AIR WAR COLLEGE

AIR UNIVERSITY

STUXNET, "SCHMITT ANALYSIS," AND THE CYBER "USE OF FORCE" DEBATE

by

Andrew C. Foltz, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

15 February 2012

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Andrew C. Foltz is a U.S. Air Force Judge Advocate attending the Air War College, Air University, Maxwell AFB, AL. He graduated from the U.S. Air Force Academy in 1991 with a Bachelor of Science degree in Political Science, the University of Maryland at College Park in 1993 with a Masters of Public Management, and the U.S. Air Force Air Command and Staff College in 2005 with a Masters of Military Operational Art and Science. He earned his *Juris Doctor* from the University of Oregon in 1999. He has served as a wing and MAJCOM intelligence officer, as a wing and deployed Staff Judge Advocate, and as a deployed combat operations legal advisor in the USCENTCOM AOR.

Abstract

One of the many vexing issues surrounding cyberspace involves whether peacetime cyber operations can constitute a prohibited use of force under Article 2(4) of the U.N. Charter. Among the analytic frameworks developed to address this issue, one of the most enduring is the so-called "Schmitt Analysis." It is also the only model that purports to adhere to preexisting legal norms, including Article 2(4). The framework consists of seven factors that states are likely to consider when characterizing cyber attacks—severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility. When the framework first debuted in 1999, however, there were few clear examples of state cyber coercion and the prospect of cyber-induced physical damage was largely theoretical. In light of several recent instances of suspected state cyber coercion—culminating in damage to Iranian nuclear facilities by the Stuxnet worm—it is now worth evaluating the framework's continued utility.

A Schmitt Analysis of Stuxnet suggests the framework's underlying analytical approach remains sound—i.e., to discern a cyber "use of force" threshold, one must predict how states will characterize cyber attacks. That said, Stuxnet reveals several limitations with the model, as well as opportunities to broaden it. Most importantly, it may be time to relax the model's strict adherence to Article 2(4), which was intended to provide more objective and predictable characterizations of force in cyberspace. In actuality, Article 2(4) has been a weak constraint on cyber coercion and it appears to be just one of many factors states will consider. Such additional factors reflect the new realities of cyberspace, such as cyber's potentially devastating effects, the non-traditional distribution of cyber capabilities and vulnerabilities, and the international community's response to events like Stuxnet. Consequently, until new norms emerge, cyber professionals must be prepared to operate in an ambiguous and contested legal environment.

Introduction

> *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.*
>
> Article 2(4), Charter of the United Nations[1]

One of the many seemingly intractable legal issues surrounding cyberspace involves whether and when peacetime cyber operations can constitute a prohibited use of force under Article 2(4) of the United Nations Charter.[2] Notwithstanding a significant body of scholarly work on this topic and extensive real-world examples from which to draw, there is no internationally recognized definition of a use of force.[3] Rather, what has emerged is a general consensus that *some* cyber operations will constitute a use of force, but that it may not be possible to identify in advance the specific criteria states will use in making such determinations.[4]

As discussed below, several analytic frameworks have been developed to help assess when cyber operations constitute a use of force. One conclusion each of these frameworks share is that cyber operations resulting in physical damage or injury will almost always be regarded as a use of force. When these frameworks were developed, however, there were few, if any,

[1] United Nations, *Charter of the United Nations and Statute of the International Court of Justice*, San Francisco, CA: 1945).

[2] The discussion in this paper addresses only *peacetime* cyber activities by states. Cyber activities conducted during armed conflict are governed by a different body of law—*jus in bello* and the Law of Armed Conflict—which is beyond the scope of this research.

[3] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1999), 925. See also, Senate, *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the Senate Armed Services Committee*, 11th Cong., 11th sess. (15 April 2010), 11.

[4] See, e.g., Walter Gary Sharp, Sr., *Cyberspace and the Use of Force*, (Falls Church, VA: Aegis Research Corp., 1999), 140 ("Any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4)"); and David E. Graham, "Cyber Threats and the Law of War," *Journal of International Law & Policy* 4 (2010): 91-2 (proponents of various analytic frameworks generally agree on the important conclusion that cyber attacks can constitute uses of force and armed attacks).

examples of peacetime state-sponsored cyber coercion. More importantly, the prospect of cyber attacks causing physical damage and injury was largely theoretical.[5] Beginning in 2007, however, a string of cyber operations—including the 2007 Distributed Denial of Service (DDoS) attack on Estonia, the 2008 DDoS attack on the country of Georgia, and the 2008 discovery that the U.S. government's most sensitive networks had been compromised—hinted at increased use of the cyber domain by states and their proxies for peacetime coercion.[6] Then, with the discovery of the Stuxnet worm in 2010, which damaged uranium enrichment equipment at a nuclear facility in Iran, theory became reality.

Although Stuxnet has been described as a watershed event, there has been little academic discussion on whether it constituted a use of force.[7] Perhaps this is because it caused physical damage and, therefore, clearly constitutes a use of force. This appears to be the emerging consensus.[8] Although I generally agree with this conclusion, I also believe that by looking beyond the physical damage, Stuxnet provides a unique opportunity to assess the adequacy and continued relevancy of these frameworks.

