2015

Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures

Christopher S. Yoo
University of Pennsylvania Law School, csyoo@law.upenn.edu

Cyber Espionage or Cyber War?: International Law, Domestic Law, and Self-Protective Measures

Christopher S Yoo*

I. INTRODUCTION

The academic discourse on cyberspace followed a pattern that is now well recognized. Early scholarship embraced cyber exceptionalism, pronouncing that the internet's inherently transnational character transcended traditional notions of sovereignty and made it inherently unregulable by nation states.[1] Others disagreed, arguing that the internet fell comfortably within established legal principles.[2] Although President Clinton once confidently stated that China's attempt to crack down on the internet was "like trying to nail Jell-O to the wall,"[3] history has largely proven him wrong. As of today, belief in the internet's unregulability is now essentially defunct, at least with respect to law.[4]

The same debate over internet exceptionalism is currently playing out in the scholarship on international law, albeit with a much more skeptical tone. Early scholarship generally took the position that established international law principles governing when it is appropriate to go to

* The author would like to thank Jonathan Smith, who has been instrumental in shaping my thinking about cyber war, and Jean Galbraith and Bill-Burke White for comments on earlier drafts. The chapter also benefitted from presentations at the 8th Annual Symposium of the Global Internet Governance Academic Network held in conjunction with the Internet Governance Forum, as well as the Roundtable on "Cyberwar and the Rule of Law," the Philadelphia Area Cyberlaw Colloquium, and the Conference on "Invisible Harms: Intellectual Property, Privacy, and Security in a Global Network," all held at the University of Pennsylvania.

[1] See, for example, John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, February 8, 1996, at <https://projects.eff.org/~barlow/Declaration-Final.html>; David Johnson and David Post, "Law and Borders—The Rise of Law in Cyberspace," (1996) 48 *Stanford Law Review*1367, 1375.

[2] See, for example, Frank H. Easterbrook, "Cyberspace and the Law of the Horse," (1996) *University of Chicago Legal Forum* 207; Jack L. Goldsmith, "Against Cyberanarchy," (1998) 65 *University of Chicago Law Review* 1199.

[3] William J. Clinton, Remarks at the Paul H. Nitze School of Advanced International Studies, March 8, 2000, in *Public Papers of the President of the United States: January 1 to June 26, 2000* (2000) 404, 407.

[4] See, for example, Alex Kozinski and Josh Goldfoot, "A Declaration of the Dependence of Cyberspace," (2009) 32 *Columbia Journal of Law & the Arts* 365; Tim Wu, "Is Internet Exceptionalism Dead?" in Berin Szoka and Adam Marcus (eds), *The Next Digital Decade: Essays on the Future of the Internet* (Washington, DC: TechFreedom, 2010) 179, 179–82, at <http://nextdigitaldecade.com/ndd_book.pdf>.

war (jus ad bellum) and the appropriate ways that war may be conducted (jus in bello) applied to cyber conflicts.[5] By September 2012, US State Department Legal Advisor Harold Koh could confidently declare that established principles of international law apply to cyberspace.[6] More recently, scholarship has begun to raise doubts about this conclusion.[7] Even those confident about the application of international law to cyber conflicts acknowledge that some types of cyber operations do not fit easily into the traditional categories.[8]

This chapter will explore how these two bodies of international law governing conflicts between states applies to cyber operations, using as its lens prominent examples that have been in the news of late. These include the surveillance programs alleged by Edward Snowden to have been conducted by the National Security Agency (NSA), the 2007 and 2008 distributed denial of service attacks launched by Russian hackers against Estonia and Georgia that disrupted their communications networks without damaging any property, and the 2008 Stuxnet virus introduced into a key Iranian nuclear facility that caused the centrifuges used to enrich uranium to accelerate and decelerate unexpectedly and eventually to destroy themselves. In addition, this chapter will examine the type of practices described in a 1999 book entitled *Unrestricted Warfare*, in which two Colonels of the Chinese People's Liberation Army (PLA) describe ways that a country in the position of China in the late 1990s could defeat an opponent that was in a stronger economic and technological position. The tactics describe in the book include lawfare

[5] See, for example, Michael N Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," (1999) 37 *Columbia Journal of Transnational Law* 885; Walter Gary Sharp, Sr, *CyberSpace and the Use of Force* (Falls Church, VA: Aegis Research Corp, 1999).
[6] Harold Hongju Koh, Legal Advisor, US Department of State, "International Law in Cyberspace," Remarks, before the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland, September 18, 2012, at <http://www.state.gov/s/l/releases/remarks/197924.htm>.
[7] See Susan W. Brenner and Leo L. Clarke, "Civilians in Cyber war: Conscripts," (2010) 43 *Vanderbilt Journal of Transnational Law* 1011; Jack M. Beard, "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law," (2014) 47 *Vanderbilt Journal of Transnational Law* 67.
[8] See, for example, Sharp (n 5); Koh (n 6).

(ie, the use of international and multilateral organizations to subvert an opponent's policies), manipulation of trade, manipulation of financial transactions, as well as network warfare (cyberwarfare) targeted at a nation's financial and communications systems, just to name a few.[9]

Section II applies current principles as understood through the *Tallinn Manual on the International Law Applicable to Cyber Warfare* produced by a special Independent Group of Experts (IGE) convened by NATO, concluding that jus ad bellum and jus in bello as well as the customary international law of non-intervention will not reach much, if any, of this behavior. Instead, such conduct is relegated to the law of espionage, described in section III, which is governed almost entirely by domestic law. The absence of an overarching legal solution to this problem heightens the importance of technological self-protective measures, described in section IV.

II. THE APPLICABILITY OF JUS AD BELLUM, JUS IN BELLO, AND NON-INTERVENTION

The law of war is dominated by two bodies of law that govern hostile activities among states.[10] Jus ad bellum determines when a use of force is justified. Jus in bello governs how states should conduct themselves during periods of armed conflict. The literature exploring these concepts is too voluminous to cite comprehensively and will only be sketched here, primarily by referring to the leading primary sources of international law as well as the interpretation offered by the *Tallinn Manual* as to how these principles will apply to cyber operations. Admittedly, the exposition presented in the *Manual* glosses over many important ongoing debates. As the leading

[9] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization* (Beijing: PLA Literature and Arts Publishing House, 1999).

[10] To date the scholarly debate has focused primarily on the application of these two areas of law to cyber war. That said, they do not represent the only relevant bodies of international law. For example, some scholars have begun to explore the extent to which human rights treaties govern electronic surveillance. See, for example, Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age," (forthcoming) 56 *Harvard International Law Journal*, draft available at http://ssrn.com/abstract=2418485.

source on how the law of war applies to cyber conflicts, it does provide an important cornerstone for analysis.

As we shall see, the threshold determination for the applicability of jus ad bellum and jus in bello has been whether the damage to persons or property is analogous to those inflicted by traditional kinetic war. This standard leaves many of the types of cyber operations that have raised the greatest concern outside the scope of the law of war.

