Law*, 9 HARVARD NATIONAL SECURITY JOURNAL 72 (2018).

146. *EA-6B Prowler Electronic Warfare Aircraft*, UNITED STATES NAVY, https://www.navy.mil/navydata/fact_display.asp?cid=1100&tid=900&ct=1 (last updated Feb. 5, 2009).

147. *P-3C Orion and EP-3 Aries*, UNITED STATES NAVY, https://www.navy.mil/navydata/fact_display.asp?cid=1100&tid=1400&ct=1 (last updated Dec. 3, 2008).

148. William H. Boothby, *Methods and Means of Cyber Warfare*, 89 INTERNATIONAL LAW STUDIES 387, 387 (2013). In the same article, Boothby assesses the potential for the existence of cyber weapons and means of warfare, finding the critical factor to be the ultimate effects of the operation. *Id.* at 389.

a target is the litmus test for qualification as a means of warfare. To reiterate, the requisite terminal effect is caused without an intermediary mechanism or action. Consider a cell phone used to detonate an improvised explosive device (IED). The cell phone, which was not designed to be integral to the operation of a means of warfare, communicates with the IED, but it is the IED that delivers the required terminal effect through its blast damage mechanism. The cell phone is not a means of warfare, whereas the IED qualifies as such. Or, consider a sonic device. It causes the body's organs to vibrate excessively to the point of physical damage, and therefore, it delivers the terminal effect. Although the consequence of the organ damage may not be immediately apparent, it is a means of warfare. And consider a ruse operation in which one party to the conflict transmits false enemy communications that cause some members of the enemy forces to go to a location where they are ambushed.[149] But for the transmission of the false signals, the attack would not have occurred, and those ambushed would not have died. However, the devices used to transmit the signals did not deliver the terminal effect. Rather, the weapons used in the ambush to wound and kill the enemy did so.

Armed with these defining characteristics of means of warfare, cyber capabilities can be assessed to determine whether they qualify as means of warfare. The weight of scholarly opinion currently slants towards classifying some cyber capabilities as means of warfare. Both the *AMW Manual* and *Tallinn Manual 2.0* adopt this position,[150] as do some scholars.[151] The tendency is to focus on the nature of the consequence of a cyber operation, the first of the two defining characteristics. As *Tallinn Manual 2.0* states,

> "Means of cyber warfare" are cyber weapons and their associated cyber systems . . . .
>
> [C]yber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack. . . .

149. AP I, *supra* note 7, art. 37(2); UK LOAC MANUAL, *supra* note 52, ¶ 5.17.2.

150. AMW MANUAL, *supra* note 18, r. 1(t), cmt. ¶ 5, at 31; TALLINN MANUAL 2.0, *supra* note 20, at 452.

151. *See, e.g.*, Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 115, 135 (2014); *see also* WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 238 (2d ed. 2016).

> Cyber means of warfare, therefore, include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack.[152]

Of particular importance in the cyber context is the extension of the notion of damage to include loss of functionality. Thus, a cyber operation that "bricks" cyber infrastructure or requires replacement of components without physically damaging the system would be an attack such that the device, system, or code used to execute the operation would comprise a weapon and perhaps, considered ensemble, a weapon system (both of which are means of warfare).[153]

However, as reflected in the use of the term capability instead of weapon or means of warfare by the U.S. Air Force and UK Ministry of Defence,[154] some States seem reluctant to characterize even cyber capabilities capable of causing the requisite consequences as means of warfare. Although no State has publicly explained its rationale for avoiding the branding of cyber capabilities as means of warfare, the apprehension of those falling into this camp is well founded because cyber capabilities do not satisfy the previously identified defining characteristics.

In particular, analysis of whether network systems (and their components) or computer code used in a cyber operation are a means of warfare must go beyond a simple catalog of an operation's ultimate effects. Consider an incident in which an individual gains physical access to industrial plant controls and manipulates the cooling system in a manner that causes physical damage when components overheat. The requisite effects occurred, but that individual clearly did not employ any weapon. The fact that a remote cyber operation can cause precisely the same effect illustrates that the definitional analysis of means of warfare requires an additional step that examines how the effect was produced, that is, whether the capability in question directly caused the terminal effect, the second criterion associated with means of warfare.

