2013

Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions

Matthew C. Waxman
Columbia Law School, mwaxma@law.columbia.edu

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1901
U.S. NAVAL WAR COLLEGE

Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions

Matthew C. Waxman

89 INT'L L. STUD. 109 (2013)

Volume 89 2013

Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions

Matthew C. Waxman[*]

I. INTRODUCTION

When does a cyber attack (or threat of cyber attack) give rise to a right of self-defense—including armed self-defense—and when should it? By "cyber attack" I mean the use of malicious computer code or electronic signals to alter, disrupt, degrade or destroy computer systems or networks or the information or programs on them. It is widely believed that sophisticated cyber attacks could cause massive harm—whether to military capabilities, economic and financial systems, or social functioning—because of modern reliance on system interconnectivity, though it is highly contested how vulnerable the United States and its allies are to such attacks.[1]

* Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Relations; Member of the Hoover Institution Task Force on National Security and Law.

1. *See* Mark Clayton, *The New Cyber Arms Race*, CHRISTIAN SCIENCE MONITOR (Mar. 7, 2011), http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race. Some experts warn of a "digital Pearl Harbor" or other likely devastating attacks on the United States. *See*, *e.g.*, Mike McConnell, *To Win the Cyber-War, Look to the Cold War*, WASHINGTON POST, Feb. 28, 2010, at B1. Other experts, however, argue that these risks are greatly exaggerated. *See*, *e.g.*, Thomas Rid, *Cyber War Will Not Take Place*, 35 JOURNAL OF STRATEGIC STUDIES 5 (2012).

This article examines these questions through three lenses: (1) a legal perspective, to examine the range of reasonable interpretations of self-defense rights as applied to cyber attacks, and the relative merits of interpretations within that range; (2) a strategic perspective, to link a purported right of armed self-defense to long-term policy interests including security and stability; and (3) a political perspective, to consider the situational context in which government decisionmakers will face these issues and predictive judgments about the reactions to cyber crises of influential actors in the international system.

My main point is that these three perspectives are interrelated, so lawyers interested in answering these questions should incorporate the strategic and political dimensions in their analysis.[2] This is not just to make the banal, generic point that politics, strategy and law are interrelated. Of course they are. Rather, this article aims to show specifically how development of politics, strategy and law will likely play out interdependently with respect to this particular threat—cyber attacks—and to draw some conclusions about legal development in this area from that analysis.

The focus of this essay on military self-defense to cyber attacks (that is, self-defense in a legal sense of resort to force) is not meant to suggest that this is the most important element of a comprehensive cybersecurity strategy—far from it. Most attention these days is properly on other components of that strategy, including better network security and "offensive" cyber measures, though military force is part of the strategic tool set. Also, an important caveat is that this analysis is self-consciously colored with an American perspective. If one assumes, as I do, though, that legal analysis and development cannot be divorced from strategy and politics, then America's power—in its various forms—and vulnerabilities to power will greatly influence its own interpretive approach to these issues, and because of its relative power globally it will greatly influence international legal movement in this area.

II. LEGAL PERSPECTIVE

A legal perspective on the question of cyber attacks as armed attacks sees the issue as one of self-defense rights under the *jus ad bellum* framework. Article 2(4) of the UN Charter mandates that "[a]ll Members shall refrain

2. This essay draws heavily on a previous article: Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011).

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."[3] Article 51 then provides, however, that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[4] A legal question then arises: when, if ever, is a cyber attack an "armed attack" such that it triggers self-defense rights?

No consensus answer yet exists to this question, and several analytic approaches are competing for adherents.[5] A strict reading of "armed attack" would confine its meaning to kinetic violence, as opposed to non-physical violence or harm with no physical damage (take, for example, economic or diplomatic sanctions), and cyber attacks might therefore be considered as unable ever—on their own—to trigger armed self-defense rights. This position offers a bright-line rule that is relatively easily applied, but it is difficult to square with the treatment of chemical or biological weapons attacks (which everyone would acknowledge as an armed attack) and fails to account for new cyber vulnerabilities. The position is therefore rarely advanced that a cyber attack could *never* constitute an armed attack.