(a) Jus ad Bellum

Although the principles on when international law permits nations to go to war have a long history, the starting point for modern analysis is the Charter of the United Nations. Although the Charter is by no means the only relevant source of law, the International Court of Justice (ICJ) has recognized that the Charter's restrictions on the use of force have become part of the customary international law of jus ad bellum.[11]

Two provisions of the UN Charter have particular importance. Article 2(4) of the Charter specifically bans the use of force against other states when it provides, "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 recognizes certain exceptions to the prohibition of the use of force. In particular, Article 51 recognizes that nothing in the Charter abrogates states' "inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."

[11] Military and Paramilitary Activities in and Against Nicaragua (*Nicaragua v US*), 1986 ICJ 14, paras 188–90 (June 27).

In addition to jus ad bellum, nations are also subject to the duty of nonintervention. Article 2(1) recognizes the "principle of sovereign equality" among UN members, which implies a principle of nonintervention preventing other states from taking actions that deprives another state of the ability to control governmental matters implicit in being a state. Although the precise contours of what constitutes intervention have long been the subject of extensive debate, the ICJ has recognized that intervention is wrongful when it constitutes coercion.[12]

The key concepts are thus the conduct that is prohibited by Article 2(4) (threat or use of force) and the occurrence that triggers the Article 51 exception to that prohibition (armed attack) as well as the threshold for the principle of nonintervention implicit in Article 2(1) (coercion). Although the most aggressive forms of cyber operations would fall within the scope of these terms, many forms of cyber surveillance and interference would not.[13]

i. Use of force

We begin our analysis with the use of force, which is the primary conduct prohibited by Article 2(4). No treaty provides a definition of the use of force, although the UN Charter does provide some guidance. For example, other Charter provisions offer guidance as to the types of conduct that fall within Article 2(4). The Charter's preamble clearly stated the signatory nations' determination "to save succeeding generations from the scourge of war" by "ensur[ing] . . . that armed force shall not be used, save in the common interest." This language is generally regarded as establishing that armed military operations within another country would constitute a use of force prohibited by Article 2(4). Furthermore, in describing measures that the Security Council may take that do "not involve[e] the use of armed force," Article 41 specifically includes the

[12] ICJ *Nicaragua* judgment, para 205.
[13] For other enlightening discussions, see also Watts (Chapter 4, this volume), Blank (Chapter 5, this volume), and Hollis (Chapter 6, this volume).

"complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication." This suggests that not all disruptive operations constitute the use of force.

The *travaux préparatoire* of Article 2(4) reveals that the San Francisco Conference specifically rejected an amendment that would have included economic coercion within the scope of the use of force prohibited by Article 2(4).[14] Moreover, when considering a draft containing language that paralleled Article 2(4), the UN Commission on Friendly Relations rejected arguments that all forms of political and economic pressure fell within its scope.[15]

This interpretation is reinforced by principles of customary international law, particularly the aspect of ICJ's *Nicaragua* judgment rejecting Nicaragua's claim that US funding of the contras constituted an impermissible use of force. Although the ICJ lacked the jurisdiction to determine whether those actions violated Article 2(4) of the UN Charter, it did have the authority to determine whether the actions taken by the US violated customary international law. The ICJ concluded that "organizing or encouraging the organization of irregular forces or armed bands . . . for incursion into the territory of another State" and "participating in acts of civil strife . . . in another State" did constitute an impermissible use of force. At the same time, the ICJ ruled that "the mere supply of funds to the *contras* . . . does not in itself amount to a use of force."[16]

---

[14] 6 UN CIO Docs. 334, 609 (1945); Doc. 2, 617 (e) (4), 3 UN CIO Docs. 251, 253–4 (1945). This drafting history also rebuts arguments that the use of the term "force" without the word "armed" in Article 2(4) suggested that Article 2(4) prohibits economic coercion that does not rise to the level of military action. This underscores that the primary impetus for the creation of the UN was to outlaw armed conflict as a legitimate instrument for effectuating national policy rather than to insulate countries from all imbalances in economic bargaining position. See Tom J Farer, "Political and Economic Coercion in Contemporary International Law," (1985), 79 *American Journal of International Law* 405, 410; Schmitt (n 5) 905; Marco Roscini, "World Wide Warfare—Jus ad Bellum and the Use of Cyber Force," (2010) 14 *Max Planck Yearbook of United Nations Law* 85, 105.

[15] UN GAOR Special Comm. on Friendly Relations, UN Doc. A/AC.125/SR.110 to 114 (1970); Rep. of the Special Comm. On Friendly Relations and Cooperation among States, 1969, UN GAOR, 24th Session, Supp. No 19, at 12, UN Doc. A/7619 (1969).

[16] ICJ *Nicaragua* judgment, para 228.

The *Tallinn Manual* drew guidance from the ICJ's focus on scale and effects when determining whether conduct constituted an armed attack. Moreover, the IGE that authored the *Tallinn Manual* took note of the historical materials indicating that the use of force excluded mere economic and political pressure and concluded that cyber operations analogous to such activities, such as psychological operations or funding a hacktivist group, did not constitute uses of force, nor would providing sanctuary or safe haven for those mounting cyber operations unless coupled with other acts.[17] Actions taken by a state's intelligence agency or a contractor whose conduct is attributable to a state can constitute a use of force despite the fact that it was not undertaken by the state's armed forces.[18]

The heart of the *Tallinn Manual*'s proposal was to identify cyber operations to kinetic operations that the international community would clearly recognize as uses of force, including all conduct that rose to the level of armed attack and acts that injure or kill persons or damage or destroy objects.[19] For other cases, the IGE put forward eight nonexclusive factors to guide the inquiry: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality.[20] The *Manual* observed that "actions such as disabling cyber security mechanisms in order to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force."[21]

Measured against this standard, the type of surveillance described in the classified documents disclosed by Edward Snowden, lacking as it did any injury to people or property, would not likely rise to the level to constitute a use of force. Similarly, the use of lawfare or

[17] Michael N Schmitt (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013) 47–9.
[18] Schmitt (n 17) 46.
[19] Schmitt (n 17) 49.
[20] Schmitt (n 17) 49–52.
[21] Schmitt (n 17) 50–1.

economic warfare through the erection of trade barriers or financial transactions would almost certainly not constitute uses of force. Presumably neither would the partial disruption of communications recognized by Article 41 of the UN Charter. And, as we shall see in subsection ii, intrusion into another state's systems by breaching firewalls and cracking passwords fails to violate nonintervention; because that standard is lower than the standard governing the use of force, *a fortiori* this type of conduct does not constitute use of force.

Attacks on a nation's financial or cyber infrastructure of the type envisioned by *Unrestricted Warfare* are a matter of degree. Temporary denial of service would be insufficient to constitute a use of force even if highly invasive. At the same time, "some may categorize massive cyber operations that cripple an economy as a use of force even though economic coercion is presumptively lawful."[22] The *Tallinn Manual* does, moreover, presume that Stuxnet constituted a use of force,[23]

ii. Self-defense

Another key concept under traditional international law is when a state may act in self-defense. As noted earlier, a nation may exercise its inherent right of self-defense under Article 51 of the UN Charter when confronted with an armed attack.