---

152. TALLINN MANUAL 2.0, *supra* note 20, at 452–53. *Tallinn Manual 2.0* defines a "cyber attack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." *Id.* r. 92, at 415–20.

153. *Id.* at 417–18. Note that the *Tallinn Manual* experts were unable to agree upon the precise threshold at which an effect on cyber infrastructure would amount to a loss of functionality. *Id.*

154. *See supra* notes 77, 88–90 and accompanying text.

To comprehend when terminal effects are delivered in the cyber context, a basic understanding of the primary aspects of a cyber operation: computer systems, network infrastructure, and data is useful. A combination of hardware and software make up computer systems. Hardware consists of the physical components of a computer used to process and store data. Various types of data referred to as software control the hardware components. Computer systems receive, process, and interpret inputs, then subsequently store or deliver an output based on its operating instructions.

Networks are created when individual computer systems are connected through shared nodes (active electronic distribution devices) that originate, route, or collect data via a data link. These networks may then connect to other networks, creating larger networks, such as the global Internet. Like computer systems, networks are also composed of hardware and the resident operational software. When a system or network is not directly connected to any other outside systems or networks, they are referred to as air-gapped systems or networks, and data communications can generally be delivered only by direct access, such as inputs from a user or insertion using storage media like a memory stick.

Any individual node connected to a network, such as the Internet, can send data to, and receive it from, any other connected node. Communication of the data occurs through a series of relayed requests between nodes that sit on common borders between multiple networks through which the data is being routed. This data may constitute either information or instructions to be interpreted or acted upon by another system. Operating instructions are a type of data known as computer, or program code. Computer programmers typically write in the source code of a programming language, which then translates the instructions into machine code from which a computer can execute the required tasks. Additional data may be delivered and interpreted by the program code in the execution of the system's tasks.

Concerning qualification as a means of warfare, it is possible to rule out as part of a weapons system, and therefore means of warfare, any system or network infrastructure component used to conduct the hostile cyber operation that was not purpose-built to conduct such operations. Recall that only systems designed to employ, or directly support employment, of a weapon are means of warfare. For example, the off-the-shelf cyber infrastructure used to mount an attack does not qualify as a means of warfare under international law. By contrast, cyber infrastructure that is specifically designed to conduct hostile cyber operations would qualify, but only if the data it communicates to the target system itself amounts to a weapon.

Thus, the issue of the data, specifically code, is key. The fulcrum on which this analysis rests is the fact that code is nothing more than a communicated set of instructions interpreted and acted upon by a set of system or network components. Those instructions can only cause the requisite physical effect if transmitted to a system in control of a tangible object. Sometimes the tangible object is a system or network hardware, such as the cooling system for a server. In this case, the malicious code may cause failure or damage to the hardware component. However, computer systems often control objects that, if malevolently manipulated, can have damaging effects beyond the boundaries of the computer system. An example would be communicating malicious instructions to a navigational satellite that results in the unavailability of information it provides terrestrial systems. The consequence could be the crash of aircraft or collision of ships that rely on the satellite's positional data.

Supervisory control and data acquisition (SCADA) systems are computer networks that control industrial equipment. These networks utilize a programmable logic controller (PLC), which is a computer adapted to control physical processes as diverse as telecommunications, manufacturing, dam operation, oil and gas refining, transportation, and electrical grid operation. SCADA systems generally work by gathering information from a network of sensors, feeding that data through a series of analytical programs in a supervisory computer, and issuing instructions to the PLCs based on the results of that analysis. Although most SCADA systems have a human-machine interface element, some operate independently of human control.