As a first step toward such an assessment, this paper tests one of the more robust analytic frameworks, known as the "Schmitt Analysis," by applying it to Stuxnet. Developed in 1999 by Professor Michael Schmitt, the Schmitt Analysis is one of the most academically rigorous and

[5] Isaac R. Porche III, Jerry M. Sollinger, and Shawn McKay, *A Cyberworm that Knows no Boundaries*, RAND Occasional Paper (Washington DC, 2011), ix.

[6] See, e.g., Thomas C. Wingfield, "International Law and Information Operations," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington DC: National Defense University Press, 2009), 531; Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* (Winter 2008-09): 60-76; and Ryan Singel, "Threat Level's Kim Zetter Writing the Book on Stuxnet," *Wired.com*, 24 October 2011.

[7] See, e.g., Duncan B. Hollis, "Could Deploying Stuxnet Be a War Crime?" *Opinio Juris* blog, 25 January 2011; and Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Forces Quarterly*, Issue 63 (4th Quarter 2011): 70-73. For a discussion of the *jus in bello* implications of Stuxnet, see John Richardson, *Stuxnet as Cyber Warfare: Applying the Law of War to the Virtual Battlefield,* Social Science Research Network Working Paper (2011).

[8] See., e.g., Hollis, "Could Deploying Stuxnet Be a War Crime?"; Michael N. Schmitt (US Naval War College, Newport RI) interview by the author, 1 December 2011; and Colonel Gary D. Brown (U.S. Cyber Command, Ft Meade, MD), interview by the author, 2 December 2011.

frequently cited frameworks for characterizing cyber operations.[9] The Schmitt Analysis consists of seven factors (severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility) that states are likely to consider when characterizing cyber activities. A key feature of the framework is that it remains faithful to Article 2(4) while at the same time effectively bridging key elements of competing analytic frameworks that do not exhibit such fidelity to the U.N. Charter. By focusing this evaluation on Professor Schmitt's model, I expect the results will have implications for the use of force debate more generally.

The paper begins with a discussion of why, as a practical matter, discerning a peacetime use of force threshold in cyberspace is important. Next, I detail Article 2(4)'s prohibition on the use of force and the difficulty applying it in the cyber context. I then review Professor Schmitt's model and perform a Schmitt Analysis of Stuxnet. Finally, I examine what the Schmitt Analysis of Stuxnet reveals about the framework's continued utility and relevance. Overall, I find Professor Schmitt's underlying analytical approach remains sound—i.e., the best way to characterize the lawfulness of peacetime cyber operations is to predict how states will evaluate and respond to them. That said, the Stuxnet analysis reveals several limitations with Professor Schmitt's framework, while also highlighting opportunities to broaden it. More importantly, I conclude that it may be time to relax the model's strict adherence to the U.N. Charter because Article 2(4) is just one of several factors states are likely to consider when characterizing the lawfulness of cyber operations.

[9] Most contemporary discussions involving the use of force in cyberspace make reference to the Schmitt Analysis. It was prominently featured in Chapter 22 of the National Defense University's 2009 book *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 525-542 (Washington DC: National Defense University Press, 2009). It also received favorable treatment in the National Research Council of the National Academies 2009 Report titled *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, edited by William A. Owens, Kenneth W. Dam, and Herbert S. Lin (Washington DC: National Academies Press, 2009), and more recently in the United States Army War College's 2011 *Information Operations Primer*, Carlisle Barracks, PA (November 2011).

Why the "Use of Force" Threshold Matters

Cyberspace represents a strategic vulnerability for many states because it is inextricably tied into their economies, critical infrastructures, and even their national security apparatus. Compounding these concerns is the fact that a wide range of actors have proven adept at exploiting these vulnerabilities. Cybercrime, for example, is now estimated to exceed $1 trillion globally per year.[10] Even the United States' most secure defense networks are not immune.[11] The scope of the problem has become so great that some claim the U.S. is engaged in a cyber war, and that it is losing.[12] The *2010 National Security Strategy* notes that: "[c]ybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[13] The White House's *2011 International Strategy for Cyberspace* goes further by proclaiming: "[w]hen warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country," to include an armed military response.[14]

Against this backdrop, discerning a cyber use of force threshold becomes important for a number of reasons. Foremost is that characterizing cyber operations is a precondition to

[10] U.S. Army War College, *IO Primer*, 23.

[11] In October 2008, National Security Agency (NSA) analysts discovered that previously-identified malware had penetrated both of the Department of Defense's classified network—the Secure Internet Protocol Router Network (SIPR-Net), which carries the bulk of the nation's routine classified information, and the Joint Worldwide Intelligence Communication System (JWICS), which carries top-secret and compartmentalized intelligence information. Ellen Nakashima, "Cyber-Intruder Sparks Massive Federal Response — and Debate Over Dealing With Threats," *Washington Post* (9 December 2011).