Because the UN Charter does not provide a definition of armed attack, customary international law and treaty law coexist side by side.[24] The ICJ's *Nicaragua* judgment distinguished between "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms" and noted that "measures which do not constitute an armed

[22] Schmitt (n 17) 55–6.
[23] Schmitt (n 17) 47.
[24] ICJ *Nicaragua* judgment, para 176.

attack . . . may nevertheless involve a use of force."[25] In so doing, the ICJ recognized that armed attack is a subset of the use of force. Thus, while all forms of armed attack constitute uses of force, not all uses of force constitute armed attacks. This in turn implies that states may be the targets of operations that are sufficiently severe to constitute uses of force that are illegal under Article 2(4), but not sufficiently severe to justify responding in kind under Article 51.[26]

The ICJ further noted that in addition to sending regular forces across an international border, armed attack also includes "'sending . . . 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.'"[27] The ICJ further observed that some instances of sending armed bands into the territory might represent "a mere frontier incident" rather than an armed attack.[28] In short, whether particular conduct constitutes an armed attack depends on its "scale and effects."[29] The ICJ seemed to entertain the possibility that a series of smaller actions might constitute an armed attack if considered together.[30] Any actions taken in self-defense to an armed attack are subject to the customary international law requirements of necessity and proportionality.[31]

In applying these principles to cyberspace, the commentary on Rule 13 governing self-defense against armed attack noted that the IGE "unanimously concluded that some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the

---

[25] ICJ *Nicaragua* judgment, paras 191, 210; see also Oil Platforms (*Iran v US*), judgment, 2003 ICJ 161, paras 51, 64 (November 6).
[26] Michael N Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context," in Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict (CYCON 2012)* (Tallinn, Estonia: NATO CCD COE Publications, 2012), 283, 286–7.
[27] ICJ *Nicaragua* judgment, para 195 (quoting Declaration on the Definition of Aggression, GA Res. 3314 (XXIX), UN Doc A/RES/29/3314 (December 14, 1974)).
[28] ICJ *Nicaragua* judgment, para 195.
[29] ICJ *Nicaragua* judgment, para 195.
[30] ICJ *Oil Platforms* judgment, para 64.
[31] ICJ *Nicaragua* judgment, paras 176, 194; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226, para 41 (July 8); ICJ *Oil Platforms* judgment, paras 43, 74, 76.

meaning of the Charter."[32] A majority of the IGE agreed that the term "armed" did not require the employment of weapons.[33] The IGE concurred that to constitute an armed attack, conduct must exceed the scale and effects needed to qualify as a use of force.[34] On the one hand, the IGE agreed that any force that injures or kills persons or damages or destroys property would have sufficient scale and effects to constitute an armed attack. On the other hand, the IGE also agreed that acts of cyber intelligence, cyber theft, and brief or periodic interruptions of nonessential cyber services do not constitute armed attacks.[35]

How to characterize intermediate cases divided the IGE. Some members held that some harm to persons or property is necessary for an incident to be considered an armed attack, while others focused on the severity of the broader effects.[36] For example, some would describe a cyber assault on the New York Stock Exchange as mere financial loss that did not rise to the level of armed attack, while others focused on the catastrophic effects of such an attack.[37] The IGE also disagreed as to the role of intent, with a majority focusing exclusively on scale and effects and a minority refusing to characterize cyber espionage that unexpectedly inflicted significant damage to another state's cyber infrastructure as an armed attack.[38]

The *Tallinn Manual* included rules imposing principles of necessity, proportionality, imminence, and immediacy.[39] But application of these rules to cyber conflicts proved controversial. The debate over imminence provides an apt illustration. Although Article 51 on its face applies when "an armed attack occurs," a majority of the IGE held that a state may defend itself against armed attacks that are "imminent," while a minority rejected the concept of

[32] Schmitt (n 17) 54.
[33] Schmitt (n 17) 54.
[34] Schmitt (n 17) 54.
[35] Schmitt (n 17) 55.
[36] Schmitt (n 17) 55.
[37] Schmitt (n 17) 55.
[38] Schmitt (n 17) 56.
[39] Schmitt (n 17) 59–63.

anticipatory self-defense.[40] While the IGE agreed that the speed of cyber operations dictated that a state need not wait until an attack had already been launched before responding, a minority would have required that an attack be about to be launched, while a majority "rejected this strict temporal analysis" in favor a "last feasible window of opportunity" standard that permits self-defense when failure to act would reasonably leave a state unable to defend itself effectively once the attack commences.[41]

Although the *Tallinn Manual* found it "indisputable" that actions of non-state actors may constitute an armed attack if undertaken under the direction of a state, the IGE divided over the legal implications of such actions in the absence of any direction by a state. A majority concluded that state practice supported the exercise of the right of self-defense against non-state actors such as terrorists and rebel groups, which in the cyber context would extend to actions taken by information technology corporations, while a minority disagreed.[42]

If the state from which the non-state actors are launching their cyber armed attack (which the *Tallinn Manual* calls the territorial state) consents, the victim state may take self-defensive actions against non-state actors within the territorial state.[43] The IGE divided on how to address situations in which the territorial state does not consent to self-defensive actions by the victim state, but remains unable or unwilling to stop the cyber armed attack. A majority of the IGE concluded that self-defensive actions by the victim state within the territorial state are permissible as a result of the duty of each state to ensure that its territory is not used to violate international law.[44] When confronted with such an attack, the victim state may ask the state from which the non-state cyber operations constituting a cyber armed attack are emanating (called the

[40] Schmitt (n 17) 60–61.
[41] Schmitt (n 17) 61.
[42] Schmitt (n 17) 56–57.
[43] Schmitt (n 17) 26, 58.
[44] Schmitt (n 17) 58.

territorial state) to address the situation.[45] A minority disagreed, arguing that such actions were impermissible absent an action based on a plea of necessity.[46]

How would these principles apply to the real world examples under consideration? The *Tallinn Manual* concluded that as of 2012, no cyber incidents had occurred that had generally been recognized as constituting an armed attack, including the 2007 cyber operations against Estonia.[47] Under these standards, because the surveillance programs described in the documents disclosed by Edward Snowden did not represent a use of force, *a fortiori* it also did not constitute an armed attack. If, as noted already, monitoring keystrokes did not rise to the lower standard of the use of force, it necessarily did not constitute an armed attack. Moreover, courts would likely not categorize the types of operations suggested by *Unrestricted Warfare*, lawfare and economic warfare through manipulation of trade or the financial transactions as armed attacks. Whether direct actions against the financial infrastructure itself that caused it to crash would meet the standard of armed attack divided the IGE.

Most interestingly, the IGE did not regard Stuxnet, often regarded as the strongest real-world candidate for being classified as an armed attack, as completely clear. Although the *Tallinn Manual* indicates that some IGE members believed that the damage to the Iranian centrifuges was sufficient to reach the level of armed attack,[48] the clear implication is that other IGE members thought otherwise.