A more common starting point for analysis is to consider the effects or consequences of a cyber attack in determining whether it crosses the threshold of "armed attack." That is, the essence of an "armed attack" and the resulting self-defense right is the direct or perhaps indirect result of a hostile action—typically, but not necessarily, in the form of kinetic violence—and legal interpretation should proceed by examining whether the results of a specific cyber attack are sufficiently like kinetic violence.[6]

Among those taking an effects-based approach to Article 51 is a further

---

3. U.N. Charter art. 2, para. 4.

4. *Id.*, art. 51.

5. For a discussion of these positions, see Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIFORNIA LAW REVIEW 817, 841–49 (2012).

6. *See* NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 33–34 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT]; Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 914–15 (1999); Katharina Ziolkowksi, *Computer Network Operations and the Law of Armed Conflict*, 49 MILITARY LAW & THE LAW OF WAR REVIEW 47, 69–75 (2010); TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 92–95 (Michael N. Schmitt ed., 2013), draft *available at* http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft /1#share.

split in method. Some legal experts have suggested that to qualify as an armed attack a cyber attack must produce *violent* consequences of the sort usually produced by bombs or bullets.[7] So, for example, a cyber attack that caused a power station to explode or one that caused airplanes to crash could legally constitute an armed attack, but cyber attacks that cause economic or social damage—like taking down the stock market or bringing transportation systems to a halt—could not. Many other legal experts take a broader view of what sort of effects could constitute an armed attack, arguing that to focus on death or physical damage fails to account for modern society's critical reliance on information infrastructure and connectivity.[8] They would, therefore, look beyond just the type of effect to its magnitude, immediacy and other factors in assessing whether a cyber attack crosses the self-defense threshold.

Any effects-based interpretive approach leads to difficult secondary questions. These include how to calculate proportionality of an armed response (especially given that the effects of cyber attacks may be difficult to measure and direct causality may be difficult to assess); how to judge imminence for the purposes of anticipatory self-defense (given that discerning cyber attacks from other cyber activities, like espionage, is so difficult and that once launched some attack sequences take place in split seconds); and how to consider State responsibility (given that attacks may be launched by individuals or groups with loose relationships to States).

The United States government has generally followed an effects-based approach, though only gradually providing information publicly about the way in which it does or would legally assess cyber attacks' effects. In testifying before the Senate committee considering his nomination to head the new U.S. Cyber Command, Lieutenant General Keith Alexander explained that "[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what con-

---

7. *See*, *e.g.*, 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) (Vol. 76, U.S. Naval War College International Law Studies).

8. *See* NRC REPORT, *supra* note 6, at 253–54 (arguing that the traditional legal emphasis on death or physical damage is problematic because "modern society depends on the existence and proper functioning of an extensive infrastructure that itself is increasingly controlled by information technology," and that therefore "[a]ctions that significantly interfere with the functionality of that infrastructure can reasonably be regarded as uses of force, whether or not they cause immediate physical damage").

stitutes a use of force."[9] He went on, however, to suggest that "[i]f the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response."[10]

More recently, the White House stated in its official cybersecurity strategy that "[c]onsistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."[11] It went on to declare:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[12]

Without expressly endorsing an effects-based legal analysis or explaining the details of that analysis, the United States hereby appears to be relying on it in asserting the same self-defense authority universally recognized as applying to conventional armed attacks. As with any armed attack, the United States is declaring its view that some cyber attacks open the full range of self-defensive instruments; a cyber attack will not necessarily be met with responses confined to the cyber realm or other measures short of armed force.

Offering a bit more detail as to its legal position on this, in 2011 the United States explained its interpretation of Article 51 to the UN Group of Global Experts in the following terms:

---

9. Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm., 111th Cong. 11 (Apr. 15, 2010), http://www.armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

10. *Id.* at 12.

11. THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 10 (2011).

12. *Id.* at 14.