[12] See, e.g., Editorial, "Mike McConnell on how to win the cyber-war we're losing," *Washington Post*, 28 February 28 2010; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It,* (New York, NY: Harper-Collins Publishers, 2010); Ryan Singel, "Is the Hacking Threat to National Security Overblown?" *Wired Magazine*, 3 June 2009; and Bruce Schneier, "The Threat of Cyberwar Has Been Grossly Exaggerated," *Schneier.com*, 7 July 2010.

[13] The White House, *National Security Strategy* (Washington DC: May 2010), 27.

[14] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington DC: May 2011), 14.

determining which legal regime governs state behavior.[15] If state-sponsored cyber activities constitute a use of force, then international law governing the use of force (*jus ad bellum*) and the law of armed conflict (*jus in bello*) apply. In appropriate circumstances, this could trigger a state's right to self-defense and thereby permit a forceful, perhaps even armed response. In contrast, cyber operations not amounting to a use of force are traditionally governed by more constrained law enforcement regimes.[16]

The need for clarity has taken on greater importance now that the U.S. and many of its allies treat cyberspace as a military operational domain.[17] Accordingly, discerning a use of force threshold would seem to be necessary for a wide-range of peacetime military activities, such as: defining the spectrum of permissible peacetime cyber operations, such as computer network exploitation; developing peacetime cyber rules of engagement; identifying appropriate approval authorities; assigning appropriate agency responsibilities and resources; signaling adversaries and allies as part of a deterrence strategy; recognizing when treaty obligations have been triggered; and determining whether U.N. Security Council authorization is required.

The "Use of Force" in Cyberspace

Notwithstanding the need for clarity discussed above, there is no international consensus on what constitutes a use of force in cyberspace,[18] nor does it appear a mechanical rule is likely

[15] Charles J. Dunlap Jr., "Perspectives for Cyber Strategists on Law and Cyberwar," *Strategic Studies Quarterly* (Spring 2011), 84; and Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Implications*, NATO Cooperative Cyber Defence Centre, Tallin, Estonia (2010), 79.

[16] Dunlap, "Perspectives for Cyber Strategists," 84.

[17] See, e.g., US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,* Washington DC (July 2011), 5; White House, *National Security Strategy,* 22; and White House, *International Strategy for Cyberspace,* 14.

[18]As Gary Sharp has noted: "[w]hat constitutes a prohibited 'threat or use of force' is a question of fact that must be subjectively analyzed in each case in the context of all relevant law and circumstances. Such a question of fact defies rote, categorical definition." Sharp, *CyberSpace and the Use of Force,* 52. As then-Lieutenant General Keith Alexander noted in testimony before the Senate Armed Services Committee prior to his confirmation as the first commander of United States Cyber Command, "[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

to emerge any time soon.[19] This section describes why the ambiguity persists and the various solutions that have been proposed to resolve it. After summarizing the relevant law governing the use of force in international relations, I highlight the technical, legal, and political challenges of applying existing norms within cyberspace.

The "Use of Force" Under the U.N. Charter

Jus ad bellum[20] describes the law governing the transition from peace to armed conflict. Though grounded in customary international law, the black letter principles of *jus ad bellum* are now contained in Article 2(4) of the U.N. Charter, which prohibits states from the "threat or use of force" in their international relations.[21] Several features of this prohibition are problematic in the cyber context. First, Article 2(4) only pertains to international relations between sovereign states—it does not proscribe the conduct of non-state actors, who appear to be the source of most malicious cyber activity. Also, as noted above, the Charter does not define the phrase "use of force." Finally, Article 2(4) does not sanction any exceptions to the prohibition on the unilateral use of force, nor does it prescribe remedies for unauthorized uses of force. Such exceptions and remedies are found in Chapter VII of the Charter which, unlike Article 2(4), is not limited to

different thresholds for what constitutes a use of force." US Senate, *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the Senate Armed Services Committee,* 11th Cong., 11th sess., 15 April 2010.

[19] As one commentator has noted, "Although the application of the UN Charter Article 2(4) to CNA [computer network attack] is an intellectually interesting question, there is reason to wonder whether, as a practical matter, the issue ever will arise in a context requiring an actual decision. The most important obstacle may be the difficulty of attributing CNA to State action. Moreover, even if State use of CNA were to emerge as a recognizable phenomenon, such CNA would have to occur in relative isolation in order squarely to pose the relevant legal issue. Because this seems improbable, it likely will be a long time, if ever, before the practice of States, decisions of the International Court of justice (ICJ), or other recognized sources of international law yield a clarification of how Article 2(4) applies to CNA." Daniel B. Silver, "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter," in *Naval War College International Law Studies, Vol. 76, Computer Network Attack and International Law,* ed. Michael N. Schmitt and Brian T. O'Donnell (Newport, RI: 2002), 77-78.

[20] Latin for "right to the war," more commonly understood as the "right to wage war."