(b). Nonintervention/coercion

Customary international law has long recognized the principle of nonintervention to be implicit in the principles of sovereignty and the equality among nations. In its *Nicaragua*

[45] Schmitt (n 17) 59.
[46] Schmitt (n 17) 59.
[47] Schmitt (n 17) 56.
[48] Schmitt (n 17) 56.

judgment, the ICJ recognized that nonintervention "forbids all States . . . to intervene directly or indirectly in internal or external affairs of other States." It also ruled, "Intervention is wrongful when it uses methods of coercion in regard to" a nation's "choice of a political, economic, social and cultural system, and the formulation of foreign policy." The relevant level of coercion "is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State."[49]

Under this standard, the ICJ found that the US's "financial support, training, supply of weapons, intelligence and logistic support" for the contras "constitute[d] a clear breach of the principle of non-intervention."[50] Such conduct clearly met the relevant standard of coercion.[51] Moreover, although simply funding the contras did not constitute a use of force, it was "undoubtedly an act of intervention in the internal affairs of Nicaragua."[52] On the other hand, humanitarian assistance would not constitute intervention,[53] nor would cessation of economic aid or the imposition of a trade quota or an embargo.[54]

The *Tallinn Manual* recognized that cyber conduct that does not rise to the level of a use of force may nonetheless constitute a violation of nonintervention.[55] At the same time, "not all cyber interference automatically violates the international law prohibition on intervention," including cyber espionage and cyber exploitation lacking a coercive element as well as mere intrusion into another state's systems even when such intrusion requires abrogating virtual

[49] ICJ *Nicaragua* judgment, para 205.
[50] ICJ *Nicaragua* judgment, para 242.
[51] ICJ *Nicaragua* judgment, para 241.
[52] ICJ *Nicaragua* judgment, para 228.
[53] ICJ *Nicaragua* judgment, para 242.
[54] ICJ *Nicaragua* judgment, para 245.
[55] Schmitt (n 17) 46.

barriers such as breaching firewalls or cracking passwords.[56] Whether other cases violate nonintervention depends on the circumstances. For example, attempts to achieve regime change by manipulating elections or public opinion in advance of elections constitute improper intervention, while lesser forms of political and economic interference do not.[57]

Measured against these standards, the surveillance practices described in the classified documents disclosed by Edward Snowden represented nothing more than the type of surveillance that the *Tallinn Manual* did not regard as constituting intervention. Lawfare similarly lacks a coercive element, and economic warfare through the erection of trade barriers or financial transactions would represent little more than the selection of trade partners that the ICJ deemed permissible. Whether a more direct assault on a nation's financial or cyber infrastructure of the type envisioned by *Unrestricted Warfare* would constitute intervention is less clear. Because nonintervention represents a lower threshold than the use of force, the fact that the *Tallinn Manual* presumes that Stuxnet constituted a use of force means that Stuxnet must necessarily constitute a violation of nonintervention as well.[58]

(c) Jus in Bello

During periods of armed conflict, state conduct is governed by jus in bello. The primary sources of law are the Geneva Conventions of 1949 and the Additional Protocols I and II of June 8, 1977, as well as customary international law. Specifically, these include the principles of distinction, which requires parties to target only those engaged in fighting, and proportionality, which requires parties to forbear from acting when the likely civilian casualties would exceed the anticipated military advantage.

---

[56] Schmitt (n 17) 47.
[57] Schmitt (n 17) 47.
[58] Schmitt (n 17) 47.

Jus in bello applies only if certain threshold considerations are met; it applies only under circumstances constituting "armed conflict;" it places restrictions on states when taking actions deemed to constitute "attacks;" and it only applies to actions by state actors and non-state actors under their control. Many common types of cyber operations that are of public concern fall outside the scope of jus in bello.

i. Armed conflict

As noted earlier, jus in bello applies only in the presence of an armed conflict. The Geneva Conventions distinguish between two types of armed conflicts: international armed conflict, defined as armed conflict among two or more states, and non-international armed conflict, defined as armed conflict within a state between the armed forces of a state and one or more armed groups or between organized armed groups.[59]

Although the treaties do not define armed conflict, Article 1(2) of Additional Protocol II to the Geneva Conventions established that "situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature" do not constitute armed conflict.[60] The International Criminal Tribunal for the Former Yugoslavia (ICTY) has also ruled that armed conflict arises "whenever there is a resort to armed force between States."[61] In making this determination, the Tribunal focused on two key criteria—the intensity of the hostilities and the organization of the parties[62]—and has developed factors by

[59] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, August 12, 1949, 75 UNTS 31, Articles 2 and 3.
[60] Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts, June 8, 1977, 1125 UNTS 609, Article 1(2).
[61] Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, October 2, 1995, para 70.
[62] ICTY *Tadić* decision, para 70. Although *Tadić* initially also included factors such as geographic scope and temporal duration as separate criteria, later decisions incorporated these concepts into intensity. *Prosecutor v Haradinaj*, Case No IT-04-84-T, Trial Chamber Judgment, April 3, 2008, para 49.

which to evaluate them.[63] The actions of a non-state organized group may be attributed to a state if that state exercises "overall control" over that group.[64] Support, such as through financing, training, equipping, and providing operational assistance, is not sufficient to establish overall control.[65] The ICJ has mentioned the overall-control test favorably without adopting it, instead applying a test that focuses on effective control.[66] Although some IGE members argued that an international armed conflict can exist between a state and a non-state armed group whose actions cannot be attributed a state, a majority of the IGE rejected that position. Instead, the *Tallinn Manual* regards such a situation as a non-international armed conflict. The IGE incorporated the intensity and organization standard established by ICTY for determining when a non-international armed conflict exists.[67] When these criteria are met, these situations are subject to many aspects of the law of armed conflict, including criminal responsibility of commanders, the principles of distinction and proportionality, the obligation and to respect medical and U.N. personnel, journalists, cultural property, and diplomatic archives, and to protect detained persons, although principles such as combatant status and belligerent immunity do not apply.[68]

The *Tallinn Manual* recognizes that jus in bello in the context of cyber operations requires the presence of an armed conflict.[69] The IGE concluded that armed conflict requires the existence of hostilities, which in turn "presuppose the collective application of means and

