THE LAW OF CYBER WARFARE: *QUO VADIS*?

Michael N. Schmitt*

INTRODUCTION

In the mid-1990s, international security affairs specialists began to consider the possibility of cyber warfare,[1] both as an element of classic armed conflict and as a stand-alone proposition. However, the subject faded from the security agenda following the 9/11 attacks. That would change in 2007 when NATO Member State Estonia suffered massive cyber attacks, primarily from ethnic Russian non-state actors. The next year, cyber operations figured prominently in the international armed conflict between Russia and Georgia.[2] In response to

* Charles H. Stockton Professor and Director, Stockton Center for the Study of International Law, United States Naval War College; Professor of Public International Law, University of Exeter; Senior Fellow NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). The author is grateful for the generous support of this research by the Naval War College Foundation and the CCD COE.

1. The term "cyber warfare" is used here in a non-normative and purely descriptive sense. It encompasses acts at the *jus ad bellum* use of force level and those that comprise an armed conflict under the *jus in bello*. The Article will also touch on the law of sovereignty as that law is relevant to such situations of cyber warfare.

2. *See* ENEKEN TIKK ET AL., INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010). The term "cyber infrastructure" refers to "the communications, storage, and computing resources upon which information systems operate. The Internet is an example of a global information infrastructure." TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 211 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]. For other book length treatments of cyberwar, see

these and other cyber incidents, the NATO Cooperative Cyber Defence Centre of Excellence launched a major research project in late 2009 to examine the public international law governing cyber warfare. Twenty world-class academics and legal practitioners (the "International Group of Experts") spent the next three years drafting the *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[3] for which the author served as project director. In light of the relative infancy of cyber operations and paucity of state practice, the Experts agreed to confine themselves to the *lex lata*; *lex ferenda* was strictly off limits, as was speculation regarding the likely development of the law.[4] This Article discards those self-imposed restraints by offering one participant's thoughts as to how the law of cyber warfare may mature in the coming decades.

Of course, the threshold issue for the International Group of Experts was whether international law applied in cyberspace at all. The Experts unanimously agreed that it did,[5] a position that the United States[6] and other key members

---

COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt & Brian T. O'Donnell eds., 2002); CYBER WARFARE: CRITICAL PERSPECTIVES (Paul Ducheine et al. eds., 2012); HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR (2012).

3. TALLINN MANUAL, *supra* note 2.

4. The resulting rules have been generally well received by states, non-governmental organizations, and academics. *See, e.g.*, Dieter Fleck, *Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual*, 18 J. CONFLICT & SECURITY L. 331 (2013); Colonel Kirby Abbott, Assistant Legal Adviser, NATO Supreme Headquarters Allied Powers Eur., Address at Chatham House (Mar. 15, 2013), *available at* http://www.chathamhouse.org/events/view/189465.

5. TALLINN MANUAL, *supra* note 2, at 42, 75. With respect to the *jus ad bellum* (the international law governing the resort to force by states), the International Court of Justice (ICJ) had confirmed that the UN Charter provisions setting forth the prohibition on the use of force, the right of self-defense, and the authority of the Security Council to authorize uses of force "apply to any use of force, regardless of the weapons employed." Legality of Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8). It had come to the same conclusion regarding the applicability of the *jus in bello* (international humanitarian law, "IHL") to new "means and methods" (weapons and tactics) of warfare. *Id.* ¶ 86. This conclusion is supported by Article 36 of Additional Protocol I, which requires a weapons review of new methods and means of warfare. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 36, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]. Obviously, new weapons can only be assessed against existing norms.

6. Harold H. Koh, Address at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland: International Law in Cyberspace (Sept. 18, 2012), *in* 54 HARV. INT'L L.J. ONLINE 1, 3 (2012). This Koh address and the *Tallinn Manual* are compared in Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and the Tallinn Manual Juxtaposed*, 54 HARV. INT'L L.J. ONLINE 13 (2012). The U.S. International Strategy for Cyberspace had earlier acknowledged that "[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace." THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011). See also the U.S. position as set forth for the UN in U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context*

of the international community have since adopted.[7] Members of the Group also unanimously agreed on 95 "Black Letter Rules" of cyber warfare that were meant to restate the existing law. However, the interpretation of these rules sometimes evoked ardent and nuanced debate.[8] The commentary accompanying each Rule captures these debates and highlights those which remain unresolved. Adding to the uncertainty regarding the precise legal parameters of cyber warfare is the fact that public international law is by nature a dynamic creature. As will be explained below, its content, interpretation, and application evolve over time in response to transformation of the security environment in which it applies.

Such ambiguity makes it inconceivable that the extant law of cyber warfare, which responds to cyber operations that are still in their relative technological infancy, will survive intact. This reality begs the question, *quo vadis* the law of cyber warfare?[9] It is a question that the International Group of Experts consciously avoided, but which was always the unspoken elephant in the room. This Article takes the Group's analysis a step further by reflecting on key *Tallinn Manual* norms that are most vulnerable to pressure for future interpretive adaptation. It sets the stage by offering a few brief thoughts on the process of normative evolution. The piece then identifies certain aspects of the law of sov-

---

of International Security: Rep. of the Secretary-General, 18-19, U.N. Doc. A/66/152 (July 20, 2010) [hereinafter UN Doc. A/66/152].

7. The UN Group of Governmental Experts, which includes representatives from Russia and China, agreed in 2013 that international law applies to cyberspace. Press Release, Dep't of State, Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues (June 7, 2013), http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm. Interestingly, Russia and China did not agree to a reference to international humanitarian law and China reportedly does not accept the applicability of IHL in cyberspace. Adam Segal, *China, International Law and Cyber Space,* THE COUNCIL ON FOREIGN REL. (Oct. 2, 2012), http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace. *See also* U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, 15, UN Doc. A/65/154 (July 20, 2010) (United Kingdom); *Government Response to the AIP/CAVV Report on Cyber Warfare*, RIJKSOVERHEID (April 26, 2012), http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf (Netherlands) [hereinafter *Government Response*]; Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, European Commission and the High Representative of the European Union For Foreign Affairs and Security Policy, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 15 (Feb. 7, 2013), http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667; UN Doc A/66/152, *supra* note 6, at 6 (Australia). The joint communication is the proposed European Union cyber security strategy, which is pending approval by the European Parliament.

8. To take a simple example, the International Group of Experts agreed that IHL prohibits cyber "attacks" against civilians. TALLINN MANUAL, *supra* note 2, at 97. Yet, as will be discussed, they could not forge a common understanding as to how that rule applies on the battlefield.

9. *Quo Vadis* is Latin for "Where are you going?" It is drawn historically from Peter's question to the risen Jesus. *John* 13:36.

ereignty, the *jus ad bellum,* and the *jus in bello* which will have to acclimate to the growing threat cyberterrorists, cyberspies, cyberthieves, cyberwarriors, cyber hacktivists, and malicious hackers pose.[10] For each, the current law will be described, the rationale for anticipating interpretive adaptation will be offered, and the probable vector of any change will be indicated. The endeavor is admittedly speculative. However, knowing where such fault lines lie should prove useful as states craft national cyberspace policies and issue rules of engagement, international organizations launch projects designed to achieve normative compatibility in cyberspace, and scholars explore the theoretical foundation for the future law of cyber warfare.

I. NORMATIVE EVOLUTION

If law is to remain effective over time, it must be responsive to context. This axiom is no less true in cyberspace than in the kinetic environment. When significant contextual transformation takes place, new norms emerge, old norms expire or pass into desuetude, and interpretation shifts. The vector and speed of this evolutionary process are the products of influence emanating from many sources—non-governmental advocacy groups, international organizations, international tribunals, domestic constituencies, political action groups, religious leaders, etc.[11]

But states still drive this process.[12] Conceived broadly, international law represents consensus among states as to the rules of the game that govern their interactions. They consent thereto either by opting into treaty regimes or by engaging in practices out of a sense of legal obligation (*opinio juris*) that, com-

10. ERIC A. FISCHER ET AL., CONG. RESEARCH SERV., R42984, THE 2013 CYBERSECURITY EXECUTIVE ORDER: OVERVIEW AND CONSIDERATIONS FOR CONGRESS 2–4 (Mar. 1, 2013).

11. As the U.S. noted in a 2011 report to the UN:

> While the principles [of the *jus ad bellum* and *jus in bello*] are well-established and apply in the context of cyberspace, it is also true that interpreting these bodies of law in the context of activities in cyberspace can present new and unique challenges that will require consultation and cooperation among nations. This is not unusual. When new technologies are developed, they often present challenges for the application of existing bodies of law.

UN Doc. A/66/152, *supra* note 6, at 19. For a fascinating and provocative discussion of the subject in the cyber context, see Michael J. Glennon, *The Road Ahead: Gaps, Leaks and Drips*, 89 INT'L L. STUD. 362 (2013).

12. This principle was famously articulated in the *Lotus* case:

> International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims.

S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, ¶ 44 (Sept. 7).

bined with similar practice by other states, eventually crystallizes into customary international law.[13]

A state's national interests undergird its consent or conduct, and, thus, the development of international law. These interests can be selfish or ignoble. States might seek, for example, to maximize power and influence at the expense of other states or pursue exploitative control over its citizenry and national assets. Yet, states also act out of principled motivations that reflect their core values. In the field of IHL, states have agreed to limitations on their battlefield freedom of action in order to achieve humanitarian ends, sometimes when doing so is militarily counter-productive.[14] Whatever the case may be, the state is the engine of normative evolution.