[21] Although the U.N. Charter is technically binding only upon signatories, Article 2(4)'s prohibition on the use of force is also considered a principle of customary international law and is thereby binding upon all states. See discussion of the issue by the International Court of Justice in *Nicaragua v. United States*, 1986 ICJ Reports 226, paragraphs 187-191 (27 June 1986) (hereinafter "*Nicaragua*").

relations between states and which employs thresholds quite distinct from the “use of force” standard.[22] Importantly, it is not the use of force, but rather an “armed attack” that triggers a state’s right to use force in self-defense.[23]

Although “use of force” is not defined, an approximate threshold has emerged through consideration of the Charter’s preparatory work, state practice, and *opinio juris*.[24] First, the framers of the Charter took an instrument-based, vice consequence-based, approach to the use of force prohibition.[25] While acknowledging that states are most concerned about the consequences of coercive activities (i.e., the degree of injury, deprivation or destruction), the framers recognized that a consequence-based criterion was too subjective to distinguish lawful from

[22] For example, compare Article 39’s “breach of the peace” and “aggression” thresholds; Article 41’s “measures short of armed force” standard; Article 42’s “such action by air, sea, or land forces as may be necessary” language; and Article 51’s “armed attack” threshold for self-defense actions.

[23] Schmitt, “Thoughts on a Normative Framework,” 920. This begs the question on what constitutes an “armed attack,” particularly in the cyber context. Again, the term is not defined in the U.N. Charter or other treaties. There is, however, a framework for assessing whether State actions amount to armed attacks that is relevant to the characterization of cyber attacks. In short, to be characterized as an “armed attack,” an action must be intentional, involve violent effects, and risk or cause of injury to persons or property. In the cyber context, so long as a cyber operation is likely to produce such violent consequences, it will likely be characterized as an armed attack. See, e.g., Dunlap, “Perspectives for Cyber Strategists,” 85-6 (“[i]t is important to understand that in determining whether the cyber activity is severe enough to amount to the legal equivalent of an armed attack (as opposed to merely a use of some force), the consequences must extend to more than mere inconvenience; there must be at least temporary damage of some kind”); and Michael N. Schmitt, “Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict,” in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 151-178 (Washington, DC: National Academies Press, 2010), 163 (“essence of an ‘armed’ operation is the causation, or risk thereof, of death or injury to persons or damage to or destruction of property and other tangible objects.”). It also appears that not all uses of “armed force” constitute an “armed attack” because the underlying actions must also be of “sufficient scope, duration, and intensity” and exhibit certain “scale and effects.” See Graham, “Cyber Threats and the Law of War,” 90. Consequently, Schmitt notes, “by contemporary international law, qualitative indicators of attack (death, injury, damage or destruction) are more reliable in identifying those actions likely to be characterized as an armed attack than quantitative ones (number of deaths or extent of destruction).” Schmitt, “Cyber Operations in International Law,” 164.

[24] Schmitt, “Thoughts on a Normative Framework,” 905-7. *Opinio juris* means a sense of legal obligation. In the international law context, it is used to judge whether State practice and adherence to norms is due to a sense of legal obligation, vice political expediency or convenience. Duhaime.org Legal Dictionary, http://www.duhaime.org/LegalDictionary/O/OpinioJuris.aspx (accessed 12 December 2011). When *opinio juris* exists and is consistent with nearly all state practice, customary international law emerges. For example, Article 38(1)(b) of the Statute of the International Court of Justice accepts “international custom” as a source of law, but only where this custom is: (1) “evidence of a general practice,” and (2) “accepted as law.”

[25] See., e.g., Schmitt, “Thoughts on a Normative Framework,” 909; and Duncan B. Hollis, “Why States Need an International Law for Information Operations,” *Lewis & Clark Law Review* 11 (2007), 1040.

unlawful state coercion.[26] Because the term "force" connotes violence, injury and destruction—consequences that pose the greatest threat to international peace and security—they adopted the instrument-based "use of force" standard as prescriptive short-hand. According to Professor Schmitt, such an approach "eases the evaluative process by simply asking whether force has been used, rather than requiring a far more difficult assessment of the consequences that have resulted."[27] According to this approach, Article 2(4)'s prohibition does not extend to all forms of state coercion. For example, the instruments of economic and political coercion are not prohibited.[28] Less clear, but generally accepted, is that the prohibition is not limited to "armed" force—it may also encompass unarmed, non-military physical force, such as releasing water from a dam.[29] The International Court of Justice (ICJ) highlighted this point in *Nicaragua v. United States* (hereinafter "*Nicaragua*"), when it concluded that arming and training guerillas amounted to a prohibited use of force, even though it did not rise to the level of an armed

[26] Schmitt, "Thoughts on a Normative Framework," 914. As Professor Schmitt notes:

> At least since promulgation of the Charter, this use of force paradigm has been instrument-based; determination of whether or not the standard has been breached depends on the type of the coercive instrument—diplomatic, economic, or military—selected to attain the national objectives in question. The first two types of instruments might rise to the level of intervention, but they do not engage the normatively more flagrant act of using force.
>
> ***
>
> In fact, the international community is not directly concerned with the particular coercive instrumentality used (force in this case), but rather the consequences of its use. However, it would prove extraordinarily difficult to quantify or qualify consequences in a normatively practical manner. Undesirable consequences fall along a continuum, but how could the criteria for placement along it be clearly expressed? In terms of severity? Severity measured by what standard of calculation? Harm to whom or what?