---

[63] On intensity, see *Prosecutor v Delalić/Mucić*, Case No IT-96-21-T, Trial Chamber Judgment, November 16, 1998, para 187; *Prosecutor v Milošević*, Case No IT-02-54-T, Decision on Motion for Judgment of Acquittal, June 16, 2004, paras 28–31 *Prosecutor v Limaj*, Case No IT-03-66-T, Trial Chamber Judgment, November 30, 2005, paras 135–67; *Prosecutor v Hadžihasanović*, Case No IT-01-47-T, Trial Chamber Judgment, March 15,2006, para 22; *Prosecutor v Mrkšić*, Case No IT-95-13/1-T, Trial Chamber Judgment, September 27, 2007, paras 39–40, 407–8, 419; ICTY *Haradinaj* judgment, para 49. On organization, see ICTY *Limaj* judgment, paras 94–129; see also *Prosecutor v Akayesu*, Case No ICTR-96-4-T, Trial Chamber Judgment, September 2, 1998, paras 619–21.
[64] ICTY *Tadić* decision, paras 131, 145, 162.
[65] ICTY *Tadić* decision, para 137.
[66] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosnia and Herzogovina v Serbia and Montenegro*), Judgment 2007 ICJ 108, para 404 (February 26).
[67] Schmitt (n 17) 72–3, 76, 77.
[68] Schmitt (n 17) 81, 84, 88, 90, 95, 97–9, 106–7, 115, 120–2, 124–5, 127, 130–2, 137, 139–44, 149, 155, 158, 168–71, 173–4, 176–7, 180, 187, 192.
[69] Schmitt (n 17) 68.

methods of warfare, consisting of kinetic and/or cyber operations."[70] IGE members disagreed as to whether a single cyber incident was sufficient to satisfy the requisite threshold of violence to constitute international armed conflict.[71] Consistent with Article 1(2) of Additional Protocol II, they did agree that "[s]poradic cyber incidents, including those that directly cause physical damage or injury," as well as that "cyber operations that incite incidents such as civil unrest or domestic terrorism" do not constitute non-international armed conflict.[72] Similarly insufficient are "network intrusions, the deletion or destruction of data (even on a large scale), computer network exploitation, and data theft" and "[t]he blocking of certain internet functions and services."[73] The IGE divided over whether such cyber operations conducted during civil disturbances or combined with other acts of violence or nondestructive but severe cyber operations might satisfy the criterion.[74]

Turning now to our motivating cases, the IGE noted that no cyber operation has been publicly characterized as an international armed conflict.[75] The *Tallinn Manual* makes clear that none of the surveillance practices described in the classified documents disclosed by Edward Snowden even arguably constituted armed conflict. The damage-free denial of service attack against Estonia and calls by the Russian minority for civil unrest in 2007 also did not rise to the level of armed conflict either in terms of harm or organization, but the similar cyber operations against Georgia in 2008, which took place in conjunction with military operations, did.[76] Neither lawfare nor the economic warfare through trade barriers or financial transactions described in *Unrestricted Warfare* would constitute armed conflict, nor would presumably more active

[70] Schmitt (n 17) 74.
[71] Schmitt (n 17) 74–5.
[72] Schmitt (n 17) 77.
[73] Schmitt (n 17) 78.
[74] Schmitt (n 17) 78.
[75] Schmitt (n 17) 75.
[76] Schmitt (n 17) 68, 74, 77.

attempts to overwhelm the financial or cyber infrastructure.[77] The IGE could not even come to agreement as to whether Stuxnet inflicted sufficient damage to constitute an armed conflict.[78]

ii Attacks

In addition, Additional Protocol I requires distinction and proportionality when states engage in certain activities. For example, Article 48 implements distinction by requiring that "the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[79] More specifically, Articles 51(2) and (4) and 52(1) prohibit signatory parties from launching an "attack" on a civilian population or on civilian objects or from indiscriminate attacks.[80] Article 51(5)(b) similarly implements proportionality by prohibiting any "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 directly military advantage anticipated."[81]

Article 49(1) defines attacks as "acts of violence against the adversary, whether in offence or defence."[82] Accompanying commentaries emphasize that attack refers to "combat action"[83] and "physical force" and does not apply to the "dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare" or to "military

[77] Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," (2012) 94 *International Review of the Red Cross* 533, 548.
[78] Schmitt (n 17) 75.
[79] Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 UNTS 3, Article 48.
[80] Additional Protocol I, Articles 51(2), (4), and 52(1).
[81] Additional Protocol I, Article 51(5)(b).
[82] Additional Protocol I, Article 49(1) and (2).
[83] Yves Sandoz, Christophe Swinarski, and Bruno Zimmerman (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: ICRC, 1977), para 1880.

movement or maneuver as such."[84] It bears mentioning that the concept of attack in jus in bello plays a role that is far different from the concept of armed attack in jus ad bellum. The former is the trigger for a range of legal protections for civilian populations, whereas the latter serves to authorize the use of force in self-defense against another state.

Rule 31 of the *Tallinn Manual* provides that "[t]he principle of distinction applies to cyber attacks," while Rule 32 incorporates the principle that civilians and civilian objects may not be attacked.[85] Rule 30 defines a cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[86]

The *Tallinn Manual* commentary on attacks emphasizes the concept of violence used in Article 49(1) of Additional Protocol I as the key concept that distinguishes attacks from other military operations and lists psychological cyber operations and cyber espionage as nonviolent operations that do not qualify as attacks.[87] As the precedents on chemical, biological, and radiological weapons indicate, attacks do not have to have a kinetic effect in order to be violent so long as they foreseeably have the consequences set for in the rule.[88] For example, a cyber operation targeted at an electrical grid that starts a fire would qualify; *de minimis* damage or destruction would not.[89]

The IGE agreed that cyber operations targeted at data could constitute an attack. The IGE divided over whether cyber interference with the functionality of an object could constitute a

[84] Michael Bothe, Karl Josef Partsch, and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts* (Boston: Martinus Nijhoff Publishers 1982), 289.
[85] Schmitt (n 17) 95, 97.
[86] Schmitt (n 17) 92.
[87] Schmitt (n 17) 92.
[88] Schmitt (n 17) 92–3.
[89] Schmitt (n 17) 92.

cyber attack, with a majority opining in the affirmative and a minority in the negative.[90] While an attack on a computer-based control system for an electrical grid that requires the replacement of components would constitute an attack, IGE members disagreed over whether an attack that required reinstallation of the operating system or the restoration of data might qualify as an attack.[91] The IGE agreed that cyber operations that do not cause damage, but result in nationwide blocking of email or other similar large-scale adverse consequences would not constitute an attack.[92] Introduction of malware or latent defects that are capable of launching an attack would, however, as would attacks that are successfully intercepted by firewalls, antivirus software, or other protective systems.[93]

The surveillance programs described in the classified documents disclosed by Edward Snowden would not rise to the level of injury to persons, damage to objects, or violence to constitute an attack under the criteria laid out in the *Tallinn Manual*, nor would apparently the type of denial of service attack directed against Estonia in 2007, although a similar attack that is part of a wider operation, as was the case in Georgia in 2008, would.[94] The same would apply to the lawfare and economic warfare through trade barriers and financial transactions described in *Unrestricted Warfare*, nor would presumably more active attempts to disrupt the financial or cyber infrastructure so long as they did not cause physical damage. The IGE did not offer an assessment as to the application of these principles to Stuxnet, although one could surmise that if introducing a bug into the control system for an electric grid that caused a fire would constitute an attack, so would introducing a bug into a control system that led to the destruction of centrifuges.