SCADA systems offer the greatest potential for physical destruction resulting from a cyber operation. Stuxnet, for example, was a malicious worm that targeted the SCADA system controlling centrifuges at the Natanz nuclear facility in Iran. The Stuxnet worm caused these centrifuges to rotate at an excessive speed, resulting in physical damage.[155] Similarly, the 2015 operation against the Ukrainian power grid involved manipulation of the SCADA system controlling power substations.[156] While Stuxnet operated through pre-written instructions for the SCADA system, the Ukrainian power-grid

155. Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon,* WIRED (Nov. 3, 2014), www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

156. Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid,* WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

operation was conducted remotely by a malicious actor taking real-time control of aspects of the SCADA system.[157] Despite this difference, both sets of effects ultimately resulted from the communication of a set of instructions acted upon by the target system. Still, it was the action of the targeted system receiving and interpreting the delivered data that in turn caused the physical effects. The code sent by the malicious actor achieved its effects in an indirect manner because it had to be acted upon by the target system. Thus, although the communicated code ultimately resulted in the physical damage, it did so indirectly and therefore was not the cause of the terminal effect.

But what of cyber operations directed against data itself? Do the systems and code used to mount the operation qualify as weapons because the terminal effect is to damage, alter, or destroy the data?

At first glance, it might seem that the answer turns upon whether data is an object, such that to the extent it is affected there is physical damage. However, this long-standing debate in international law circles is a red herring in terms of qualification as a weapon. Even if one takes the position that data is an object that can be damaged or destroyed, the question remains as to whether the networked system and the code it communicates as part of a malicious operation caused the terminal effect on the data.

In such an operation, there is no intermediary PLC or other device controlling a physical object upon which an effect occurs, as data resident in the targeted system itself is the objective. Numerous methods for manipulating or erasing data exist. For example, after a malicious actor gains access to a system, he or she can communicate malicious code to the target system, instructing it to alter or delete its program code (or even source code), or to manipulate or delete (overwrite) informational data.[158] The method used will depend on the aims of the actor, the level of access gained, and the vulnerability exploited.

But whether utilizing pre-written code or real-time operator inputs, in every case the hostile actor is simply communicating instructions to the target system. The system interprets the instruction and acts based on it, as when it alters or erases data. Thus, there is always an intermediate step between the hostile action and the terminal effect. These steps are difficult to conceptualize because they often take place in measures of time so small as

157. *Id.*

158. *See, e.g.*, Kim Zetter, *'Google' Hackers Had Ability to Alter Source Code*, WIRED (Mar. 3, 2010), https://www.wired.com/2010/03/source-code-hacks/.

to appear simultaneous. However, the harmful effects are nevertheless indirect; they are not terminal vis-à-vis the code. Therefore, by their very nature, computer code and associated systems cannot qualify as means of warfare.

This counterintuitive conclusion is logical when viewed in the abstract. Digital data is but a form of language, and computer code is simply a communication from one system to another system or from one component of a system to another. Much like human communications, they never directly cause the requisite effects. The cyber operation may ultimately result in such an effect, but the entity actually causing the terminal effect is the system receiving the communication. To illustrate this point with a non-cyber example, consider a case in which a human air traffic controller falsely tells an aircraft experiencing altimeter malfunction in bad weather that it is at two thousand feet above ground level. In fact, the aircraft is only five hundred feet above ground level, and as a result, it crashes upon approach to landing. The direct cause of the crash (terminal effect) is the pilot taking the physical steps to descend the plane into the ground short of the runway, not the communication. Whereas the controller is responsible for the crash, no one would consider the communication to be a weapon. There is no reason to distinguish this human-to-human communication from computer-to-computer communication or some combination of the two.

It might be asserted that computer code should amount to a weapon because it is analogous to two types of damage mechanisms—biological and electromagnetic. Like biological weapons, cyber capabilities do not involve the transfer of energy. However, a virus is a physical organism that directly causes physical damage to the target's healthy cells, which can occur either by killing health cells or by interfering with their normal function. The targeted body need not take any action for the virus to cause the damage. This is unlike cyber operations, which require the targeted system to take actions based on the delivered communication to achieve the desired effect.