[27] Ibid., 911.

[28] Ibid. A compelling argument does exist, however, that political and economic coercion that threatens the territorial integrity or political independence of another state constitutes an unlawful use of force under Article 2(4). See Sharp, *Cyberspace and the Use of Force,* 89-90, 118.

[29] Sharp, *Cyberspace and the Use of Force*, 101. It is according to this principle that the use of chemical or biological weapons is also considered a use of force, even though they do not produce the kinetic effects traditionally ascribed to armed force.

attack.[30] Accordingly, the use of force threshold has traditionally been viewed as lying somewhere between purely economic and political coercion on the one hand and activities that result in physical damage or injury on the other.[31] As discussed below, discerning a clear use of force threshold in this grey area—a difficult task even in traditional kinetic context—has proven particularly difficult in the cyber context.[32]

The "Use of Force" in Cyberspace

The difficulty applying Article 2(4) in cyberspace is that the instrument-based paradigm does not cleanly translate to cyber operations—particularly for grey area operations that do not result in physical harm.[33] According to a strict instrument-based interpretation, even highly disruptive peacetime cyber operations may not qualify as a use of force because they lack the traditional kinetic characteristics associated with armed force.[34] Most commentators reject this strict interpretation because of the potential widespread destabilizing consequences of cyber operations. That said, by focusing on consequences to determine whether prohibited force has been used, they call Article 2(4)'s instrument-based paradigm into question.

The perceived shortcomings of Article 2(4) have led many to propose new treaty law to govern cyber operations.[35] Others counter that states are unlikely to negotiate any meaningful treaties in the foreseeable future. They argue that divergent strategic interests and significant attribution problems make treaty enforcement unrealistic. They suggest that existing

[30] *Nicaragua*, para 228. According to the ICJ, the distinction between the threat or use of force (including armed force) and an armed attack is based on the operation's "scale and effects." *Nicaragua*, para 195.

[31] Schmitt, "Cyber Operations in International Law," 155.

[32] See Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *The Yale Journal of International Law* 36 (2011), 445-47.

[33] Hollis, "Why States Need an International Law for IO," 1040.

[34] Ibid., 1041. Professor Schmitt highlighted this dilemma when he noted: "The advent of cyber operations threw the instrument-based approach into disarray by creating the possibility of dramatically destabilizing effects caused by other than kinetic actions." Schmitt, "Cyber Operations in International Law," 177.

[35] See, e.g., Clark and Knake, *Cyber War*, 219-55; Hollis, "Why States Need an International Law for IO," 1053; and Silver, "Computer Network Attack as a Use of Force," 78.

international norms, though imperfect, are adequate for extrapolating general principles governing the use of force in cyberspace and urge gradual expansion of international norms within the Article 2(4) framework.[36]

Over the past two decades, proponents of this gradualist approach have developed several analytic frameworks to characterize the legality of cyber operations. First is the “effects-based” approach, which states that the quantum of damage, and not the means of attack, is all that matters.[37] The advantage of this approach—which is generally favored by U.S. policy makers and military operators—is that it is fairly simple to apply and it acknowledges that states are principally concerned about consequences.[38] The drawback is that it represents a hard break from the Charter’s instrument-based approach and thereby relies on inherently subjective assessments among states that have divergent strategic capabilities, vulnerabilities and interests. A second approach relies upon kinetic equivalency, arguing that cyber operations constitute a use of force only if the damage they cause could previously have been achieved only by a kinetic

[36] See, e .g., US Department of Defense, *An Assessment of International Legal Issues in Information Operations,* (Washington DC: Office of General Counsel, May 1999), 11 (advent of new information operation rules appears premature and the “process of extrapolation appears to be relatively predictable”); Dunlap, “Perspectives for Cyber Strategists,” 83 (“it is not likely that any new international treaty governing cyberwar or cyber weaponry will be forthcoming in the foreseeable future”); Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Falls Church, VA: Aegis Research Corp., 2000), 31 (“[I]t is possible to articulate an intellectual framework describing the relationship of these thresholds, and their general applicability to any given fact pattern.”); Hollis, “Why States Need an International Law for IO,”1038 (“majority of military thinkers … in favor of an analogy approach or decrying the possibility of IO-specific rules as premature or unrealistic”); Schmitt, “Cyber Operations in International Law,” 177 (“highly unlikely that any meaningful treaty will be negotiated to govern cyber operations in the foreseeable future”); and International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* 4 (2003) (“existing legal framework is on the whole adequate to deal with present day international armed conflicts”).

[37] For example, the National Research Council of the National Academies recently noted: “In the committee’s view, the essential framework for the legal analysis of cyberattack is based on the principle that notions related to ‘use of force’ and ‘armed attack’ (terms of special relevance to the Charter of the United Nations) should be judged primarily by the effects of an action rather than its modality. That is, the fact that an attack is carried out through the use of cyberweapons rather than kinetic weapons is far less significant than the effects that result from such use, where ‘effects’ are understood to include both direct and indirect effects. National Research Council of the National Academy of Science, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, edited by William A. Owens, Kenneth W. Dam, and Herbert S. Lin (Washington DC: National Academies Press, 2009), 3.