A turbulent period should be expected vis-à-vis the law of cyber warfare as current international legal norms adjust to the changing national interests of states in cyberspace. Today, information and computer technology "is ubiquitous and relied upon for government services, corporate business processes, and individual professional and personal pursuits—almost every facet of modern life."[15] The near absolute dependence of critical infrastructure on cyberspace looms particularly large as a security concern.[16] Similarly, most contemporary military activities of the United States and other advanced nations, which range from naval warfare, air campaigns and ground attacks to counter-terrorist

13. Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055; *see* North Sea Continental Shelf (Ger. v. Den.; Ger. v. Neth.), 1969 I.C.J. 3, ¶ 77 (Feb. 20) (describing customary international law); *see also* SIR ROBERT JENNINGS & SIR ARTHUR WATTS, OPPENHEIM'S INTERNATIONAL LAW 27-31 (9th ed. 1996); Allain Pellet, *Article 38*, *in* THE STATUTE OF THE INTERNATIONAL COURT OF JUSTICE A COMMENTARY 677-792 (Andreas Zimmerman et al. eds., 1st ed. 2006); Yoram Dinstein, *The Interaction Between Customary International Law and Treaties*, 322 RECUEIL DES COURS 243 (2006).

14. A paradigmatic example is the IHL rule of proportionality, which prohibits attacks on valid military objectives based on the degree of collateral damage likely to be caused to civilians and civilian objects. Additional Protocol I, in TALLINN MANUAL, *supra* note 2, at arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b).

15. FISCHER, *supra* note 10, at 1. For instance, cellular telephone subscriptions worldwide increased from less than 20 per 100 inhabitants in 2001 to 85.7 by 2011. In the developed world, the latter figure was 122.3 per 100 inhabitants. By 2012, 32.5% of individuals used the Internet; in developed countries the figure was 70.2%. In 2010, global revenue from telecommunications services stood at a trillion and a half dollars. The U.S. figure was over two hundred billion dollars. INT'L TELECOMM. UNION, MEASURING THE INFORMATION SOCIETY 1-3, 133-35, 147-48 (2012), *available at* http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf.

16. Critical infrastructure comprises "[t]he physical or virtual systems and assets under the jurisdiction of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment." TALLINN MANUAL, *supra* note 2, at 211. Examples include energy production and distribution, transportation networks, and communications systems upon which essential societal functions and activities depend.

strikes and Special Forces "black operations," would be hobbled by the loss of cyber related assets and capabilities.[17]

As states become ever more dependent on cyber activities, they will increasingly value their access to, and ability to exploit, cyberspace. To protect these values, states will assuredly employ their cyber capabilities to safeguard the cyber infrastructure and cyber activities upon which they rely. However, success will necessitate departure from the received norms that have been set forth by the International Group of Experts in the *Tallinn Manual*. These norms fall into three categories: sovereignty, the *jus ad bellum*, and the *jus in bello*.

II. SOVEREIGNTY

Over the course of the *Tallinn Manual* project, the International Group of Experts realized the need to examine the law of sovereignty in order to afford a more complete picture of state obligations *vis-à-vis* cyber activities, as well as the response options available to states targeted by cyber operations. Foremost among the resulting rules on the subject is the right of states to "exercise control over cyber infrastructure and activities within [their] sovereign territory."[18] It allows states "to exercise . . . to the exclusion of any other State, the functions of a State" on their territory.[19] Effectively, this means that states may regulate all cyber activities taking place on their territory, control the use of any cyber infrastructure located there, and exercise legal jurisdiction over such activities.[20]

As noted by the International Court of Justice (ICJ) in *Nicaragua*, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[21] Consequently, hostile cyber operations directed against cyber infrastructure located on another state's territory, whether government owned or not, constitute, inter alia, a violation of that state's

17. U.S. military budget projections through fiscal year 2018 call for nearly $23 billion in cyber-related expenditures. Of this figure, $9.3 billion will be dedicated to information assurance, with $8.9 billion allocated to defensive and offensive operation capability. The U.S. Cyber Command headquarters' budget, which was $182 million in 2013, will more than double to $405 million the following year. Tony Capaccio, *Pentagon Five-Year Cybersecurity Plan Seeks $23 Billion*, BLOOMBERG (June 10, 2013, 10:36 AM), http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html.

18. TALLINN MANUAL, *supra* note 2, at 25.

19. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

20. On sovereignty generally, see Samantha Besson, *Sovereignty*, MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. (2011), http://opil.ouplaw.com/home/EPIL. The Tallinn Manual Rules on sovereignty and jurisdiction are set forth in TALLINN MANUAL, *supra* note 2, at 25-35.

21. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 202 (June 27) [hereinafter *Nicaragua*]. The case involved U.S. assistance to Nicaraguan guerrillas known as the *Contras* and the mining of Nicaraguan harbors.

sovereignty whenever they cause physical damage or injury.[22] Even if the operations result in no damage or injury, they will qualify as an unlawful "intervention" if they are intended to coerce (as distinct from lawfully influence) the targeted state's government in matters reserved to that state (e.g., by using cyber means to interfere with election results).[23]

A crucial unresolved issue with respect to these sovereign rights and obligations is whether cyber operations that neither cause physical damage nor amount to an intervention nevertheless violate the targeted state's sovereignty. Consider a situation in which State A wishes to monitor certain cyber activities by State B. It has three options for doing so: 1) monitoring the activities by intercepting the signals as they pass through servers on its own territory; 2) sending malware into the target network remotely; or 3) implanting the malware through a spy's use of a memory stick. The first option poses no legal obstacles because international law does not prohibit espionage and the operation is physically harmless and involves no coercive intent.[24] The third is a clear violation of the targeted state's sovereignty because the operation occurs on its territory without its consent. The second option, however, is legally ambiguous. Does the remote implantation of the malware into State B's cyber systems, as distinct from the fact that State A is monitoring its activities, violate State B's sovereignty? Other examples falling into this category include State A remotely conducting denial of service attacks that interrupt cyber transmissions in State B or erasing or altering data in order to harass that state.

The International Group of Experts could achieve no consensus as to whether such activities amounted to sovereignty violations.[25] Arguably, the distinction between cyber operations resulting in physical damage or injury and those that do not is overly formalistic. Although physical violation was contemplated, as reflected in the derivative principle of territorial integrity,[26] physicality was not the norm's exclusive focus. The prohibition on intervention, which requires coercive intent but not physical damage or injury, illustrates, it would seem, the lack of an all-encompassing requirement for physical effects. Nonetheless, the disagreement remains unsettled.

---

22. This assumes there is no legal justification for the operations, such as self-defense or the taking of countermeasures (see discussion below).

23. *Nicaragua*, *supra* note 21, ¶ 205. The prohibition derives from the principle of the sovereign equality of states as codified in Article 2(1) of the UN Charter. It is specifically acknowledged in the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, G.A. Res. 2625, Annex, 25 U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/5217, at 121 (Oct. 24, 1970). On intervention, see Philip Kunig, *Prohibition of Intervention*, MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. (2008), http://opil.ouplaw.com/home/EPIL.

24. TALLINN MANUAL, *supra* note 2, at 44.

25. *Id*. at 6.

26. Samuel K.N. Blay, *Territorial Integrity and Political Independence*, MAX PLANCK ENCYCLOPEDIA PUB. INT'L L. (2010), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1116?rskey=6BhtzU&result=1&prd=EPIL.

This lack of clarity opens the door to an interpretive widening of the notion of sovereignty. With states and their citizens becoming ever more reliant on cyber activities, a strengthening of the normative firewalls that safeguard cyber activities against external interference is to be expected. The ongoing Snowden affair, which revealed widespread monitoring of activities abroad by the U.S. National Security Agency, illustrates the international community's unease with cyber operations that target other states or their citizens, even when non-destructive and, perhaps, lawful under current understandings of international law.[27] In this environment, it will prove difficult for states to mount defensible arguments that sovereignty only restricts destructive cyber operations.

International law rights are balanced by corresponding obligations. A state enjoys the right to control activities on its territory, but it also equally shoulders an obligation to not "allow knowingly its territory to be used for acts contrary to the rights of other States."[28] Accordingly, the International Group of Experts included a Rule in the *Tallinn Manual* to the effect that states may "not knowingly allow the cyber infrastructure located in their territory or under [their] exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[29] The offending activities need not be physically destructive or injurious; they only have to be unlawful (contrary to the legal rights of the affected state) and detrimental.

The obligation is subject to the condition of feasibility. Feasibility looms large in the cyber context because a state may lack the technical wherewithal to know when deleterious activities are occurring on its territory or to take measures to stop them. Additionally, cyber operations may unfold so quickly that the state cannot react in time to end them. Of course, states need not go to extremes to remedy a situation, as in shutting down all communications from their territory in response to minor harmful cyber operations against another state. A rule of reason applies.

Uncertainty surrounds a number of related issues. The first is whether states are obligated to prevent future harmful cyber operations about which they have advance knowledge. For instance, human intelligence sources in the state from which harmful operations are to be launched may reveal a plan to mount them. Or the targeted state may, through technical means, notice the

---

27. Edward Snowden is a computer specialist who worked for the National Security Agency as an employee of Booz, Allen, Hamilton, a government contractor. He is responsible for the leak of a large number of classified documents and information regarding U.S. cyber operations to the British paper *The Guardian*. He fled the United States and is presently living in Russia.

28. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9). *See also* Trail Smelter (U.S. v. Can.), 2 R.I.A.A. 1905, 1963-1965 (1945).