> It may be difficult to reach a definitive legal conclusion as to whether a disruptive activity in cyberspace constitutes an armed attack triggering the right to self-defence. For example, where the threat actor and the motive are unknown, and effects result that do not directly cause substantial death or physical destruction, it may be possible to reach differing conclusions about whether an armed attack has occurred. However, such ambiguities and room for disagreement do not suggest the need for a new legal framework specific to cyberspace. Instead, they simply reflect the challenges in applying the Charter framework that already exists in many contexts.[13]

Nevertheless, the U.S. statement concludes that "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack."[14]

In September 2012, State Department Legal Advisor Harold Koh elaborated a little further the U.S. position in a public address, explaining that some cyber attacks could constitute a prohibited use of force:

> *Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.* In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including: the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes.[15]

He went on to explain the long-standing U.S. position that any such use of force could potentially trigger self-defense rights as an armed attack.[16]

At the time of this writing, some U.S. allies have moved cautiously in this general direction through public statements, while some other power-

---

13. *See* U.N. Secretary-General, Replies to the Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the U.N. Secretary-General 18, U.N. Doc. A/66/152 (July 15, 2011).

14. *Id.*

15. Harold Hongju Koh, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm (emphasis in original).

16. *Id.*

ful States have expressed concern about it. In 2012, for instance, the British Armed Forces Minister stated in response to parliamentary questioning that a cyber attack like that suffered by Estonia in 2007—which was widely blamed on Russia and which caused massive economic and social disruption—might trigger NATO's collective self-defense provisions.[17] NATO as a collective body has been working on a joint approach to cybersecurity, though NATO's official rhetoric in the field of self-defense has been quite cautious.[18] In 2011, the United States and Australia announced that their mutual defense treaty extends to cyberspace, signaling a joint intention to treat cyber attacks within the same cooperative framework as armed threats though without explicitly referencing an armed response.[19] Meanwhile, however, in diplomatic groupings China has resisted the idea that cyber attacks could trigger a traditional right of self-defense, urging instead new forms of international legal regulation and a broader understanding of cyber threats, to include Internet content threatening to regime stability, while Russia has advocated an international agreement to fill what it sees as gaps in international law with respect to cyber weapons.[20]

Despite calls from some circles that they urgently demand clear resolution, it is likely that legal questions about cyber attacks as armed attacks will be answered not through formal, multilateral instruments[21]—like a new treaty convention—but incrementally through State practice. That is, the law will evolve and adapt over time through the prevailing conduct and legal views expressed by States in planning for and responding to cyber-attack incidents.

---

17. *See UK Minister: Cyberattack Could Prompt NATO Action*, GUARDIAN (May 16, 2012), http://www.guardian.co.uk/world/feedarticle/10245167.

18. *See* NORTH ATLANTIC TREATY ORGANIZATION, STRATEGIC CONCEPT FOR THE DEFENCE AND SECURITY OF THE MEMBERS OF THE NORTH ATLANTIC TREATY ORGANIZATION ¶ 19 (2010), *available at* http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (discussing the need to develop joint policies on cyber defense).

19. *See* Media Note, Office of the Spokesperson, U.S. Department of State, U.S.-Australia Ministerial Consultations 2011 Joint Statement on Cyberspace (Sept. 15, 2011), http://www.state.gov/r/pa/prs/ps/2011/09/172490.htm.

20. *See* Adam Segal & Matthew Waxman, *Why a Cybersecurity Treaty Is a Pipe Dream*, CNN (Oct. 26, 2011, 2:01 PM), http://globalpublicsquare.blogs.cnn.com/2011/10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/.

21. *See* Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW 5 (Peter Berkowitz ed., 2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf; Segal & Waxman, *supra* note 20.