[38] See, e.g., Thomas C. Wingfield, “When is a Cyber Attack an ‘Armed Attack?’ Legal Thresholds for Distinguishing Military Activities in Cyberspace” (Cyber Conflict Studies Association, 1 February 2006), 6; and Graham, “Cyber Threats and the Law of War,” 92.

attack.[39] This framework generally adheres to the Charter's instrument-based approach, but it struggles to characterize hostile grey area cyber operations—such as projecting false targets on an adversary's early warning radars—that do not result in physical damage. A third approach applies a "strict liability" test for any cyber operations that targets a state's critical infrastructure and vital interests because of the severe consequences that could result from such attacks. According to this model, the mere penetration of such systems—such as power production, stock exchanges and air traffic control—can constitute evidence of hostile intent and thereby trigger the right of self-defense.[40] This framework suffers from the inherent subjectivity of defining what constitutes "critical infrastructure and vital interests," and because it expands the grey area by encompassing activities, such as computer network exploitation, that are not currently prohibited by international law. Professor Schmitt's framework, discussed in detail below, represents the fourth major model.

The Schmitt Analysis

Professor Schmitt recognized that discerning the use of force threshold is really about predicting how states will characterize and respond to cyber incidents in light of prevailing international norms.[41] To aid in such predictions, his framework bridges the instrument- and consequence-based approaches. In keeping with Article 2(4)'s instrument-based standard, his framework consists of seven factors that represent the major distinctions between permissible (i.e., economic and political) and impermissible (i.e., armed) instruments of coercion.[42] When

[39] See, e.g., Hollis, "Why States Need an International Law for IO," 1041; and Graham, "Cyber Threats and the Law of War," 91.
[40] Sharp, *Cyberspace and the Use of Force*, 129-31; and Hollis, "Why States Need an International Law for IO," 1041.
[41] Schmitt, interview by the author. In this regard, Professor Schmitt noted that states would likely seek to balance the conflicting objectives of maximizing their own freedom of action in cyberspace while avoiding the harmful consequences caused by adversaries. See also, Schmitt, "Cyber Operations in International Law," 155.
[42] Schmitt, "Thoughts on a Normative Framework," 914.

applying these factors, the more the attributes of a cyber operation approximate the attributes of armed force, the more likely states are to characterize the operation as a prohibited use of force. The Schmitt Analysis factors consist of:

1. Severity: Cyber operations that threaten physical harm more closely approximate an armed attack. Relevant factors in the analysis include scope, duration and intensity.

2. Immediacy: Consequences that manifest quickly without time to mitigate harmful effects or seek peaceful accommodation are more likely to be viewed as a use of force.

3. Directness: The more direct the causal connection between the cyber operation and the consequences, the more likely states will deem it to be a use of force.

4. Invasiveness: The more a cyber operation impairs the territorial integrity or sovereignty of a state, the more likely it will be viewed as a use of force.

5. Measurability: States are more likely to view a cyber operation as a use of force if the consequences are easily identifiable and objectively quantifiable.

6. Presumptive legitimacy: To the extent certain activities are legitimate outside of the cyber context, they remain so in the cyber domain; e.g., espionage, psychological operations, and propaganda.

7. Responsibility: The closer the nexus between the cyber operation and a state, the more likely it will be characterized as a use of force.[43]

According to Professor Schmitt, evaluating these factors is an imprecise and subjective endeavor. The factors are useful, but not determinative, and they should not be applied mechanically. Rather, they need to be applied holistically according to the relevant context; i.e., which factors are important and how they should be weighted will vary on a case-by-case basis. Moreover, he never intended the factors to be exhaustive, though they are often treated as such.[44]

[43] Professor Schmitt's detailed description of each factor appears in the Appendix.

[44] Schmitt, interview with author. See also, Michael N. Schmitt, "The Sixteenth Waldemar A. Solf Lecture in International Law," *Military Law Review* 176 (2003), 417.

Finally, the framework is more useful for post-hoc forensic analysis of particular cyber attacks than for characterizing real-time operations.[45]

Professor Schmitt also acknowledged that his adherence to Article 2(4)'s instrument-based paradigm appears tortuous, particularly given the appeal of simple effects-based frameworks. However, he reasoned that such adherence is necessary to properly describe where the cyber use of force threshold lies under prevailing standards—in contrast to the other leading models, which prescribe new standards for where the use of force threshold *should* lie.[46] He also believed that "reference to the instrument-based shorthand facilitates greater internal consistency and predictability within the preexisting framework …. As a result, subscription by the international community is more likely, and application should prove less disruptive and controversial."[47] In the end, the Schmitt Analysis has generally stood the test of time and it remains one of the most commonly referenced frameworks for characterizing the use of force in cyberspace. In the next section, I conduct a Schmitt Analysis of Stuxnet to assess the framework's continued utility.