It is similarly tempting to equate cyber capabilities with electromagnetic weapons, such as the electromagnetic pulse or directed-energy weapons discussed above. While cyber capabilities utilize the electromagnetic spectrum, there is an important distinction. An electromagnetic weapon employs the electromagnetic wave as a damage mechanism that involves the transfer of energy. In cyber capabilities, the electromagnetic wave transports a communication. As a result, electromagnetic weapons directly deliver the damaging effect, while cyber capabilities do not.

In sum, because computer code is a communication it cannot constitute a damage mechanism because it does not deliver a terminal effect. As such,

we conclude that code used in hostile cyber operations does not qualify as a means of warfare as a matter of logic and law. If code is not a weapon, the network hardware components that deliver it to the target system do not comprise components of a weapon system. The exception is the network system designed to employ, or assist in the employment, of a weapon with a damage mechanism, such as the computer controlling a surface-to-air missile system. Thus, although the *Tallinn Manual 2.0* experts did not reject classification of cyber capabilities as a means of warfare, they were prescient in defining a weapon as "that aspect of the system used to cause damage or destruction to objects or injury or death to persons."[159] This code does not do.

C. Use of Code as a Method of Warfare

All of the above definitions and discussions of the term methods of warfare are encompassed within the *Tallinn Manual 2.0* explication of a method of warfare as how "hostilities are conducted."[160] The *Manual* states,

> The phrase 'cyber tactics, techniques, and procedures whereby hostilities are conducted' does not include cyber activities that, for instance, involve communications between friendly forces. On the other hand, it is intended to denote more than those operations that rise to the level of an 'attack' (Rule 92). For example, a particular type of cyber operation designed to interfere with the enemy's capability to communicate may not qualify as an attack (as that term is used in this Manual), but would constitute a method of warfare.[161]

We agree that this definition accurately captures the meaning of the term method of warfare in the IHL context. Thus, although communications per se, including communications by cyber means, cannot logically be considered a means of warfare, in our view cyber operations are properly characterized as a method of warfare when employed to harm or interfere with enemy forces, military objectives, the civilian population, or civilian objects. The fact that cyber operations generally do not employ a means of warfare has no bearing on their qualification as such. As previously mentioned, there is no requirement that a means of warfare be used when engaging in a

159. TALLINN MANUAL 2.0, *supra* note 20, at 452.
160. *Id.* r. 103(b), at 452–53.
161. *Id.* at 453.

method of warfare. There being no such requirement, it is unnecessary that the cyber capability in question directly causes the terminal effect.

Characterizing cyber operations as a method of warfare makes sense on several grounds. First, they are typically categorized by methodology—hacking, phishing, distributed denial of service, honeypot, watering hole, et cetera. Second, the development of a single piece of code to exploit a specific vulnerability, which then allows an operator to gain access to and manipulate an opponent's system, resembles a TTP more closely than the creation of a weapon. And like TTP, the code may need to be refined regularly to take account of enemy actions or to be tailored to a particular operation to achieve its desired effects. In fact, the cyber operator sometimes writes the code in real-time as the operation reacts to changing conditions.

To summarize, a means of warfare is the instrumentality that directly causes the terminal effect of death, injury, damage, or destruction. Code and its associated cyber infrastructure only indirectly cause that effect by instructing the targeted system to perform an action. It is this action that typically causes the terminal effect. Methods of warfare refers to techniques for harming the enemy or civilian population, the "how" of the conduct of hostilities. The exploitation of vulnerabilities in enemy systems is one such possibility and exploiting these vulnerabilities is one method for achieving the desired effects in the battlespace.

V. INTERNATIONAL LAW IMPLICATIONS

Having concluded that cyber capabilities cannot meet the definition of a weapon or means of warfare, but that cyber operations may qualify as methods of warfare, it is possible to address the three legal issues that are determined by these characterizations—the requirement for legal review, taking of precautions in attack, and the transportation of munitions across neutral territory. The conclusions reached based on these characterizations are of particular practical importance regarding the conduct of cyber operations.