This means that legal evolution is likely to occur in significant part through defensive planning doctrine and declaratory policies issued in advance of actual cyber-attack crises, so to understand that development we need to rotate our analytic lens toward a strategic angle. In addition to the unilateral and joint self-defense policy statements cited earlier, for instance, Japan's national security agencies have reportedly been following the U.S. lead, generally accepting the U.S. legal interpretation of Article 51 with respect to cyber attacks in planning their defense.[22] Given Japan's reliance on U.S. security guarantees, this is not so surprising and illustrates the tight linkage between legal development and strategic relations.

Legal development is also likely to occur incrementally through actions and reactions of States and other major international actors during and following actual cyber-attack crises. This means we will need to rotate our analytic lens toward a political angle, too.

III. A STRATEGIC PERSPECTIVE

A strategic perspective on the question of cyber attacks as armed attacks sees the issue as one linking a purported right of armed self-defense to long-term policy interests—both national interests and global ones in the case of the United States—including security and stability. The substance and clarity of any such legal right has the potential to significantly enhance or detract from those strategic ends.

Armed self-defense to cyber attacks may be strategically valuable in several respects. First, anticipatory or responsive military actions might be important in some cases to protecting military and critical infrastructure vulnerable to cyber attacks—for example, by striking at facilities or individuals responsible for launching or directing them—though, because the physical infrastructure associated with cyber attacks may be quite small and widely dispersed, this sort of preventive use of force specifically to neutralize the possibility of initial or follow-on cyber attacks has not been the subject of much discussion. Second, the credible threat of self-defensive military actions might help deter cyber attacks by raising the prospective costs of hostile cyber activities in the minds of adversaries (though probably not much so of non-State adversaries, against whom deterrent threats of military action will not be very potent). Such strategic logic likely underlies the

22. *See Govt Claims Cyberdefense Right: Says International Laws Should Be Applied to Computer Infiltration*, DAILY YOMIURI ONLINE (May 17, 2012), http://www.yomiuri.co.jp/dy/national/T120516005387.htm.

U.S. declaratory postures described in the previous section, putting adversaries on notice that they should expect a possible military response to some cyber threats.

This is not the place to discuss in any detail the specific challenges and nuances of relying in part on military defense or deterrence against cyber attacks, a topic that many others have written about in detail.[23] The salient concern here is the way in which—to turn our lens back a bit and open the aperture to capture the legal and strategic perspectives together—legally regarding some cyber attacks to constitute armed attack might contribute strategically. It could do so in a number of ways.

For example, if one believes that armed self-defense is important to protecting against cyber attacks through anticipatory or responsive military actions, internally a well-established legal right helps strengthen the hand of political leaders weighing such options (an issue taken up further in the next session, which turns our lens toward a political perspective). An established or articulated right adds legitimacy to forceful options and may be taken as a guide of likely global reactions. A well-established right also facilitates military planning for such contingencies by clearing internal obstacles and bolstering the legitimacy and bureaucratic expectation of doing so. Within agencies charged with operationalizing them, it is much easier to plan and develop options for policy routes that are declared legal.

By thinking externally about the expectations of others, a legal right of armed self-defense might contribute to deterrence by establishing and communicating more emphatically and clearly red lines associated with self-defensive threats.[24] It helps to signal to others thresholds beyond which they should expect significant escalation, to include military means. When combined with rules of State responsibility, a right of armed self-defense might also induce States to crack down more strongly on cyber attacks launched from their territory, or perhaps to share more intelligence about cyber threats within their jurisdiction, whether out of a sense of legal obligation or for fear of being targeted with armed self-defense.

---

23. On the special difficulties of deterring cyber attacks, see MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 41–52 (2009); NRC REPORT, *supra* note 6, at 303; John Markoff, David E. Sanger & Thom Shanker, *In Digital Combat, U.S. Finds No Easy Deterrent*, NEW YORK TIMES, Jan. 26, 2010, at A1.