29. TALLINN MANUAL, *supra* note 2, at 32-33. The United States, in a report to the UN, has noted: "States are required to take all necessary measures to ensure that their territories are not used by other States or non-State actors for purposes of armed activities, including planning, threatening, perpetrating or providing material support for armed attacks against other States and their interests." U.N. Doc. A/66/152, *supra* note 6, at 19.

probing of its cyber systems and report this to the state from which the probing originates. Must the state of origin act to preclude the operations from taking place?

It would appear incongruent to suggest that a state has a duty to take remedial action once a harmful cyber operation is launched from its territory, but may sit idly by while planning and preparatory acts are underway. This is especially true with regard to cyber operations, which can occur so quickly (and sometimes last for only a fraction of a second) that the state from which they are launched will be unable to react in a timely fashion. Preventive measures by that state may be the sole viable means of protecting the targeted state from hostile operations. Moreover, the International Group of Experts generally agreed that a victim state is entitled to take proportionate measures to end harmful ongoing cyber operations if the state of origin fails to meet its obligation to end them.[30] It would be peculiar if international law allowed victim states to respond to ongoing harmful actions from another state's territory (a piercing of its sovereignty), but imposed no ex ante obligation on the latter to prevent them in the first place. In all likelihood, most states will eventually take the position that the Rule requires states to employ measures to preclude known forthcoming cyber operations against other states.

The more difficult question is whether states have a duty to take preventive measures to diminish the likelihood that cyber infrastructure on their territory might be used for operations harmful to other states. There is little state practice in this regard. On the contrary, it is typically left to potential targeted states to safeguard cyber activities and cyber infrastructure on their territory.

Survival of this *laissez-faire* approach is unlikely. Some states act as cyber sanctuaries in the sense that harmful cyber operations are mounted from their territory at levels far exceeding those occurring in other states. Additionally, an overall upsurge in the frequency and severity of harmful extraterritorial cyber operations can be expected in the future. It is therefore conceivable that states will begin, in light of their reliance on cyberspace, to interpret the obligation to put an end to harmful activities from their territory as extending to purely preventive measures. Such measures might include, for example, requiring Internet Service Providers (ISPs) to employ outgoing traffic malware filters or shutting down ISPs that are habitually used for harmful operations.

States will be selective in populating any requirements along these lines. As an example, states could monitor communications as a means of identifying and preventing harmful cyber operations that are in preparation or underway. However, extensive monitoring, while helping states to ensure lawful usage of their cyber infrastructure, raises privacy law and policy concerns, as aptly illustrated by the controversy over National Security Agency practices.[31] These and

30. TALLINN MANUAL, *supra* note 2, at 41.

31. For instance, in Europe, cyber activities raise concerns regarding communications rights and data protection. *See* Charter of Fundamental Rights of the European Union, 2000

similar worries will induce states to move cautiously in broadening their interpretation of the norm.

The International Group of Experts also grappled with the issue of whether constructive knowledge suffices.[32] Does a state which fails to act in a situation in which it is unaware of the harmful cyber operations being launched from its territory breach the obligation to end the operation if it could have discovered the activities through the exercise of due care, i.e., if it should have known of the harmful activities?

As the criticality of cyber activities to economic, societal, and governmental functioning grows, so too will the willingness of states to adopt a constructive knowledge approach. The challenge lies in determining when the standard of due care has not been met. For instance, attribution of a cyber operation can involve complex technical measures designed to counter an originator's efforts to mask or spoof its location and identity. Since states have dissimilar capabilities to attribute or geo-locate a cyber operation, due care is necessarily a relative standard. Relativity always complicates consistent and reliable legal appraisals of due care. Additionally, the means of cyber identification and attribution are typically classified, lest those launching the offending operations (or future ones) develop effective counters. The fact that states will be reticent to reveal their capabilities makes it highly problematic to determine with some certainty whether a particular state's technical capabilities are at a level at which the offending cyber operations should, through the exercise of due care, have been identified and attributed. It is apparent that practicalities will hamper adoption of a constructive knowledge approach, no matter how appealing doing so may be.

Finally, the International Group of Experts failed to reach agreement on whether the obligation of taking measures to stop harmful cyber activities reached those states through which the activities are routed.[33] Daunting practical difficulties would impede effective implementation of such a duty in cyberspace. In particular, blocking an offending cyber transmission in a transit state may simply result in its routing through servers elsewhere. An additional complicating factor is that transmissions passing through the servers will have been broken into packets, some of which may be encrypted. Indeed, the malware itself will likely have been disassembled for transmission. This makes identifying transmissions consisting of (or containing) malware extremely problematical. Nevertheless, at least to the extent that it is feasible for transit states to take measures to "clean" or otherwise counter malware passing through their servers, an interpretation of the law by which they have to do so will probably gain traction.

O.J. (C 364) 1, arts. 7-8; Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222.

32. TALLINN MANUAL, *supra* note 2, at 34, 206.

33. *Id*.

III. THE *JUS AD BELLUM*

The *jus ad bellum* determines *when* states may lawfully resort to force. It is completely distinct from the *jus in bello* (discussed below), which governs *how* force may be used once an armed conflict has commenced.

A. *The Use of Force*

Article 2(4) of the UN Charter, which undoubtedly reflects customary international law,[34] sets forth the foundational prescriptive norm of this body of law: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." The Charter contains two exceptions to the general prohibition—uses of force authorized by the Security Council pursuant to Article 42 and self-defense in accordance with Article 51. Article 2(4) and its customary analog apply only to actions conducted by states or otherwise attributable to them pursuant to the law of state responsibility; it has no bearing on the actions of non-state actors such as terrorist groups.[35]

Since the advent of cyber operations, states and scholars have struggled mightily to define the threshold at which an act becomes a "use of force."[36] Just as classic kinetic hostilities qualify, so too do cyber operations causing damage or injury. The interpretive dilemma lies in application of the norm to cyber operations that, while not unleashing destructive or injurious force, nevertheless produce severe non-physical consequences. Do such operations qualify as a use of force that, in the absence of legal justification, violates the prohibition?

The ICJ has rejected a narrow interpretation of "use of force" that limits the term to the employment of either kinetic force or non-kinetic operations generating comparable effects. In *Nicaragua*, the Court held that a state's arming and training of guerrilla forces engaged in hostilities against another state qualified as a use of force,[37] a position that has since become widely accept-

34. *Nicaragua*, *supra* note 21, ¶¶ 188-90.

35. U.N. Charter arts. 2(4), 42, 51. On the rules of attribution, see Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, Annex, U.N. Doc. A/RES/56/83 (Dec. 12, 2001) [hereinafter Articles of State Responsibility].

36. *See, e.g.*, Marco Roscini, *World Wide Warfare—The* Jus ad Bellum *and the Use of Cyber Force,* 14 MAX PLANCK Y.B. UNITED NATIONS L. 85 (2010); Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited,* 56 VILL. L. REV. 569, 571-81 (2011); Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* 26 YALE J. INT'L L. 421 (2011).

37. *Nicaragua*, *supra* note 21, ¶ 228.

ed.[38] The logic of the holding leads to the conclusion that non-destructive cyber operations can sometimes amount to a use of force. For example, providing malware to a rebel group and training its members to employ that malware in a destructive manner would seemingly qualify.

However, every unfriendly act does not cross the use of force threshold. In *Nicaragua,* the Court held that financing guerrillas, albeit an unlawful "intervention," did not rise to that level.[39] Moreover, the drafters of the UN Charter rejected a proposal to include economic coercion in the meaning of the term.[40] It may consequently be concluded that cyber operations intended to economically coerce another state to engage in, or desist from, a particular course of action would not amount to a use of force; nor would financing a rebel group's cyber operations.[41] Beyond these directly parallel examples, uncertainty remains as to where the threshold lies.

Frustrated in their effort to craft a consensus bright-line test for these situations,[42] the International Group of Experts developed a nonexclusive list of factors that would likely influence the characterization of cyber operations by states as uses of force: severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality.[43] Addi-

---

38. *See, e.g.*, Albrecht Randelzhofer & Olivier Dörr, *Article 2(4)*, *in* I THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 200, 211-13 (Bruno Simma et al. eds., 3d ed. 2012).

39. *Nicaragua*, *supra* note 21, ¶ 228.

40. 6 UNITED NATIONS CONF. INT'L ORG., Docs. 2, 334, 609, 617(e)(4) (1945); 3 UNITED NATIONS CONF. INT'L ORG., Docs. 251, 253-54 (1945). The General Assembly likewise rejected the inclusion of economic coercion in the concept during the proceedings leading to adoption of the Declaration on Friendly Relations. U.N. Special Comm. on Friendly Relations, U.N. Doc. A/AC.125/SR.110-14 (1970). *See also* Rep. of the Special Comm. On Friendly Relations and Co-operation Among States, 12, U.N. Doc. A/7619; U.N. GAOR, 24th Sess., Supp. No. 19 (1969). A December 2011 report endorsed by the Dutch government, stated, "[p]urely economic, diplomatic and political pressure or coercion is not defined as a use of force under article 2, paragraph 4." ADVISORY COUNCIL ON INT'L AFFAIRS AND THE ADVISORY COMM. ON ISSUES OF PUB. INT'L LAW, CYBER WARFARE 20 (No. 77, AIV/No. 22, CAVV) (Dec. 2011) [hereinafter AIV/CAVV Report], *available at* http://www.aivadvies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf, endorsed by *Government Response*, *supra* note 7, at 4. On the issue of economic coercion, see also Randelzhofer and Dörr, *supra* note 38, at 208-10.

41. This conclusion is limited to *coercion*, as in the case of cutting off another state's access to cloud services based in its territory, thereby forcing that state to move data to a more expensive cloud elsewhere, or to create its own. It would not include cyber operations directed against the economic cyber infrastructure (such as that upon which a stock market or banking system is dependent).