[45] Schmitt, interview with author. Professor Schmitt's framework has been described as too cumbersome and complex to support real-time cyber operations. In response, Professor Schmitt notes that the factors he articulated were never intended to serve as an operational model. Rather, it is the underlying analytic approach that is important—i.e., trying to predict how other states are likely to characterize cyber operations in light of current international norms. The factors themselves are simply derived from the premise that states will likely characterize as uses of force those cyber operations that manifest many of the same characteristics as armed force, as it is understood in the context of Article 2(4).

[46] Schmitt, "Thoughts on a Normative Framework," 917. Professor Schmitt noted that the adoption of an effects-based framework "would constitute a new standard." In contrast, he went on to explain, "reference to the instrument-based shorthand facilitates greater internal consistency and predictability within the preexisting framework for inter-state coercion. It allows determinations on the inclusivity of the use of force to more closely approximate the current system than analysis based solely on consequentiality would allow. As a result, subscription by the international community is more likely, and application should prove less disruptive and controversial. This is not to say that greater focus on core objectives, on consequentiality in its pure form, is not to be sought. It is only a recognition that until the international community casts off its current cognitive approach, community values are, for practical reasons, best advanced in terms of that which is familiar and widely accepted."

[47] Ibid.

Characterizing “Stuxnet”

Background

Stuxnet has been described as a game changer—the first digital “fire and forget” precision-guided munition and perhaps the first peacetime act of cyberwar.[48] According to reports, the Stuxnet worm was designed to target gas centrifuges used in Iran’s uranium enrichment program in Natanz. Specifically, the worm exploited the software used in programmable logic controllers (PLCs) manufactured by Siemens. These PLCs controlled frequency converter drives that, in turn, controlled the speed of the centrifuges. By manipulating the speed of already temperamental and frequency-sensitive centrifuges over time (weeks, and perhaps months), Stuxnet caused as many as 1,000 of the centrifuges to break. Estimates suggest Stuxnet set Iran’s nuclear program back by several years.[49]

Although some have described Stuxnet’s code as a relatively unsophisticated “Frankenstein patchwork of existing tradecraft, code and best practices drawn from the global cyber-crime community,” its true sophistication lies in the synergy of its components and its method of infection.[50] First, Stuxnet’s designers required incredibly precise intelligence about Iran’s PLCs and frequency converters, as well as the performance parameters of Iran’s centrifuges.[51] Second, the malware was self-replicating and designed to infect systems that were not connected to the internet (“air-gapped”), thereby requiring the use of intermediary devices such as thumb drives. Stuxnet also employed four “zero-day” exploits and two stolen digital

[48] See, e.g., Lukas Milevski, “Stuxnet and Strategy: A Special Operation in Cyberspace?” *Joint Forces Quarterly*, Issue 63 (4th Quarter 2011), 64; and Porche, Sollinger, and McKay, *A Cyberworm that Knows no Boundaries*, 1.

[49] See Kim Zetter, “How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History,” *Wired.com* (11 July 2011); Porche, Sollinger, and McKay, *A Cyberworm that Knows no Boundaries*; Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*, (Symantec, February 2011); and Hollis, “Could Deploying Stuxnet Be a War Crime?”

[50] Milevski, “Stuxnet and Strategy,” 66 (citing James P. Farwell and Rafal Rohozinski, “Stuxnet and the Future of Cyber War,” *Survival* 53, no. 1 (January 2011), 24.).

[51] According to reports, representatives from the International Atomic Energy Agency who had inspected Natanz did not even have this level of information. Ibid., 65.

signatures to gain access to targeted systems.[52] Finally, Stuxnet appears to have been designed to avoid collateral damage.[53] If the malware did not detect the specific software-hardware configuration associated with Iran's enrichment program, the program would lie dormant. It was also designed to delete itself from thumb drives after infecting three machines, and it contained a built-in self-destruct feature. Thus, even though the worm is reported to have infected more than 100,000 hosts in 155 countries, 60% of the infections were localized to Iran, and there are no reports of physical damage outside of Iran.[54] Although no one has claimed responsibility for Stuxnet, it has the signature of a state operation.[55] Most speculation and some anecdotal evidence points to Israel, with possible support from the U.S. and/or Germany.[56]

Schmitt Analysis of Stuxnet

Although there is an emerging consensus that Stuxnet constituted a use of force, there is value in looking beyond the physical damage to see what the operation reveals about the strengths and weaknesses of existing analytic frameworks, such as the Schmitt Analysis. Accordingly, the following analysis is offered not only to characterize Stuxnet, but to help evaluate Professor Schmitt's framework.

Severity: According to this criterion, Stuxnet is per se a use of force because it caused physical damage. Moreover, the damage was inflicted upon a critical Iranian interest—its nuclear program. By setting Iran's nuclear program back by several years, the duration of Stuxnet's consequences also supports characterizing it as a use of force—though this delay is

[52] A zero-day threat is a software vulnerability unknown to the user or software developer that can be exploited before the vulnerability can be fixed.