24. *See* James A. Lewis, *Multilateral Agreements to Constrain Cyberconflict*, ARMS CONTROL TODAY, June 2010, at 16; Adam Segal, *Cyberspace Governance: The Next Step*, Council on Foreign Relations Policy Innovation Memorandum No. 2 (Mar. 14, 2011), http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

These strategic benefits, however, must be balanced with strategic risks associated with legal treatment of some cyber attacks as armed attacks. Calibrating among such benefits and risks has always been a purpose and sustaining foundation of the *jus ad bellum* regime, and adapting it to this domain will be especially tricky.[25]

One strategic risk is the possibility of eroding normative constraints on war, shifting our focus back toward the legal perspective. As capabilities proliferate among State and non-State actors to conduct various sorts of malicious, hostile or intelligence-gathering activities in cyberspace, any deterrence value of treating them as armed attacks triggering self-defense rights under Article 51 might be outweighed by the dangers of lowering legal barriers to military force in a wider range of circumstances or conditions. Indeed, some would argue that the strategic value of promoting a right of armed self-defense against cyber attacks could turn out to be quite low—since, among other reasons that are discussed in the following section, it may be difficult to sufficiently prove one's case publicly in justifying military responses—while doing so may introduce greater insecurity and instability to the international system by eroding normative constraints on military responses to non-military harms.

Another strategic danger is that of miscalculated escalation: perhaps we want law to help stay the hand of political leaderships who might be inclined to overreact to cyber crisis with force. Rather than clearing the way—normatively and bureaucratically—for decisionmakers pressing for forceful responses, international law can play a role in promoting more thorough deliberation, even if one doubts that in extreme situations it imposes perfect constraints on powerful States. This again suggests the need to think about the strategy of cyber attacks as armed attacks while examining the issue through a political lens, too.

IV. A POLITICAL PERSPECTIVE

A political perspective considers the situational context in which political decision makers will face these issues and predictive judgments about the reactions to cyber-attack crises of influential actors in the international system. The politics of cyber attacks will undoubtedly be shaped by law and

25. *See* NRC REPORT, *supra* note 6, at 256 (discussing costs and benefits to preventing escalation in setting an appropriate threshold for self-defense).

strategy in this area, but no effective legal or strategic doctrine can be designed that does not account for the politics.

The domestic and international politics of a future cyber crisis are, of course, impossible to predict accurately. A few features of such cases are very likely to influence those politics, however. First, cyber-attack incidents will probably involve a publicly ambiguous set of facts. Conventional military attacks are usually quite visible—kinetic violence can be and often is broadcast widely, immediately and understandably—and the common experience of them makes political reactions fairly (though far from entirely) predictable. Malicious computer code or actions in cyberspace, by contrast, are opaque to public view, technically very complex and likely to emerge piecemeal.

Second, and closely related, responses and reactions to cyber attacks will probably involve high levels of government secrecy. The perpetrators of cyber attacks may try to keep their responsibility and methods secret. Defenders too, though, may be reluctant to disclose details or even the very existence of cyber attacks, whether to protect secrets about their vulnerabilities and defenses, prevent public panic, avoid political embarrassment, or escape unwanted domestic pressure to take retaliatory actions. Consider the case of Stuxnet and other cyber attacks against Iran's nuclear development program: press accounts report that the United States and Israel launched these attacks covertly—trying not only to mask their responsibility but to mask the very existence of a cyber attack—while Iran officially denied that it had been attacked or suffered any significant harm.[26]

Third, cyber-attack incidents will involve difficulties in proving attribution. It is hotly debated how effectively States can trace digital fingerprints of cyber attacks, which may be routed through many unwitting third parties' computer systems, back to their ultimate source, and it is widely believed that some States would conduct cyber attacks through loosely affiliated or unofficial private parties. As a purely technical matter, these attribution challenges may be overstated, especially for the United States and its premier intelligence and cyber-forensic capabilities. As a political matter, however, a critical issue is whether attacked States or their allies can demonstrate the aggressor's culpability to domestic and international audiences sufficiently to justify armed self-defense. There may be a significant

26. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1.

gap between sufficiently establishing attribution for internal intelligence purposes and doing so for external justification of forceful responses.