42. TALLINN MANUAL, *supra* note 2, at 45. The relevant rule simply provides: "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful." *Id*.

43. TALLINN MANUAL, *supra* note 2, at 47-52. An earlier version of the approach was set forth in Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

tional factors found meaningful by the Experts included, inter alia, the prevailing political environment, the nexus of an operation to prospective military force, the attacker's identity, the attacker's track record with respect to cyber operations, and the nature of the target. These and other factors operate in concert as states make case-by-case determinations. Of them, only severity alone can qualify a cyber operation as a use of force. In this regard, the Group unanimously agreed that any cyber operation causing greater than *de minimis* damage or injury suffices. For instance, they concurred that the damage to Iranian nuclear facilities in 2010 resulting from the Stuxnet virus crossed the threshold.[44]

Over time, the reaction of states to cyber operations, as well as how they characterize their own cyber operations, will inform the process of interpretive maturation. The use of force threshold, wherever it may presently lie, will almost certainly drop in lock step with the increasing dependency of states on cyberspace. Although it is difficult to predict whether any bright-line test will materialize or whether states will simply make use of force characterizations more liberally, a number of options for clarifying the threshold exist. One is an interpretation by which cyber operations directed against certain categories of targets create a rebuttable presumption that force has been used. In particular, operations that non-destructively target critical infrastructure may come to be viewed by states as presumptive uses of force. The same approach might be applied to military targets or state systems designed to provide cyber security. Another possibility is that states will begin to treat data destruction as the functional equivalent of physical destruction for use of force characterization purposes whenever the destruction of the data severely disrupts societal, economic or governmental functions. Whatever the case, states will eventually be compelled by circumstances to take a position on whether particular cyber operations have breached the use of force prohibition; these assessments will add significant granularity to the norm in the cyber context.

B. *Self-Defense*

While the use-of-force prohibition determines whether a cyber operation conducted by, or attributable to, a state violates that norm of international law, the right of self-defense addresses when states may use force in response to cyber operations. Article 51 of the UN Charter, which like Article 2(4) reflects customary international law, sets forth the right: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security

44. TALLINN MANUAL, *supra* note 2, at 47 (noting that Stuxnet would be unlawful only if launched by a state without legal justification, such as anticipatory self-defense).

Council has taken measures necessary to maintain international peace and security."[45]

As with the use of force, the space for interpretive development is primarily definitional.[46] The International Group of Experts agreed that the term "armed attack" differs from "use of force."[47] It did so based on the ICJ's finding in *Nicaragua* that it is necessary to "distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[48] By this holding, all armed attacks are uses of force, but not all uses of force are armed attacks.

The Experts unanimously concluded that "any use of force that injures or kills persons or damages or destroys property" amounted to an armed attack against which a state enjoys the right to resort to force in self-defense.[49] The requisite degree of damage or injury remains, however, the subject of some disagreement. For instance, the ICJ excluded a "mere frontier incident" from the ambit of armed attack, a distinction that has generated criticism.[50] On the other hand, the court has elsewhere suggested that an attack on a single military platform or installation could rise to the armed attack level.[51] Wherever the threshold may lie, it is indisputable that a cyber operation causing significant damage or injury qualifies as an armed attack, whereas many nondestructive cyber operations like intelligence gathering, cyber theft, or periodic disruption or denial of nonessential cyber services do not.

Two areas of uncertainty with respect to the law of self-defense pose the greatest interpretive potential. First, it is unclear whether a cyber operation that does not result in physical damage or injury can nevertheless amount to an armed attack when it generates severe non-destructive or non-injurious conse-

---

45. U.N. Charter art. 51. On self-defense in the treaty and customary contexts, see Terry D. Gill, *Legal Basis of the Right of Self-Defence under the UN Charter and Under Customary International Law*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS 187 (Terry D. Gill & Dieter Fleck eds., 2010); Albrecht Randelzhofer & Georg Nolte, *Article 51*, *in* II THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 1397, 1403-04 (Bruno Simma et al. eds., 3d ed. 2012).

46. On self-defense in cyberspace, see Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002); Matthew C. Waxman, *Self-Defensive Force Against Cyber Attacks: Legal, Strategic, and Political Dimensions*, 89 INT'L L. STUD. 109 (2013); Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, *supra* note 36, at 586-603.

47. TALLINN MANUAL, *supra* note 2, at 47, 52. *See also* Randelzhofer & Nolte, *supra* note 45, at 1401-03.

48. *Nicaragua*, *supra* note 21, ¶ 191. *See also* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 51 (Nov. 6); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116, ¶ 147 (Dec. 19).

49. TALLINN MANUAL, *supra* note 2, at 55.

50. *Nicaragua*, *supra* note 21, ¶ 195. *But see, e.g.*, YORAM DINSTEIN, WAR, AGGRESSION AND SELF DEFENCE 210-12 (5th ed. 2011).

51. *Oil Platforms*, 2003 I.C.J. 161, ¶¶ 57, 61.

quences. Some of the Experts adopted a narrow approach that limited the current law to physical effects. Others supported an interpretation that focused not on the nature of the consequences (physical), but rather on their severity. The scenario typically proffered in this regard is a massive cyber operation targeting a state's economic infrastructure. Those Experts taking the latter approach argued that it would be incongruent to consider such an operation as falling below the armed attack threshold, but treat an operation that resulted in physical damage to, for instance, a few factories as meeting it.[52]

The better view is that, in the absence of conclusive state practice, the law of self-defense has not quite evolved to the point where non-destructive or non-injurious cyber operations can qualify as armed attacks. That said, it is almost certain that states will begin to treat such cyber operations as armed attacks to which they can respond forcefully when the consequences are sufficiently severe. Cyber operations make possible the dramatic disruption of a state's normal functioning and the imposition of other non-destructive consequences to a degree heretofore unimaginable absent a military attack. This transformed security environment will render evolution of the law of self-defense inevitable.

Some states are taking the lead in driving the process. For instance, the United States, in a report to the UN, has asserted, "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack."[53] It did not indicate which sorts of disruptive activities would qualify. The Netherlands appears to have gone further. In 2011, the Dutch Advisory Council on International Affairs and the Advisory Committee on Issues of Public International Law issued a report that, after confirming that significant destruction or injury would qualify as an armed attack, noted:

> It is more difficult to conclude whether this is the case if there are no actual or potential fatalities, casualties or physical damage. A serious, organised cyber attack on essential functions of the state could conceivably be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state. In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks for it to be qualified as an armed attack. A disruption of banking transactions or the hindrance of government activity would not qualify as an armed attack. However, a cyber attack that targets the entire financial system or prevents the government from carrying out essential tasks, for example an attack on the entire military communication and command network that makes it impossible to deploy the armed forces, could well be equated with an armed attack.[54]

52. Other examples abound. For example, hostile cyber operations could effectively ground air transportation, cause massive blackouts, or destroy government data upon which the functioning of the Social Security or national tax system relies.

53. UN Doc. A/66/152, *supra* note 6, at 18.

54. AIV/CAVV Report, *supra* note 40, at 21.

Although the government response to the report did not expressly endorse this position, it noted, "the findings of the AIV/CAVV with regard to the use of force and the right of self-defence are largely in line with the government's position."[55]

While future understandings of the notion of armed attack will probably be severity based, how that severity will be measured remains open to question. As with the use of force threshold, the norm could evolve based on certain categories of targets, such as critical infrastructure, that present particular risks of harm or based on various essential activities, like cyber security. Alternatively, severity might be measured in terms of degree of harm, as in the case of economic impact.

In that global stability relies on normative predictability, the need for a well-defined standard is greater in the armed attack than in the use of force context. As a practical matter, characterization of a cyber operation as a wrongful use of force merely serves to label the state involved as a violator of international law. Furthermore, while state responses to uses of force are capped at the non-forceful countermeasures level,[56] an armed attack gives the targeted state the right to respond with its own use of force. Therefore, the consequences of a situation in which a state mounting a cyber operation miscalculates how the targeted state will characterize it (and respond based on that characterization) are graver with respect to the armed attack threshold.

A second prospect for interpretive development lies in the relationship between the use of force and armed attack thresholds. As noted, the International Group of Experts unanimously endorsed the view that posits a gap between the two. By contrast, the United States has rejected the premise of a gap since its original articulation in *Nicaragua*. As former State Department Legal Advisor Harold Koh stated,

> [T]he United States has for a long time taken the position that the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response.[57]

The U.S. stance, which presently represents a minority view among states and international law experts, is liable to weaken over time. In the kinetic context, the approach made sense for states that wielded significant military power. Although its *de jure* effect was to allow states targeted by military operations that cross the use of force threshold, and therefore that of an armed attack, to respond forcefully, the *de facto* disparity in military power meant that it would

---

55. Government Response, *supra* note 7, at 5.

56. Articles of State Responsibility, *supra* note 35, art. 50(1)(a).

57. Koh, *supra* note 6, at 7. *See also* Abraham D. Sofaer, *Terrorism, the Law, and the National Defense*, 126 MIL. L. REV. 89, 93-96 (1989); William H. Taft, IV, *Self-Defense and the* Oil Platforms *Decision*, 29 YALE J. INT'L L. 295, 299-302 (2004). Both of the authors served as State Department Legal Advisers. For criticism of the approach, see Yoram Dinstein, *Cyber War and International Law*, 89 INT'L L. STUD. 276, 279-80 (2013).

usually be imprudent for targeted states to do so. This logic breaks down in cyberspace because militarily weak states may nevertheless enjoy the ability to inflict significant damage by cyber means. The relative impunity afforded by military superiority therefore dissipates significantly in cyberspace, an especially problematic dynamic if, as was suggested above, the use of force threshold drops. States presently maintaining the U.S. view will soon realize that a gap affords them greater freedom of action to conduct cyber operations without risking forceful kinetic or cyber responses.