---

[90] Schmitt (n 17) 93.
[91] Schmitt (n 17) 93–4.
[92] Schmitt (n 17) 94.
[93] Schmitt (n 17) 94.
[94] Schmitt (n 17) 94.

iii. Attribution to the state

In addition to constituting an armed conflict, the acts must be attributable to a state for jus in bello to apply. According to the International Law Commission's Articles on Responsibility of States for Intentionally Wrongful Acts, states are responsible for private actors who are operating under their direction and control.[95] The ICJ and ICTY have ruled that the conduct of non-state actors may be attributed to the state if the state exercises "effective control" or "overall control."[96]

As an initial matter, the inherent anonymity of internet-based communications makes the true source of a packet hard, if not impossible, to verify. Furthermore, many attacks rely on botnets where a bot controller can use thousands or millions of infected computers to launch an attack without their owners' permission or awareness. The fact that many cyberwar capabilities are developed and executed by private companies raises questions when this conduct may be fairly attributed to the state. Such groups must be organized; collective activity of "hacktivists" acting independently is not sufficient.[97]

Perhaps the most corrosive aspect of cyberwarfare is its tendency to break down the preconditions needed to support cooperation. International law scholarship typically falls into two traditions. The first views states as rational actors that cooperate only when it is in their self-

[95] Int'l L Comm'n, Responsibility of States for Internationally Wrongful Acts, GA Res 56/83 annex, UN Doc. A/RES/56/83, December 12, 2001.
[96] ICJ *Nicaragua* judgment, para 115; ICJ *Genocide* judgment paras 399–401; ICTY *Tadić* decision, paras 131, 145.
[97] Schmitt (n 17) 38, 73–4.

interest to do so.[98] The second believes that international law embodies a set of norms that states feel some obligation to follow.[99]

Both approaches find aspects of cyber war that destabilize cooperation. Both function best when the number of relevant actors is relatively small and when information about compliance and noncompliance is highly visible and attributable.[100] Unfortunately, cyber operations weaken both considerations. The fact that cyber conflicts can be waged relatively cheaply when compared with kinetic war radically increases the number of relevant players. Moreover, the fact that participants need not be geographically proximate to any location and can anonymize their identities makes information about their conduct much harder to perceive and to verify. One would expect the emergence of cyber operations to cause the informal governance structures on which international law relies to weaken.

III. THE APPLICABILITY OF THE LAW OF ESPIONAGE

With a few narrow exceptions, jus ad bellum and jus in bello does not govern the type of information gathering or interference that characterize cyber operations such as the type of surveillance described in the confidential documents disclosed by Edward Snowden, the denial of service attacks directed at Estonia, or the type of measures described in *Unrestricted Warfare*. Indeed, the initial section regarding the scope of the *Tallinn Manual* explicitly notes that it does not address such matters as "[c]yber espionage, theft of intellectual property, and a wide variety of criminal activities in cyberspace" because "the international law on uses of force and armed

[98] For example, Hans Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, (New York: McGraw-Hill, 5th edn, 1973); Jack L Goldsmith and Eric A Posner, *The Limits of International Law* (New York: Oxford University Press, 2006).
[99] For example, Louis Henkin, *How Nations Behave*, (New York: Columbia University Press, 2nd edn, 1979); Harold Hongju Koh, "Why Do Nations Obey International Law?" (1997) 106 *Yale Law Journal* 2599.
[100] Robert C Ellickson, *Order Without Law: How Neighbors Settle Disputes* (Cambridge, MA: Harvard University Press, 1991).

conflict plays little or no role" with respect to those subjects.[101] It explains why the IGE members did not regard practices such as monitoring keystrokes, breaching firewalls, cracking passwords, or intruding into another state's systems as a use of force for purposes of jus ad bellum.[102] It also explains why they did not "network intrusions, the deletion or destruction of data (even on a large scale), computer network exploitation, . . . data theft," "[t]he blocking of certain internet functions and services, and the nationwide disruption of email as constituting an armed conflict for purposes of *jus in bello*."[103]

Instead, this type of conduct falls within the province of the law of espionage. Sometimes called the second oldest profession,[104] espionage traces its roots back to ancient Egypt, Greece, Rome, and China.[105] Indeed, the great seventeenth-century legal scholar Hugo Grotius noted that "there is no doubt, but the law of nations allows anyone to send spies, as Moses did to the land of promise, of whom Joshua was one."[106] The law of espionage has remained relatively undeveloped, with what little work that exists focusing on espionage during times of war, with the most salient example being the Hague Regulations provision providing that "a spy who, after re-joining the army to which he belongs, is subsequently captured by the enemy, is treated as a prisoner of war, and incurs no responsibility for his previous acts of spying."[107] Thus, Falk's admonition that "[t]raditional international law is remarkably oblivious to the peacetime practice

---

[101] Schmitt (n 17) 18.
[102] Schmitt (n 17) 47, 50.
[103] Schmitt (n 17) 78, 94.
[104] Allison Ind, *A Short History of Espionage* (New York: David West Co., 1963); Phillip Knightley, *The Second Oldest Profession: Spies and Spying in the Twentieth Century* (New York: W.W. Norton & Co., 1986).
[105] Allen Dulles, *The Craft of Intelligence* (Guilford, CT: Globe Pequot, 1961); Richard A Falk, "Forward," in Roland J. Stranger (ed), *Essays on Espionage and International Law* (Columbus, OH: Ohio State University Press, 1962); Adrienne Wilmoth Lerner, "Espionage and Intelligence, Early Historical Foundations," in Lee Lerner and Brenda Wilmoth Lerner (eds), *Encyclopedia of Espionage, Intelligence, and Security*, (New York: Thomson Gale, 2004) at <http://www.encyclopedia.com/doc/fullarticle/1G2-3403300282.html>.
[106] Hugo Grotius, *The Rights of War and Peace, Including the Law of Nature and of Nations* (New York: Cosimo, Inc., 2007) 331.
[107] Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, October 18, 1907, Article 31, 36 Statute 2277, 2304.

of espionage" continues to hold true today.[108] Indeed, the ICJ appears to be going out of its way to avoid creating opinio juris with respect to peacetime espionage.[109]

Scholars have divided sharply on the legality of peacetime espionage. The majority of scholars assert that it *is* legal, pointing to the predominance of the practice and asserting that better information about what other countries are doing promotes stability and is implicit in the right of preemptive self-defense.[110] Others disagree, condemning it as an impressible violation of the spied-upon country's territorial integrity.[111] Still others assert that the legal status of espionage remains ambiguous, with international law neither condemning nor condoning it.[112] In the absence of any clear principles, with the exception of a handful of exceptions such as interference with diplomatic communiques, espionage remains the province of domestic law and falls outside the province of jus ad bellum and jus in bello.

---

[108] Falk (n 107) v.

[109] Dieter Fleck, "Individual and State Responsibility for Intelligence Gathering," (2007) 28 *Michigan Journal of International Law* 687.