A. Legal Reviews of Weapons, Means, and Methods

Assertions that cyber capabilities, and particularly computer code, constitute means of warfare present significant practical problems due to what military

strategists often refer to as the "speed of cyber."[162] This term references the ability to achieve rapid effects, sometimes measured in fractions of a second, on the battlefield. Although cyber operations can take weeks or months of detailed preparation,[163] particular phases of those operations that rely on rapidly developed capabilities can be very short. Indeed, and as noted above, in some cases, cyber capabilities are developed and employed in real-time. The development of automated systems to detect threats, analyze target vulnerabilities, develop response capabilities, and deploy those capabilities will increasingly compress timelines.[164]

Recognizing this dilemma, a majority of the *Tallinn Manual 2.0* experts concluded that the weapon review requirement does not require a formal legal review before employment of a cyber capability. Instead, they opined that "the advice of a legal advisor at the relevant level of command . . . suffice[s]."[165] In particular, they concluded "[i]f a method or means of cyber warfare is being developed for immediate operational use, the lawyer who advises the commander planning to use it will be responsible for advising whether the cyber weapon or the intended method of its use accord with the State's international law obligations."[166] Nevertheless, even with legal advisers in cyber mission planning cells, the pace of cyber operations could prove a significant obstacle to the rendering of meaningful reviews.[167]

Moreover, many cyber capabilities are tailored to achieve a specialized objective and consist of specific exploits designed to take advantage of particular vulnerabilities in the targeted cyber infrastructure. As such, they are either non-reusable or require alteration with each employment. This reality would impose a significant practical burden on forces employing cyber capabilities because of the volume of reviews required if code is considered a means of warfare. By contrast, most conventional weapons are fungible in

---

162. *See, e.g.*, J.R. Wilson, *Cyber Warfare Takes a Front Seat in U.S. Military Operations*, MILITARY & AEROSPACE ELECTRONICS (Dec. 1, 2017), https://www.militaryaerospace.com/trusted-computing/article/16709751/cyber-warfare-takes-a-front-seat-in-us-military-operations.

163. George Seffers, *Speed of Cyber is Not Always in Milliseconds*, SIGNAL (Oct. 1, 2018), https://www.afcea.org/content/speed-cyber-not-always-milliseconds.

164. *See generally* Caitríona H. Heinl, *Artificial (Intelligent) Agents and Active Cyber Defence: Policy Implications*, *in* 6TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 53 (Pascal Brangetto, Markus Maybaum & Jan Stinissen eds., 2014).

165. TALLINN MANUAL 2.0, *supra* note 20, at 465.

166. *Id.* at 466.

167. Although outside the scope of this article, the rapid pace of cyber operations might even necessitate the automation of legal reviews.

the sense that they may be employed in a wide variety of situations, all of which can be encompassed in the initial formal legal review.

Although operational exigencies do not relieve States of international legal obligations, States need to grasp the impact that normative interpretation has on practices. If cyber capabilities were a means of warfare, procedures would need to be developed to accommodate the aforementioned realities. However, by our definition, these obstacles do not exist for cyber capabilities. Rather, a legal review is required only if the cyber operation amounts to a method of warfare and only if the State is either a party to Additional Protocol I or the requirement is customary. While we agree with those States that do not treat the requirement for legal reviews of methods of warfare as customary in nature, we also recognize that this position may shift over time. States, of course, may also make a policy choice to conduct legal reviews of types of cyber operations, as the United States does.[168]

In assessing the scope of the legal obligation, it is useful to recall that methods of warfare are the tactics, techniques, and procedures (TTPs) for conducting hostilities. TTPs do not refer to individual operations, but rather to how operations are conducted, as they are categories of operations. The *AMW Manual* also adopts this approach, defining aerial methods of warfare as "the various general categories of operations, such as bombing, as well as the special tactics used for an attack, such as high-altitude bombing."[169]