Further global development of robust cyber capabilities will also likely sound the death knell for classic temporal approaches to anticipatory self-defense.[58] Although it is occasionally suggested that the right of self-defense does not extend to prospective armed attacks,[59] the great weight of informed opinion supports the existence of a right of anticipatory self-defense in the face of an "imminent" armed attack.[60]

The notion of imminency finds its genesis in an exchange of diplomatic notes between the United States and Great Britain during the nineteenth century *Caroline* incident. In that exchange, U.S. Secretary of State Daniel Webster claimed that the right of self-defense only applied when "the necessity of that self-defence [was] instant, overwhelming, and leaving no choice of means, and no moment for deliberation."[61] In the ensuing decades, this statement became the *locus classicus* against which self-defense actions were measured.[62] In application, it was traditionally interpreted as a temporal benchmark by which states could only act when the impending attack was about to be launched.

Coexistence of transnational terrorism and the risk of weapons of mass destruction proved to be a self-defense game-changer. As the 2002 U.S. National Security Strategy noted in the aftermath of the 9/11 attacks, "Rogue States and terrorists do not seek to attack us using conventional means . . . . Instead, they rely on acts of terror and, potentially, the use of weapons of mass destruction—weapons that can be easily concealed, delivered covertly, and used without warning."[63] In these circumstances, a purely temporal standard was insensible since a single catastrophic attack could occur without warning. If the right

58. On anticipatory self-defense in cyberspace, see Terry D. Gill & Paul A.L. Ducheine, *Anticipatory Self-Defense in the Cyber Context*, 89 INT'L L. STUD. 438 (2013).

59. *See, e.g.*, IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 275-78 (1963); DINSTEIN, *supra* note 50, at 203-04.

60. Randelzhofer & Nolte, *supra* note 45, at 1421-25.

61. Letter from Daniel Webster to Lord Ashburton (Aug. 6, 1842), *in* 2 INTERNATIONAL LAW DIGEST 412 (John Bassett Moore ed., 1906).

62. R.Y. Jennings, *The* Caroline *and* McLeod *Cases*, 32 AM. J. INT'L L. 82, 92 (1938). For instance, the Nuremberg Tribunal cited the standard with approval. *Judgment of the International Military Tribunal Sitting at Nuremberg, Germany* (Sept. 30, 1946), *in* 22 THE TRIAL OF GERMAN MAJOR WAR CRIMINALS: PROCEEDINGS OF THE INTERNATIONAL MILITARY TRIBUNAL SITTING AT NUREMBERG, GERMANY 435 (1950).

63. THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES 15 (Sept. 2002).

of self-defense was to remain meaningful, it had to adapt to the changed security environment.

A contemporary interpretation, which was adopted by the International Group of Experts, focuses on the opportunity to defend oneself rather than temporal proximity of the defensive actions to the prospective armed attack.[64] It requires a confluence of three factual conditions precedent.[65] First, the prospective attacker must have the capability to conduct the attack, or at least be on the verge of acquiring it. Self-defense is not permitted simply because another state is generally hostile. Second, the attacker must intend to mount an armed attack. Self-defense does not allow a state to preventively remove capabilities until the intent to use them has solidified. Third, the state in question is only empowered to use force anticipatorily once the window of opportunity to take effective defensive measures is about to close. This approach has become known has the "last window of opportunity" test.[66]

Cyber operations heighten the motivation for adopting the last window of opportunity approach. Such operations are usually mounted covertly, can occur instantaneously, may be difficult to attribute reliably in real time, and can produce cataclysmic consequences. Cyber attack capabilities are also relatively easy to acquire and are broadly distributed. In light of these operational realities, slavishly adhering to a temporal standard is both illogical and dangerous. After all, the lapse of time between the decision to conduct a cyber armed attack, its execution, and the manifestation of its consequences may be measured in milliseconds. If the right of self-defense is to have any substance, a state must be able to act forcefully to avert an armed cyber attack once it learns that the operation is going to be mounted and it risks losing the chance to defend itself effectively if it hesitates.

Significant controversy has surrounded the question of whether non-state actors may conduct armed attacks as a matter of law. It is indisputable that their actions are sometimes attributable to a state such that the victim state can re-

---

64. TALLINN MANUAL, *supra* note 2, at 61.

65. *Id*. The approach was developed in Michael N. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum*: A Normative Framework*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 157 (Michael N. Schmitt & Jelena Pejic eds., 2007). *See also* Michael N. Schmitt, *21st Century Conflict: Can the Law Survive?*, 8 MELB. J. INT'L L. 443, 454 (2007).

66. The last window of opportunity approach was first set forth in Michael N. Schmitt, *Preemptive Strategies in International Law,* 24 MICH. J. INT'L L. 513, 534-36 (2003). The U.S. government has since adopted the standard. *See, e.g*., DEP'T OF JUSTICE, WHITE PAPER: LAWFULNESS OF A LETHAL OPERATION DIRECTED AGAINST A U.S. CITIZEN WHO IS A SENIOR OPERATIONAL LEADER OF AL-QA'IDA OR AN ASSOCIATED FORCE, Draft, 7 (Nov. 8, 2011), *available at* http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf [hereinafter WHITE PAPER]; Eric Holder, U.S. Att'y Gen., Speech at Northwestern University School of Law (March 5, 2012), *available at* http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html.

spond forcefully against both the non-state actors involved and the state to which their actions are attributable. As noted by the ICJ in *Nicaragua*,

> An armed attack must be understood as including not merely action by regular forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (*inter alia*) an actual armed attack conducted by regular forces, "or its substantial involvement therein."[67]

The more legally troublesome situation is one in which non-state actors with no ties to a state conduct operations at the armed attack level. In the aftermath of al-Qaeda's 9/11 attacks, most states and commentators appeared to regard Article 51 and its customary counterpart as applicable to attacks by non-state actors.[68] Although the ICJ seemed to back away from that interpretation in the *Wall* Advisory Opinion and the *Armed Activities* Judgment,[69] the United States and numerous other states continue to advocate it.[70]

Future cyber operations will weaken the ICJ's narrow interpretation. Cyberspace is a fertile environment for non-state actors who wish to attack states. While it can be difficult for non-state actors to acquire the kinetic means and find the opportunity to conduct an operation at the armed attack level, the wide availability of destructive malware and the vulnerability of critical cyber systems make it likely that non-state actors will soon turn to cyber operations to attack states.

Once that occurs, states will become uneasy about relying entirely upon a law enforcement paradigm to combat serious cyber attacks mounted by non-state actors. On the contrary, the more severe and frequent the attacks, the more

---

67. *Nicaragua*, *supra* note 21, ¶ 195.

68. TALLINN MANUAL, *supra* note 2, at 57-58. Post-9/11, the UN Security Council, international organizations, and individual states took the stance that the right of self-defense applied. *See, e.g.*, S.C. Res 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001); S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001); Terrorist Threat to the Americas, Res. 1, OAS Doc. RC.24/RES.1/01 (Sept. 21, 2001); Brendan Pearson, *PM Commits to Mutual Defence,* AUSTRALIAN FIN. REV., Sept. 15, 2001, at 9; Press Release, NATO, Statement by the North Atlantic Council (Sept. 12, 2001) (on file with author).

69. Legal Consequences of Construction of Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9) [hereinafter *Wall*]; Oil Platforms, *supra* note 48, ¶¶ 146-47. A number of the ICJ's judges expressed concern with this position. *See, e.g.*, *Armed Activities*, *supra* note 48, ¶ 11 (Sep. Op. Judge Simma); *Wall*, *supra,* ¶ 33 (Sep. Op. Judge Higgins); *id.*, ¶ 35 (Sep. Op. Judge Kooijmans); *id.*, ¶ 6 (Decl. Judge Buergenthal).

70. *See, e.g.*, WHITE PAPER, *supra* note 66, at 2. *See also* Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, The Obama Administration and International Law, Address Before the Annual Meeting of the American Society of International Law (March 25, 2010), *available at* http://www.state.gov/s/l/releases/remarks/139119.htm [hereinafter ASIL Address]. The Dutch Government also openly supports this view. Government Response, *supra* note 7, at 5. For scholarly comment, see DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE, *supra* note 50, at 227-30; Schmitt, *Responding to Transnational Terrorism, supra* note 65, at 157.

likely states will be to reject the ICJ's cautiousness in lieu of the approach that appeared to have crystallized in the aftermath of the 9/11 attacks. Failure to act aggressively against highly destructive or injurious cyber attacks conducted by non-state actors will prove politically unpalatable and practically unworkable.

Finally, the disagreement that has surrounded the self-defense justification for cross-border drone operations against transnational terrorists has bleed-over effects in the context of cyber operations.[71] The question is whether a state may launch cyber operations against groups that have mounted armed attacks (cyber or kinetic) from other states or are currently located abroad.

The United States has adopted an interpretation of the law of self-defense that permits cross-border operations when the territorial state is either unwilling or unable to put an end to the use of its territory, as it is required to do by international law.[72] The rationale for this interpretation is especially compelling with respect to cyber operations because they can be launched from any location where connectivity to the target cyber system can be established. States in which the cyber attackers are located may lack the technical capability to detect the attacks and/or take those measures necessary to stop them. Additionally, cyber attacks unfold so rapidly that the targeted state may have no opportunity to notify the state from which the attacks emanate that they are underway and afford the latter the chance to take remedial measures.