[110] Lassa Oppenheim, *International Law* (New York: Longmans, Green, and Co., 2nd edn, 1912); Julius Stone, "Legal Problems of Espionage in Conditions of Modern Conflict," in Stranger (n 107); Beth M Polebaum, "National Self-defense in International Law: An Emerging Standard For a Nuclear Age," (1984) 59 *New York University Law Review* 187; John Kish and David Turns, *International Law and Espionage* (Boston: Martinus Nijhoff, 1995); Geoffrey Demarest, "Espionage in International Law," (1996) 24 *Denver Journal of International Law & Policy* 321; Roger D. Scott, "Territorial Intrusive Intelligence Collection and International Law," (1999) 46 *Air Force Law Review* 217; Simon Chesterman, "The Spy Who Came in From the Cold War: Intelligence and International Law," (2006) 27 *Michigan Journal of International Law* 1071; Fleck (n 111); Luke Pelican, "Peacetime Cyberespionage: A Dangerous, but Necessary Game," (2012) 20 *CommLaw Conspectus* 363.

[111] Falk (n 107); Quincy Wright, "Espionage and the Doctrine of Noninterference in Internal Affairs," in Stranger (n 107); Manuel R Garcia-Mora, "Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition," (1964) 26 *University of Pittsburgh Law Review* 65; Ingrid Delupis, "Foreign Ships and Immunity for Espionage," (1984) 78 *American Journal of International Law* 53; A John Radsan, "The Unresolved Equation of Espionage and International Law," (2007) 28 *Michigan Journal of International Law* 595; John F. Murphy, "Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?," (2013) 89 *International Law Studies*309.

[112] Christopher D Baker, "Tolerance of International Espionage: A Functional Approach," (2004) 19 *American University International Law Review*1091; Daniel B Silver, "Intelligence and Counterintelligence," in John Norton Moore and Robert F Turner (eds), *National Security Law* (Durham, NC: Carolina Academic Press, 2nd edn, 2005) (updated and revised by Frederick P Hitz and J E Shreve Ariail), 965.

A literature has only begun to emerge regarding cyber espionage.[113] There are aspects of cyber espionage that may change the optimal outcome. On the one hand, as was the case with satellite surveillance,[114] the lack of territorial invasion makes cyber surveillance less problematic.[115] On the other hand, the dramatic drop in the cost of surveillance and the lower likelihood of apprehension may lead firms to engage in it when before the benefits did not justify the costs. Some regard this as a benefit, as the nonlethal aspects of cyber capabilities make them preferable to other means.[116] Others take the contrary view, arguing that because cyber espionage increases the scale of intelligence-gathering capability, it should be curbed by treating it more severely than traditional espionage.[117] Still others support doing nothing and allowing state practices to evolve.[118] In any event, general agreement never emerged with respect to traditional espionage, and there seems little reason to expect that consensus is more likely to appear in the cyber context.

The law of war, thus, has little to say about the types of surveillance that are generating the most concern. That is why Rule 66(a) of the *Tallinn Manual* explicitly states, "Cyber espionage and other forms of information gathering directed at an adversary during an armed conflict do not violate the law of armed conflict."[119] The commentary similarly notes that cyber espionage does not constitute the use of force or armed attack for purposes of jus ad bellum, armed conflict or attack for purposes *of jus in bello*, or a violation of the principle of

[113] Sean P Kanuck, "Information Warfare: New Challenges for Public International Law," (1996) 37 *Harvard International Law Journal* 272; Pelican (n 112); Murphy (n 113); David Weissbrodt, "Cyber-conflict, Cyber-crime, and Cyber-espionage," (2013) 22 *Minnesota Journal of International Law* 347.
[114] Stone (n 112).
[115] Pelican (n 112).
[116] Jeffrey TG Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare," (2008) 106 *Michigan Law Review* 1427.
[117] Anna Wartham, "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?" (2012) 64 *Federal Communications Law Journal* 643; Alexander Melnitzky, "Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses," (2012) 20 *Cardozo Journal of International and Comparative Law* 537.
[118] Pelican (n 112).
[119] Schmitt (n 17) 158.

nonintervention.[120] It also explains why the commentary notes at several points that international law does not address espionage per se and that, as such, conduct related to espionage is presumptively legal as a matter of international law.[121]

Even more tellingly, the *Tallinn Manual* commentary distinguishes between cyber espionage, which necessarily takes place in territory controlled by one of the parties to the armed conflict, from computer network exploitation and cyber reconnaissance, which are conducted from outside enemy controlled territory. Such conduct is not cyber espionage at all.[122]

The type of activities described in the classified documents disclosed by Edward Snowden, the denial of service attack on Estonia, and the tactics described in *Unrestricted Warfare* are, thus, not governed by international law at all. The legality of such conduct is consigned instead to domestic law.

IV. POTENTIAL CYBER WARFARE DEFENSE STRATEGIES

Given the unlikely prospect of legal solutions to the problems posed by cyber war, those confronting the risk of cyber attacks must necessarily undertake self-protective measures to protect themselves. In this section of the article we examine defenses and defensive strategies intended to preserve the functioning of a society's information infrastructures and the systems controlled by them.

(a) "Air gaps"

As many of the problems of information infrastructures exploitable by adversaries are enabled by internet connectivity, one defensive strategy that suggests itself is to keep machines

[120] Schmitt (n 17) 47, 50–1, 52, 56, 75, 92.
[121] Schmitt (n 17) 36, 50, 52, 159.
[122] Schmitt (n 17) 159.

off the global internet. For example, a network intended to carry sensitive military traffic might be created, with its own internet protocol (IP) address and domain name system (DNS) infrastructures and web servers; as long as there is no interchange with the conventional global internet, this can be very effective.[123] There are at least two difficulties, however. First, replicating an internet is logistically challenging and, therefore, expensive, and to truly "air gap" one must prevent all accidental interconnections (e.g., with a laptop connected to the military network with a cable and connected to the global internet with WiFi).

A second issue, also logistical in essence, is that data transfers and updates of software must be done in a way that preserves the "air gap," for example, via storage media such as USB memory sticks and CDs or DVDs. As Stuxnet demonstrates, the data transfers must be carried out carefully to ensure that there is no hidden malware on the medium, and the individuals involved must be trusted to ensure such checking is performed 100% of the time.[124]

(b) "Kill switches"

The "kill switch" idea is that a national authority would have the capability to disconnect their nation from the global internet, to disable network-based attacks of various types. As an example, consider the directed denial of service (DDoS) attacks against Estonia. If Estonia had a kill switch capability, then the floods of external traffic would be cut off. Some engineering would be required to accomplish this, notably ensuring that the DNS would continue to work via caches and redirections.

---

[123] Defense Advanced Research Projects Agency, "Military Networking Protocol (MNP)," FedBizzOps.gov, October 28, 2008, at <http://www.fbo.gov/index?s=opportunity&mode=form&id=01886bf13926063b1cc0e996b223440f&tab=core&_cview=1>.