Thus, with respect to legal reviews of cyber methods of warfare, a review is not required for each individual cyber capability. Rather, for States bearing the obligation or adopting it as a matter of policy, the review requirement encompasses only the various TTP for employing categories of cyber capabilities. The law does not require a specific taxonomy or format for reviews of methods of warfare, and the development of a schema in the cyber context is beyond the scope of this article. The more important point is that the review only extends to the expected use of a category of cyber operation.[170]

Of course, use of a particular cyber capability utilizing a set of TTPs in an individual attack would still have to comply with all prohibitions and limitations that apply to attacks, a contextual determination. To illustrate, consider the use of a weaponized honeypot,[171] a method of warfare subject to

168. *See supra* notes 25–32 and accompanying text.

169. AMW MANUAL, *supra* note 18, r. 1(v), at 34–35.

170. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 91, ¶ 1125.

171. A weaponized honeypot is a system configured to be both attractive and vulnerable to adversarial entities, which when exploited by that adversary contains malicious code.

review. Even if such operations pass muster as a method of warfare, use of the technique in circumstances likely to affect civilians might be barred by the prohibition on indiscriminate attack[172] and, if nevertheless meeting that limitation, the rule of proportionality and the requirement to take precautions in attack.[173] While those who plan, approve, and execute a cyber operation bear the burden of decision in these cases, given the complexity of cyber operations, the immediate availability of a legal adviser is strongly advisable and a best practice militaries should adopt.

B. Selection of Means and Methods of Warfare

The requirement to select from among feasible means of warfare to minimize incidental death or injury to civilians and damage to civilian property does not apply to cyber capabilities for they do not qualify as such. However, as methods of warfare, cyber operations are governed by the same requirement. Because the obligation is customary,[174] it is binding on all States.

As a result, a party to an armed conflict is obliged, subject to the condition of feasibility, to conduct a cyber operation in lieu of a kinetic one when the former is likely to cause less collateral damage to civilians or civilian objects and it is unlikely that military advantage will be sacrificed by conducting the cyber operation. For instance, consider a proposed kinetic attack against a civilian radio station used to transmit coded messages to enemy forces. Assume that civilians will likely be hurt or killed in the attack, but given the importance of disrupting the transmissions, the strike does not violate the rule of proportionality. If using available cyber means can render the relevant equipment non-functional, the attacker would be obligated to employ them as a matter of law. Conversely, sometimes a non-cyber method of warfare poses less risk to protected persons and objects, such as a precise kinetic strike against an isolated military facility that relies on the civilian electrical grid. Here, the kinetic strike poses less risk of collateral harm to civilians and civilian objects than a cyber attack against the electrical grid.

The obligation to select among methods of warfare applies to cyber operations when those operations pose differing risks of causing damage (including loss of functionality) or destruction of civilian objects, or injury or

---

See Rock Stevens & Jeffrey Biller, *Offensive Digital Countermeasures: Exploring the Implications for Governments*, 3 CYBER DEFENSE REVIEW, Fall 2018, at 93.

172. AP I, *supra* note 7, art. 51(4); CIHL, *supra* note 8, rr. 11–12, at 37–43.

173. AP I, *supra* note 7, arts. 51 & 57; CIHL, *supra* note 8, chs. 4–5, at 46–67.

174. CIHL, *supra* note 8, r. 17, at 56–58.

death of civilians. As an example, take the case of a proposed cyber attack against an electricity generating facility to deprive the enemy forces of power during a specified period Imagine that the cyber attack presents risks to the civilian population such as disruption of medical care, emergency services, and civil defense. One option might be to encrypt the supporting cyber infrastructure during the requisite period, while another is to cause the system to overheat, thereby damaging it and requiring significant repair before it returns to full service. If both options were feasible, the former method of warfare would have to be selected because it achieves the effect sought by the attacking party and does so with less risk of collateral damage to the civilian population.