A political upshot of these factors is that armed self-defense to a cyber attack will likely require quite a high minimum threshold of harm—probably a much higher quantum of harm than would be required if it were a conventional armed attack. Political decisionmakers will have a very difficult time rallying support at home and abroad for military responses to isolated cyber attacks that do not cause significant and publicly discernible damage, even though legal arguments might strengthen their hand in doing so. Whereas even low levels of hostile kinetic violence—say a barrage of small missiles that fail to detonate or cause much injury—will not only justify politically an armed response but may *demand* it politically, dud or stymied cyber attacks probably will not. Swiveling back to the legal perspective, this means that although legal line-drawing near the margins is very challenging for lawyers applying an effects-based analysis, it may not be quite so problematic in practice, because States are unlikely to respond to small-scale attacks with military force.

That said, it is also likely that very harmful cyber attacks for which armed self-defense is an option will occur against the background of or in combination with other hostile activities. In other words, and considering also the strategic perspective, there are likely to be few "naked" cases of cyber attacks—bolt-from-the-blue actions in the complete absence of other significant hostile actions or threats—against which political leaders will consider armed self-defense a viable response. States launching cyber attacks will likely be doing so in combination with other strategic acts, including militarily threatening moves. Non-State groups such as terrorist organizations against which military self-defense might make any sense will generally have already threatened other violence. Regardless of how such non-cyber moves and threats figure formally into a defending State's legal analysis, as a political matter they will no doubt figure significantly in its public justification of force.

V. CONCLUSIONS: LOOKING FORWARD

As the issue of cyber attacks as armed attacks is examined simultaneously through the three lenses—the legal, strategic and political—several general conclusions emerge. First, there is a range of reasonable interpretations of cyber "armed attacks" for the purposes of triggering militarily forceful self-defense, and a stable consensus is unlikely for the foreseeable

future. One reason for this legal instability is that strategic asymmetries pull interpretation in different directions.[27] I previously stated it this way:

> The United States appears to be placing its legal bets on a future world in which it can continue to rely partly on its comparative military edge to deter cyber-attacks while supplementing that deterrence with its own offensive, defensive, and preemptive cyber-capabilities—a bet that plays to some advantages but also carries risks. Reaching legal consensus with other major powers on these issues will be difficult in part because they perceive a different combination of strategic risks and opportunities. Therefore, U.S. policymakers should prepare to operate in a highly contested and uncertain international legal environment.[28]

The legal positions between States—and even within States—may shift over time as offensive advantages and defensive vulnerabilities shift. Moreover, international law regulating force changes very slowly, while the information technology creating these strategic opportunities and risks will continue to evolve rapidly.

Second, incremental legal development through State practice will be especially difficult to assess because of several features of cyber attacks. Actions and counteractions with respect to cyber attacks will lack the transparency of most other forms of conflict, sometimes for technical reasons but sometimes for political and strategic reasons. It will be difficult to develop consensus understandings even of the fact patterns on which States' legal claims and counterclaims are based, assuming those claims are leveled publicly at all, when so many of the key facts will be contested, secret, or difficult to observe or measure. Furthermore, the likely infrequency of "naked" cases of cyber attacks—outside the context of other threats or ongoing hostilities—means that there will be few opportunities to develop and assess State practice and reactions to them in ways that establish widely applicable precedent.

Finally, law can and should be used to support strategy in calibrating appropriate triggers and thresholds for self-defense, though the political features of cyber-attack crises—many of them directly linked to the technical features of cyber attacks—make doing so in advance more difficult than it has been with respect to conventional military threats. This means

---

27. On some of these asymmetries, see Thomas Rid, *Think Again: Cyberwar*, FOREIGN POLICY, Mar.–Apr. 2012, at 58.

28. Waxman, *supra* note 2, at 448–49.

that the adaptation of international law and the development among allies and partners of strategy to combat cyber threats go hand in hand. Those taking a more formalistic method to self-defense law may view this approach to legal interpretation as too malleable and subordinating of law to power politics. But any legal approach that fails to account for the strategic and political dynamics of cyber attacks is unlikely to survive early encounters with those realities.