[124] Nicholas Falliere, Liam O Murchu, and Eric Chien, "Symantec W32.Stuxnet Dossier, Version 1.4," Symantec, February 2011, at <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

To engineer such a defensive solution requires that all, or a vast majority, of the network resources incorporate a control mechanism by which the national authority can exercise the cut-off decision. Economics and reliability suggest that minimizing the number of such control points makes sense, but this has the unfortunate consequence of creating fewer points that can fail before a catastrophe. These control points also create an attractive target for an adversary, and by the nature of their role are difficult to test previous to their engagement.

(c) Special treatment of information systems for critical infrastructure

Consistent with the observations in subsections (a) and (b), connectivity to the global internet enables attacks on critical infrastructures. Imagine, for example, that a bored employee at a control point in the electrical power grid connects a personal laptop, tablet, or WiFi-enabled smartphone into the building network to access entertainment such as online gaming. There are various scenarios, for example, a cellular network/building network bridge, that conceivably could provide malware or malicious actors with access to the power grid.

Here, the right strategy is isolation of the grid control interfaces from the internet and machines connected to it. While it is conceptually possible (see subsection (d), below) to have application-specific gateways, complexity seems to inevitably creep in and create opportunities for malware to overcome the gateway's role (isolation) in the system design.

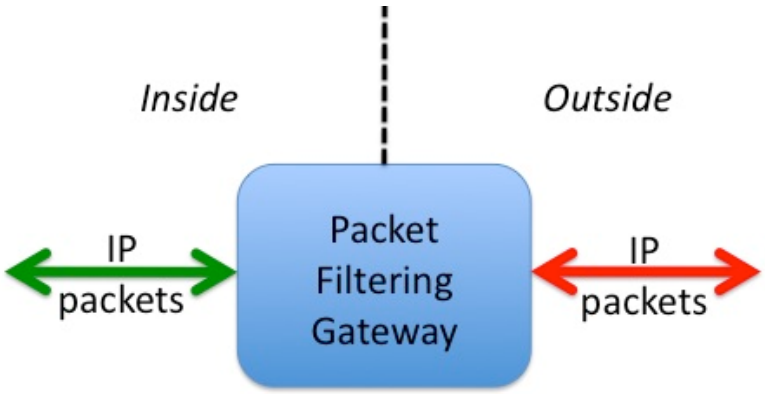
(d) Network-embedded perimeter defenses

An alternative to physical air gaps is the idea of a packet-filtering gateway or firewall, as illustrated in Figure 12.1. A "firewall" is a packet-filtering gateway.[125] The typical role of such a

[125] WR Cheswick and SM Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker* (Boston: Addison-Wesley, 1994).

device is to segregate packet traffic into an “inside” and “outside,” where certain activities are allowable if originating from the inside but not if originating from the outside.

Figure 12.1: Packet-filtering gateways used for network defense



The decisions about what activities are allowable and not allowable is encoded in a packet-filtering policy implemented by the firewall. The problem with firewalling as a strategy is that many security threats have moved into applications, for example, into interpreters embedded into applications such as document formatters and renderers, as well as browsers. “Port 80” (used by the Web’s HTTP) cannot be closed, yet much of today’s dangerous material flows in from the web. This suggests application gateways that provide extremely constrained interfaces to applications, perhaps complemented by one or more packet-filtering gateways.

(e) Improved software engineering

A major issue in cyberwarfare is software that can be exploited to perform unwanted actions. The very fact that such unwanted actions are feasible is a sign that there are mistakes in the software’s design. The discipline of software engineering is intended to produce correct

software.[126] Software correctness in the context of security means that the right action is performed for the right person in the right place at the right time, with no missing functions, errors or "extras." Modern design techniques, such as software development with the aid of theorem provers,[127] and use of modern programming languages, such as Haskell and OCaml, preclude many of the most common errors (e.g., buffer overflows) that pervade software implementations.[128] While such tools do not guarantee a correct or appropriate design, they remove a great deal of low-hanging fruit exploitable by the attacker and allow the defending programmer to focus more attention on the software logic, interfaces, and overall design.

Software engineering has a great deal to offer as a discipline,[129] yet it is underutilized as a defensive mechanism, not least because market forces pressure developers towards a strategy of release early and often that may or may not be wise. Cyber security considerations have very limited traction in the marketplace, as there seems to be little in the way of financial gain or penalty for writing software that is more secure or less secure. One policy, for better or worse, that would create financial incentives for correct functioning would be to create a legal doctrine of software liability, involving torts for failures of the software, as well as the inevitable documentation of "best-practices" defenses against such torts.[130]

---

[126] Daniel M Hoffman and David M Weiss (eds) *Software Fundamentals: Collected Papers by David L. Parnas* (Boston: Addison-Wesley, 2001).
[127] Benjamin C Pierce, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, and Brent Yorgey, "Software Foundations," Penn Engineering: Computer and Information Science, July 2014, at <http://www.cis.upenn.edu/~bcpierce/sf/>.
[128] Graham Hutton, *Programming in Haskell* (Cambridge: Cambridge University Press, 2007); Xavier Leroy, Damien Doligez, Alain Frisch, Jacques Garrigue, Didier Rémy, and Jérôme Vouillon, "The OCaml System (Release 4.01): Documentation and User's Manual," The Caml Language, September 12, 2013, at <http://caml.inria.fr/pub/docs/manual-ocaml/>.
[129] Hoffman and Weiss (n 128); John Viega and Gary McGraw, *Building Secure Software: How to Avoid Security Problems the Right Way* (Boston: Addison-Wesley, 2002).
[130] Jonathan M Smith, "At Issue: Should Software Manufacturers be Liable for Vulnerabilities in Their Software?" (2003) 13 *CQ Researcher* 811.

V. CONCLUSION

At several points in the discussion, the disturbing impression arises that the technology has run ahead of the policy thinking in the domain of cyberwar. We make here a few suggestions on questions and directions that might lead to informed policy-making in this area.

International policies and agreements should clarify how cyber actions fit into existing international law. Although the *Tallinn Manual* is a step in the right direction within its scope, the more problematic area of espionage remains largely unaddressed. Cyber war's greater ability to deploy latent disruptive capabilities and a greater ability to conduct surveillance will make guidelines to determine the propriety of this type of conduct increasingly important in years to come.[131]

On the technological side, engineers should developed means to ensure reliable attribution of actions in cyberspace. In addition, they should develop the technical means to distinguish combatants from non-combatants in order to honor distinction and neutrality. If developed, these capabilities would make it easier to reconcile cyber war with existing principles of international law.

On a broader level, any proposals should account for the huge social and economic value inherent in cooperation, as exemplified by the success of the internet's federated but cooperative architecture. At the same time, they should recognize how a lack of alignment in underlying interests, the increase in the number of participants, and the reduced ability to verify others' compliance have the tendency to cause cooperation to break down. In the absence of such

[131] Baker (n 114); Demarest (n 112).

cooperation, nation-states may use lawfare as a tool of obstruction in the course of waging total war.[132]

These are not concrete proposals as such, but rather directions that might result in productive discussions by technologists interested in policy issues and policy-makers interested in the risks and management challenges associated with a defensive posture in cyber space.

[132] Qiao and Wang (n 9).