In light of these and other realities, targeted states will increasingly find themselves confronted with situations in which the sole option for effectively defending themselves against an extraterritorial attack is immediate action, ei-

---

71. For a survey of the issue, see Michael N. Schmitt, *Extraterritorial Lethal Targeting: Deconstructing the Logic of International Law*, 52 COLUM. J. TRANSNAT'L L. 77 (2014).

72. The majority of the International Group of Experts supported this position. TALLINN MANUAL, *supra* note 2, at 59. For recent U.S. expressions of the approach, see THE WHITE HOUSE, FACT SHEET: U.S. POLICY STANDARDS AND PROCEDURES FOR THE USE OF FORCE IN COUNTERTERRORISM OPERATIONS OUTSIDE THE UNITED STATES AND AREAS OF ACTIVE HOSTILITIES (MAY 23, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism; John O. Brennan, Assistant to the President for Homeland Sec. and Counterterrorism, Remarks at the Program on Law and Security, Harvard Law School: Strengthening Our Security by Adhering to Our Values and Laws (Sept. 16, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an; President Barack Obama, Remarks at National Defense University, 2013 DAILY COMP. PRES. 361 (May 23, 2013); Koh, ASIL Address, *supra* note 70; WHITE PAPER, *supra* note 66, at 1-2. The approach reflects long-standing U.S. legal policy. *See, e.g.*, Letter Dated Aug. 20, 1998 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, U.N. Doc. S/1998/780 (Aug. 20, 1998); John B. Bellinger, III, Legal Adviser, U.S. Dep't of State, Legal Issues in the War on Terrorism, Address at the London School of Economics (Oct. 31, 2006), *available at* http://www.state.gov/s/l/2006/98861.htm; Sofaer, *supra* note 57, at 108. For academic discussion, see Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483 (2012); earlier academic treatment can be found in *Schmitt, Preemptive Strategies*, *supra* note 66, at 540-43.

ther against the attackers themselves or the cyber infrastructure which the attackers are using to carry out the attack. As a result, the logic of the "unwilling or unable" approach will become ever more evident.

IV. THE *JUS IN BELLO*

The *jus in bello*, and classic interpretations thereof, are likely to prove more resilient than the *jus ad bellum* when applied to cyber operations.[73] Most of the current norms have survived the test of time as new means and methods of warfare have been fielded. So too are they likely to withstand the appearance of cyber operations in the battlespace.[74]

Some normative evolution is, however, inescapable, for cyber operations are qualitatively different from their kinetic counterparts. Of particular relevance is the fact that the international humanitarian law governing the conduct of hostilities is premised on a paradigm in which most of the deleterious consequences that it seeks to temper are physically destructive or injurious. Cyber operations deviate from this underlying paradigm.[75] They may be launched far from the active battlespace, thereby raising concerns about the practical and normative borders of armed conflict. The ability to mask or spoof the origin of a cyber operation complicates the response options available to those targeted. Their effects can produce devastating, albeit non-destructive or injurious, consequences for the civilian population. And the fact that cyber operations rely heavily on cyber infrastructure that serves both military and civilian purposes affects the targetability of that infrastructure. However, the greatest evolutionary shift will occur with respect to the legal characterization of conflict and the law of targeting.

---

73. For survey articles on the subject, see Cordula Droege, *Get Off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94(866) INT'L REV. RED CROSS 533 (2012); Michael N. Schmitt, *Cyber Operations in the* Jus in Bello*: Key Issues,* 87 INT'L L. STUD. SERIES U.S. NAVAL WAR COLLECTION 89 (2011); Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 (846) INT'L REV. RED CROSS 365 (2002).

74. Doctrine has been developed for such operations. *See, e.g.*, JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-13: INFORMATION OPERATIONS, (Nov. 27, 2012), *available at* http://www.defenseinnovationmarketplace.mil/resources/12102012_io1.pdf.

75. The term "principles" refers to broad underlying notions of international humanitarian law from which specific "rules" of conduct are drawn. For instance, the principle of distinction requires an attacker to differentiate between combatants and protected persons. A derivative rule is that a civilian may not be attacked unless he or she is directly participating in hostilities.

A. *Conflict Characterization*

Cyber operations used during an ongoing armed conflict are governed by the law applicable to either international or non-international armed conflict.[76] This begs the question of whether an armed conflict of either genre can consist entirely of a cyber exchange.

International armed conflict, that is, armed conflict between two or more states, requires the resort to armed force between states.[77] It may also involve the use of armed force by a non-state organized armed group against a state so long as the group is acting under the overall control of another state.[78] There is no logical or legal basis for asserting the existence of a distinction between kinetic and cyber operations with respect to initiation of an international armed conflict when the latter can cause consequences on par with the former.

Obviously, not all cyber operations would constitute a resort to armed force. To be an "armed" force, hostilities (the "collective application of means and methods of warfare") have to take place.[79] The troublesome issue in this regard is whether actions resulting in severe non-destructive and non-injurious consequences qualify.[80] Although the question has generated fascinating de-

76. See discussion of the subject of characterization of cyber warfare in Michael N. Schmitt, *Classification of Cyber Conflict*, 89 INT'L L. STUD. 233 (2013).

77. Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

78. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment ¶¶ 131-40, 145 (Intl'l Crim. Trib. for the Former Yugoslavia July 15, 1999). *See also* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro.), 2007 I.C.J. 108, ¶ 404 (Feb. 26); Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on Confirmation of Charges, ¶ 211 (Jan. 29, 2007), http://www.icc-cpi.int/iccdocs/doc/doc266175.pdf. On the internationalization of a non-international armed conflict, see *Tadić*, Decision on Defence Motion, *supra* note 77, ¶ 76.

79. TALLINN MANUAL, *supra* note 2, at 74. *See also* INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 43 (Nils Melzer ed., 2009), *available at* http://www.icrc.org/eng/resources/documents/publication/p0990.htm.

80. Interestingly, the Dutch government appears to have taken a very liberal approach in this regard by endorsing a report which noted:

> A cyber attack that impacts civil or military computer systems and only results in the modification or destruction of non-essential data would not rise to the threshold of an armed conflict. Even if an attack has clear political, financial or economic consequences, such as the DDoS attack on Estonia in 2007, it would not be sufficient to breach the threshold of an armed conflict. Acts that have such consequences in the physical world are not subject to international humanitarian law either. However, if an organised cyber attack (or series of attacks) leads to the destruction of or substantial or long-lasting damage to computer systems managing critical military or civil infrastructure, it could conceivably be considered an armed conflict and international humanitarian law would apply. The same is true of a cyber attack that seriously damages the state's ability to perform essential tasks, causing serious and lasting harm to the economic or financial stability of that state and its people. An example would be a coordinated and organised attack on the entire computer network of the financial system (or a major part of it) leading to prolonged and large-scale disruption and instability that cannot easily be averted or alleviated by normal computer security systems.

bate,[81] it would seem sufficient to simply treat any cyber operation that amounted to an "attack" under IHL as crossing the hostilities threshold. As will be discussed, the precise meaning of "attack" in the cyber context is a contentious issue. But resolution of that matter would appear to equally resolve the instant issue without the need for interpretive creativity or normative sea changes.

The International Group of Experts achieved no agreement regarding the requisite quantum of damage or injury necessary to initiate an international armed conflict.[82] According to the ICRC *Commentaries* to the 1949 Geneva Conventions: "Any difference arising between two States and leading to the intervention of armed forces is an armed conflict . . . . It makes no difference how long the conflict lasts or how much slaughter takes place."[83] However, some of the Experts espoused a more restrictive position that entails "greater extent, duration, or intensity of hostilities."[84]

It is difficult to predict which of the approaches will prevail in the cyber context. On the one hand, the former is preferable if states wish to extend the protections of IHL to those persons and objects likely to be affected by cyber conflict. On the other, the latter has the benefit of limiting instances in which the operations are branded as international armed conflict, thereby avoiding the interstate instability that attends such characterizations. Given the trend toward increasing regulation of interstate violence, perhaps the ICRC view will, and should, enjoy the advantage.

The likelihood of cyber operations initiating a non-international armed conflict, that is, one between a non-state organized armed group and a state (or between two or more organized armed groups), is more remote.[85] A key obsta-

---

AIV/CAVV Report, *supra* note 40, at 24, endorsed by Government Response, *supra* note 7, at 4.

81. *See, e.g.*, Droege, *supra* note 73, at 546-49.

82. TALLINN MANUAL, *supra* note 2, at 74-75.

83. INT'L COMM. OF THE RED CROSS COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN ARMED FORCES IN THE FIELD 32 (Jean Pictet ed., 1952); INT'L COMM. OF THE RED CROSS, COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED, SICK AND SHIPWRECKED MEMBERS OF THE ARMED FORCES AT SEA 28 (Jean S. Pictet ed., 1960); INT'L COMM. OF THE RED CROSS, COMMENTARY: GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 23 (Jean Pictet ed., 1960); INT'L COMM. OF THE RED CROSS, COMMENTARY: GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 20 (Jean Pictet ed., 1958).

84. TALLINN MANUAL, *supra* note 2, at 74; *see also* Christopher Greenwood, *Scope of Application of Humanitarian Law*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 45, 57 (Dieter Fleck ed., 2d ed. 2008); Howard S. Levie, *The Status of Belligerent Personnel 'Splashed' and Rescued by a Neutral in the Persian Gulf Area*, 31 VA. J. INT'L L. 611, 613-14 (1991).