Although a facile reading of the provision indicates only choice among varying methods is required, there may be circumstances in which options falling within a particular category of cyber methods present themselves. The obligation should logically be understood as extending to choices within a particular category of methods as well. Consider again the attack on an electrical grid. One type of malware will permanently encrypt key components of the network, whereas another will only do so temporarily, but throughout the period during which the military commander wants to deprive enemy assets of power. The fact that both employ encryption as a method of warfare does not relieve the commander of the obligation to select the latter if it avoids or minimizes collateral damage.

C. Passage of Cyber Capabilities through Neutral States

As noted above, the customary law of neutrality, codified in Hague Convention V, prohibits the transportation of "munitions of war or supplies" across neutral territory.[175] In that cyber capabilities are not means of warfare, the transmission of hostile code through cyber infrastructure located on neutral territory does not breach the prohibition. Nor are cyber capabilities prohibited as supplies; for just as it is illogical to view communications as munitions or weapons, it is also illogical to view them as supplies.

More appropriately, cyber capabilities, as a communication, should fall under Article 8 of Hague Convention V, which does not require a "neutral Power . . . to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it

175. *See* discussion *infra* Section II.C.

or to companies or private individuals."[176] We align ourselves with the *Tallinn Manual 2.0* experts who were of the view that this exception applied *mutatis mutandis* to communication by cyber means. In the same way that a communication providing intelligence information or ordering the movement of troops qualifies for the exception, so too should any form of cyber communication, even those that may involve the transmission of code that will contribute to an attack on enemy forces. Thus, the knowing transmission of harmful computer code by cyber communications across neutral territory does not violate the law of neutrality, nor does a neutral State violate the law of neutrality when it knows of such transmissions and fails to stop them.

VI. CONCLUSION

In 2013, Tom Rid described a weapon as "a tool that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things."[177] Adapting this definition to the cyber context, he defined a cyber weapon as "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[178]

With the passage of time, Rid has had second thoughts. In his afterword to the reprinting of the book in 2017, he observes,

> [t]he dynamics of vulnerability discovery, exploit development, payload design, entry vectors, command-and-control infrastructure, scalability, exfiltration, disclosure, counter-forensics, or patching are diverse and fast-evolving. Most weapons analogies break down even more quickly today than they did four years ago. Serious research and wider public debate would be best served if we all stop using the hackneyed moniker 'cyber weapons' entirely.[179]

Although Rid may not have been thinking in terms of international law, he is nevertheless correct. The physical damage (including loss of functionality) or injury that occurs as the result of malicious computer code used in a cyber attack is the result of actions ultimately undertaken by the targeted system itself. The code is but a communication to that system instructing it

176. 1907 Hague Convention No. V, *supra* note 13, art. 8; *see also* DOD LAW OF WAR MANUAL, *supra* note 25, § 16.4.1; TALLINN MANUAL 2.0, *supra* note 20, at 556–57.

177. THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 37 (2013).

178. *Id.*

179. THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 188 (2d prtg. 2017).

to undertake a harmful action, function in an unintended manner, or cease to function. In no other type of weapon is an intervening step by the target itself required to achieve the sought-after harm. Thus, the notion that a communication of code alone can constitute a damage mechanism fails to stand up to logical and legal analysis based on current understandings of means of warfare. That said, there is no question that categories of cyber operations are methods of warfare subject to relevant legal prohibitions and limitations, as well as policy restrictions.

In no way do our conclusions upset the foundational balance animating IHL between the humanitarian considerations and military necessity.[180] Cyber operations that amount to an attack remain fully subject to the numerous targeting provisions of IHL. And for States party to Additional Protocol I, the requirement for legal reviews of methods of warfare provides an additional layer of analysis that should be adopted as a matter of policy by those that are not a party to the instrument. These safeguards will ensure that IHL retains its protective balance with respect to the use of cyber operations during armed conflicts.

180. On the balancing between humanitarian considerations and military necessity, see Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance,* 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 795 (2010). *But see* Adil Ahmad Haque, *Indeterminacy in the Law of Armed Conflict*, 95 INTERNATIONAL LAW STUDIES, 118, 120, 147–51 (2019).