85. On cyber operations during a non-international armed conflict, see Robin Geiss, *Cyber Warfare: Implications for Non-International Armed Conflicts*, 89 INT'L L. STUD. 627 (2013); Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to

cle is that, unlike international armed conflict, non-international armed conflict requires significant hostilities—an act that would qualify as an attack under IHL does not necessarily suffice. It is well accepted, for example, that non-international armed conflict excludes "situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature."[86] Thus, "sporadic cyber incidents, including those that directly cause physical damage or injury, do not . . . constitute non-international armed conflict."[87]

Although non-state actors could in the future engage in hostilities that consist entirely of cyber operations meeting this intensity requirement, such actions would still have to satisfy a second criterion—organization. As the International Criminal Tribunal for the Former Yugoslavia noted in *Tadić*, a non-international armed conflict requires protracted armed violence between *organized* armed groups.[88] The International Group of Experts interpreted this requirement as satisfied when the group in question operates "under an established command structure and has the capability to sustain military operations."[89] Cyber operations conducted by individuals or by unorganized groups of "hackers," no matter how intense, do not fulfill the condition and, therefore, cannot qualify as non-international armed conflict.

Of particular note in this regard are groups organized virtually. Although the Experts opined that the failure of group members to meet physically does not preclude qualification as an organized armed group, the fact that members

---

the Protection of Victims of Non-international Armed Conflicts art. 1(1), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II].

86. Additional Protocol II, *supra* note 85, at 84. That the standard applies not only to Additional Protocol II situations, which require a degree of territorial control by the rebels forces, those encompassed by Common Article 3 to the four 1949 Geneva Conventions (that is, all non-international armed conflicts), is illustrated by inclusion of this level in the International Criminal Court Statute. Rome Statute of the International Criminal Court art. 8(f), July 17, 1998, 2187 U.N.T.S. 90. Common Article 3 is also set forth in the Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 3, Aug. 12, 1949, 6 U.S.T. 3114; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, art. 3, Aug. 12, 1949, 6 U.S.T. 3217; Convention Relative to the Protection of Civilian Persons in Time of War, art. 3, Aug. 12, 1949, 6 U.S.T. 3516; Convention Relative to the Treatment of Prisoners of War, art. 3, Aug. 12, 1949, 6 U.S.T. 3316.

87. TALLINN MANUAL, *supra* note 2, at 77.

88. *Tadić*, Decision on Defence Motion, *supra* note 78, ¶ 70. *See Lubanga*, *supra* note 79, ¶ 233; Rome Statute of the International Criminal Court, *supra* note 86, art. 8(2)(f). *See also* Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Judgment, ¶ 619 (Sept. 2, 1998); Prosecutor v. Bemba Gombo ICC-01/05-01/08, Decision on Confirmation of Charges, ¶ 229 (June 15, 2006); Prosecutor v. Norman, Case No. SCSL-2004-14-AR73, Decision on Appeal Against "Decision on Prosecution's Motion for Judicial Notice and Admission of Evidence," ¶ 32 (May 16, 2005) (Robertson, J., separate opinion); Prosecutor v. Rutaganda, Case No. ICTR-96-3-T, Judgment, ¶ 92 (Dec. 6, 1999); *Lubanga*, *supra* note 79, ¶ 233.

89. TALLINN MANUAL, *supra* note 2, at 79. *See also* Prosecutor v. Limaj, Case No. IT-03-66-T, Trial Chamber Judgment, ¶ 129 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 30, 2005).

may be operating in tandem, for instance by targeting particular objectives identified on the group's website, does not, in their view, necessarily suffice to meet the organization requirement. The group would have to operate cooperatively with a common purpose, be subject to the instructions of an acknowledged leadership, and, perhaps, have the means to implement IHL.[90] Most groups organized entirely online would not comply with these requirements.

There is no reason to suggest that the intensity criterion applicable in non-international armed conflict will soften. It would be illogical to submit that the use of cyber means and methods of warfare necessitates a lowering of the bar currently applicable to kinetic operations. However, the formation of groups organized entirely online for, e.g., social, economic, and academic purposes may presage the formation of virtual groups for the purpose of conducting cyber hostilities against a state. One need only consider the effectiveness of cooperative online operations directed against Estonia in 2007 and Georgia in 2008, as well as the success of groups like Anonymous, to realize the potential for highly destructive or injurious cyber operations by groups that do not meet current criteria for organization. Should such groups begin to engage in sufficiently intense operations, states are certain to begin interpreting the organizational requirements for non-international armed conflict with greater liberality.

B. *Attacks*

The most widely discussed issue regarding cyber operations during both international and non-international armed conflict is that of the meaning of "attack."[91] The concept is primarily relevant in the context of the principle of distinction.[92] This customary law principle, codified in Article 48 of Additional Protocol I to the 1949 Geneva Conventions, requires parties to a conflict to "at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly direct their operations only against military objectives."[93]

---

90. *See* Schmitt, *Classification of Cyber Conflict*, *supra* note 76, at 246; *see also* INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 4470 (Yves Sandoz et al. eds., 1987) [hereinafter Additional Protocols Commentary] (referring to the requirement in Additional Protocol II, *supra* note 85, art. 1(1). It is unclear whether the implementation requirement applies beyond Additional Protocol II to all non-international armed conflicts.).

91. *See, e.g.*, Droege, *supra* note 73, at 24-28; Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, *in* PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283, 289-93 (Christian Czosseck et al. eds., 2012).

92. On distinction in the cyber context, see Robin Geiß & Henning Lahmann, *Cyber-Warfare: Applying the Principle of Distinction in an Interconnected Space*, 45 ISR. L. REV. 381 (2012); Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, 89 INT'L L. STUD. 252 (2013).

93. Additional Protocol I, *supra* note 5, art. 48. The ICJ has recognized the principle as one of two "cardinal" principles of IHL (the other being the prohibition of unnecessary suf-

Distinction has been operationalized in a number of Additional Protocol I provisions, many of which reflect customary international law. For instance, Article 51 prohibits making the civilian population or individual civilians the object of attack, conducting indiscriminate attacks, mounting terror attacks, and engaging in reprisal attacks against civilians; Article 52 bans attacks on civilian objects; Article 54 prohibits attacking objects indispensable to the survival of the civilian population; Article 55 outlaws reprisal attacks against the natural environment; and Article 56 limits attacks on works or installations containing dangerous forces.[94] Additional Protocol I and customary international law also provide guidance on how attacks may be conducted. Of particular note are the proportionality and precautions in attack requirements.[95]

Since each of these prescriptive norms applies fully to cyber operations, the meaning of attack is critical because humanitarian law's prohibitions and requirements apply only to cyber operations that qualify as such. Additional Protocol I defines the term in Article 49(1): "'Attacks' means acts of violence against the adversary, whether in offence or in defence."[96] This definition sufficed in an era in which attacks were carried out almost exclusively by kinetic means, for such means are by nature violent. Cyber operations have complicated matters in that they can be highly useful militarily without generating destructive or injurious effects.

The result has been a long and somewhat formalistic debate. On the one hand, some IHL specialists have taken a narrow approach that limits the scope of attacks to military operations that result in damage or injury.[97] These commentators focus on the plain meaning of the text, as well as the prevailing understanding of the concept among states. Others have taken a broader approach that extends the concept to certain nondestructive or injurious operations.[98] They emphasize the nonbinding ICRC *Commentary* to the key Additional Protocol I articles.

---

fering). *Nuclear Weapons*, *supra* note 5, ¶ 78. As to its customary character, see INT'L COMM. OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 1-34 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005), *available at* http://www.icrc.org/eng/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf [hereinafter Customary IHL].

94. Additional Protocol I, *supra* note 5, arts. 51-52, 54-56; Customary IHL, *supra* note 93, at 1, 9, 25, 37, 139, 189.

95. Additional Protocol I, *supra* note 5, arts. 52, 57; Customary IHL, *supra* note 93, at 46, 51; *see also* Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INT'L L. STUD. 198 (2013).

96. Additional Protocol I, *supra* note 5, art. 49(1).

97. The lead article advocating this view is Michael N. Schmitt, *Wired Warfare: Computer Network Attack and International Law, supra* note 73, at 365-99 (2002). The author has since moderated his views to accord with the functionality approach set forth in the *Tallinn Manual*.

98. The lead article advocating this view is Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, INT'L COMM. OF THE RED CROSS (Nov. 19, 2004), http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

Both approaches have strengths and weaknesses. Neither garnered unanimous support among the International Group of Experts. All that could be agreed upon was the Rule that a cyber operation, whether in offense or defense, "that is reasonably expected to cause injury or death to persons or damage or destruction to objects" qualifies as an attack.[99] Of course, *de minimis* damage or destruction does not meet this threshold.

Some Experts opined that, there being no state practice on the issue, the current law limits the term to physical harm caused to persons and tangible objects. However, the majority took the position that a reasonable interpretation of "attack" in the cyber context would include "interference by cyber means with the functionality of an object."[100] For them, a cyber operation that necessitates repair of the target cyber infrastructure qualifies as an attack. They cited the example of a cyber operation against an electrical distribution grid's computer-based control system in which functionality can only be restored by replacement of the system or its components. A number of these Experts extended the definition to encompass cyber operations requiring reinstallation of the operating system of target cyber infrastructure. Others went further still by arguing that cyber infrastructure is "damaged" (and thus "attacked") whenever functionality necessitates data restoration. In the last approach, the key to the concept of attack is the target's "loss of usability."[101] No one suggested that a mere denial of service with a cyber operation that did not at least alter or destroy data qualified as an attack.

In resolving the differences, it must be understood that interpretation of legal norms should be based on the object and purpose of the norm in question, as it is understood in the contemporary context.[102] This is especially true with respect to IHL, which must maintain valence in the face of emergent methods and means of warfare. The object and purpose approach to the interpretation of IHL entails finding the appropriate balance between military necessity and humanitarian concerns in light of the nature of present-day conflict and the values that states wish to protect.[103]

This dynamic is the key to understanding how the term attack is likely to be interpreted in the future. Given the pervasive importance of cyber activities, an interpretation that limits the notion of attacks to acts generating physical effects cannot possibly survive. Suggestions that civilian activities may lawfully be seriously disrupted or that important data can be altered or destroyed because there is no resulting physical damage or injury will surely collide with future assessments of the military necessity/humanitarian considerations bal-

99. TALLINN MANUAL, *supra* note 2, at 92.

100. *Id*. at 93.

101. *Id*. at 93-94.

102. Vienna Convention on the Law of Treaties, art. 31, May 23, 1969, 1155 U.N.T.S. 331.

103. *See generally* Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance,* 50 VA. J. INT'L L. 795 (2010).

ance. This is particularly so given the difficulty of fashioning arguments that the disruption of civilian activities yields direct military advantage.

The more challenging question is how such protection will be realized.[104] It would seem apparent that a prophylactic ban on directing cyber operations against civilian activities and data is implausible. For instance, non-destructive psychological operations directed at the civilian population are common and lawful. When effective, they can even minimize civilian casualties and damage to civilian property, hasten the end of the conflict, or enhance security during occupations. States are unlikely to countenance the emergence of any norm that would preclude conducting such actions by cyber means. Moreover, no norm is likely to materialize that bars cyber operations when they only cause inconvenience or interference with non-essential services and activities. War is ordinarily disruptive for the civilian population; it would mark a revolution in IHL theory to suggest that any disruption of civilian activities is prohibited.

Perhaps the likeliest prospect is an eventual expansion of the notion of attack to include interference with essential civilian functions. The difficulty with such an approach is that the notion of attack does not currently contain a severity of consequences component other than the exclusion of *de minimis* damage or injury. Rather, it focuses on the nature of the harm—damage, destruction, injury, or death. This fact may cause formalists disquiet. Yet, there are but two alternatives: 1) the emergence of a new norm through treaty law, an unlikely prospect given the difficulty of treaty promulgation; or 2) crystallization of a customary norm, a process which runs counter to the current trend towards codification and which is, in any event, unwieldy and indeterminate.

A more plausible prospect is that states will simply begin to treat operations against essential civilian services and data as attacks by refraining from conducting them and condemning those who do, thereby creating the state practice upon which an evolution in meaning can be based. Of course, the devil is in the details. Some activities, like banking and operation of critical civilian infrastructure, are evidently essential. Beyond that, and although scholarly comment and the explicative projects by the ICRC may speed the process, only state practice will definitively pinpoint those civilian activities and data that qualify as essential.

The trend towards greater protection for essential civilian activities and data will reverberate throughout the IHL provisions governing the conduct of attacks. In particular, application of the rule of proportionality is likely to be affected. This customary norm, codified in Articles 51 and 57 of Additional Protocol I, prohibits "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military

104. On the threshold of harm question, see Lubell, *supra* note 92, at 264-74.

advantage anticipated."[105] The interpretation of the terms "damage" and "objects" will likely evolve.

The notion of damage in the proportionality context will probably expand beyond a strict limitation to physical effects. Recall that most members of the International Group of Experts effectively took this position by accepting certain effects on the functionality of cyber infrastructure as an attack. Eventually, damage will analogously also probably be understood as including interference, albeit, for the reasons outlined above, only with regard to essential services and data. Once this occurs, such consequences will have to be taken into account when an attacker is assessing whether expected collateral damage is excessive relative to the military advantage that the cyber operation is anticipated to achieve.

It is foreseeable that a concomitant shift will occur in the meaning attributed to the term "objects" in the rule of proportionality. Reinterpretation will also shape the prohibition on attacking civilian objects, as well as the customary rule set forth in Article 57 requiring attackers to take precautions to spare civilian objects.[106]

The ICRC *Commentary* to the Additional Protocols describes an object as something that is "visible and tangible."[107] Data does not fit easily into this description, nor does the ordinary meaning[108] of the term "object" include data. Accordingly, the majority of the International Group of Experts was unwilling to expand the concept of objects to data, at least as a matter of *lex lata*.[109]

This view is unlikely to endure. Today, the importance of data usually exceeds that of their physical manifestation. In fact, the existence of data serves to diminish the significance of corresponding physical objects. To take a simple example, most governments maintain digital copies of records for activities such as census taking, the provision of social benefits, voting, taxation, and so forth. Loss of the digitized records would be a much greater impediment to the continuation of governmental functions than would destruction of their physical equivalents; indeed, in the future there will be no "hard copy" records. IHL will assuredly evolve to meet the shift in the relative importance of physical and virtual data.

---

105. Additional Protocol I, *supra* note 5, art. 51(5)(b). *See* Customary IHL, *supra* note 94, at 46.

106. Additional Protocol I, *supra* note 5, arts. 52, 57(1); Customary IHL, *supra* note 94, at 25, 51.

107. Additional Protocols Commentary, *supra* note 90, ¶ 2008.

108. This legal standard of interpretation is found in the Vienna Convention, *supra* note 102, art. 31(1).

109. TALLINN MANUAL, *supra* note 2, at 187. While some members were willing to characterize data upon which cyber infrastructure relies as an object, doing so distorts the law. The cyber infrastructure itself, not the data, is the object. Its loss of functionality constitutes the damage to be considered in proportionality calculations.

However, as with the definition of attack, care must be taken to avoid definitional overreach. Treating all data as objects would have the effect of precluding any operation directly targeting civilian data. As noted with respect to psychological operations, states are unlikely to surrender their ability to conduct certain types of cyber activities that are meant to have effects on the civilian population. Similarly, it is difficult to imagine states accepting an interpretation of objects that requires any loss of civilian data to be treated as collateral damage or as engaging the precautions in attack requirements. Ultimately, the most that can be anticipated is that states will increasingly treat data upon which the essential civilian services rely as civilian objects immune from direct attack and subject to the proportionality limitation and precautions-in-attack requirement.

Finally, the so-called "dual use" issue looms particularly large in the cyber context. A dual use object is one used for both military and civilian purposes. It is well accepted in IHL that once a civilian object begins to be used for military purposes it becomes a lawful military objective.[110] The extent of military use is irrelevant; so long as the object is being employed militarily, it qualifies as a military objective subject to attack.[111]

The dilemma is that much of the existing cyber infrastructure is already dual-use in nature, and this will not change in the future. For instance, military communications occur in part across cables and other media that are also used for civilian traffic. Weapons often rely on data generated by the Global Positioning Satellite (GPS) system, which serves civilian purposes such as navigation. Social media like Facebook and Twitter have been widely used during recent conflicts to transmit militarily important information. Militaries are also increasingly turning to "off the shelf" equipment like commercial computer systems for their forces, thereby qualifying the factories which produce the products as military objectives.

This reality was the source of extensive consideration by the International Group of Experts, which concluded, "all dual-use objects and facilities are military objectives, without qualification."[112] Any protection the civilian aspects of the targeted dual use cyber infrastructure enjoy derives from application of the principle of proportionality and the requirement to take precautions in attack. In particular, the Experts noted, "an attack on the internet itself, or large portions thereof, might equally run afoul of the principle of proportionality."[113]

It is doubtful that this view will continue to prevail as military reliance on civilian cyber infrastructure grows. With states struggling to maintain military forces and capabilities in the face of declining budgets, it will be difficult to

110. Additional Protocol I, *supra* note 5, art. 52(2); Customary IHL, *supra* note 93, at 29.

111. TALLINN MANUAL, *supra* note 2, at 112.

112. *Id*. at 113.

113. *Id*. at 114.

justify funding the maintenance of separate cyber networks or the acquisition of products designed specifically for military purposes. This reality will place states on the horns of a dilemma. On the one hand, they will want to deprive their enemies of the usage of dual-use cyber infrastructure. On the other, states will want to immunize that cyber infrastructure upon which their civilian population and its activities rely. It is unclear how this classic military necessity/humanity conflict will be resolved.

CONCLUDING THOUGHTS

International law is designed to govern the present and shape the future. And so it shall. However, the face of conflict has been fundamentally transformed by the advent of cyber operations. As Yogi Berra is said to have mused: "The future ain't what it used to be." That is the dilemma. Not only does cyber warfare create effects that the extant law did not envisage, but it also strikes at values, such as connectivity, that were unimaginable at the time the law was drafted. Evolutionary change in the normative architecture governing international security and armed conflict is, simply put, unpreventable.

This being so, the question is "*quo vadis*?" The thread of logic running through this article is that as cyber activities become ever more central to the functioning of modern societies, the law is likely to adapt by affording them greater protection. It will impose obligations on states to act as responsible inhabitants of cyberspace, lower the point at which cyber operations violate the prohibition on the use of force, allow states to respond forcefully to some non-destructive cyber operations, and enhance the protection of cyber infrastructure, data, and activities during armed conflicts. These shifts will not be cost-free. They may, *inter alia*, prove expensive, affect privacy interests, extend to kinetic operations, and deprive battlefield commanders of options previously available to them. Ultimately, though, law reflects national interests. States will inescapably eventually find it in their interests to take such measures to protect their access to cyberspace and the goods it bestows.