[53] Richardson, *Stuxnet as Cyber Warfare*, 7.

[54] Falliere, Murchu, and Chien, *W32.Stuxnet Dossier*, 10. Despite early speculation that Stuxnet damaged an Indian satellite, the claim has never been substantiated.

[55] Porche, Sollinger, and McKay, *A Cyberworm that Knows no Boundaries*, 8.

[56] See, e.g., Zetter, "How Digital Detectives Deciphered Stuxnet;" Brown, "Why Iran Didn't Admit Stuxnet Was an Attack;" Richardson, *Stuxnet as Cyber Warfare*, 30; and William J. Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," New York Times, 15 January 2011.

more a function of economic sanctions that bar Iran from legitimately acquiring new centrifuges. It is also worth noting that the scope of the actual damage appears to have been relatively minor, fairly discrete, and that it posed no apparent risk of harm to personnel.

Immediacy: According to this factor, Stuxnet would probably not be viewed as a use of force. The attack, which consisted of at least three waves over 10 months, took time to evolve.[57] More importantly, once a targeted system was infected, it appears the damage took weeks or even months to manifest. Given the nature of how the attack unfolded, there was—and remains—adequate opportunity for Iran to mitigate the harmful effects and to seek peaceful accommodation. That said, given the physical damage inflicted, immediacy is probably not a factor that warrants much emphasis in this analysis.

Directness: There appears to be a direct causal connection between Stuxnet and the damaged centrifuges.

Invasiveness: Stuxnet represents a significant intrusion on Iranian sovereignty. Not only did it cross international borders, but it targeted sensitive and highly secure systems that were air-gapped from the internet. That said, Stuxnet would have been just as invasive if it had simply collected intelligence on the inner workings of the Natanz facility—an activity the international community would likely not regard as a use of force.[58]

Measurability: Taking into account the already high failure rate of Iran's centrifuges, the consequences attributed to Stuxnet appear both quantifiable and identifiable.

[57] Falliere, Murchu, and Chien, *W32.Stuxnet Dossier,* 8.

[58] Professor Schmitt acknowledged this problem with the "invasiveness" factor when he noted: "In the cyber context, this factor must be cautiously applied. In particular, cyber exploitation is a pervasive tool of modern espionage. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target-State's territory, as in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace. Thus, actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force." Schmitt, "Cyber Operations in International Law," 156.

Presumptive legitimacy: Stuxnet does not enjoy presumptive legitimacy. Short of U.N. Security Council authorization or actions taken in self-defense—both of which would constitute *lawful* uses of force—there is no customary acceptance within the international community for damaging another state's nuclear facilities. Even so, it is worth considering the effect of existing Iranian sanctions upon this analysis. First, Iran cannot import or export nuclear-related materials or technology. If such Iranian-owned nuclear materials are discovered outside of Iran, they can be lawfully seized and destroyed. Second, prior to Stuxnet, Iran had been operating its centrifuges for several years in violation of multiple U.N. Security Council Resolutions.[59] Although these points may relate more to whether Stuxnet constituted a *lawful* use of force, they also seem to bear on the factor of presumptive legitimacy.

Responsibility: Although no state has claimed responsibility for Stuxnet, the worm's purpose and design clearly point to state involvement.

On balance, the Schmitt Analysis suggests most states would characterize Stuxnet as a use of force. The worm was highly invasive, caused direct and measurable physical damage, lacked a clear presumption of legitimacy, and it bore the markings of a state-sponsored operation.

Discussion

What does the foregoing analysis of Stuxnet reveal about the continued usefulness of Professor Schmitt's framework? Most importantly, the model's underlying analytic approach appears sound; i.e., discerning the use of force threshold entails predicting how states will characterize and respond to cyber operations. That said, the analysis reveals several limitations with the framework, as well as opportunities for its expansion.

[59] See, e.g., U.N. Security Council Resolutions 1737 (2006), 1747 (2007); 1803 (2008), and 1929 (2010).

First, it appears that in any given Schmitt Analysis, the characterization of a cyber operation is likely to be derived by a single factor: severity of the consequences. If true, then the framework could arguably be reduced to an effects-based model with little remaining affinity with Article 2(4)'s instrument-based paradigm.[60] To illustrate the point, what if—instead of damaging Iran's centrifuges—Stuxnet achieved the same effects by causing the centrifuges to operate inefficiently or not at all? Except for severity, each of Schmitt's factors would likely be evaluated the same. It is debatable, though, whether the international community would consider such an operation a prohibited use of force. This is not to suggest that the other factors are irrelevant, but it highlights what Professor Schmitt himself acknowledged: "severity is self-evidently the most significant factor in the analysis."[61]

Next, the characteristics of Stuxnet and its intended target suggest at least one additional factor that may be relevant when performing a Schmitt Analysis: apparent compliance with the law of armed conflict (LOAC). Assuming reports are true, the fact Stuxnet was targeted so precisely and designed to minimize collateral damage reveals something about the identity and intent of its creators. First, it reinforces the notion that Stuxnet was a state-sponsored operation, which is important because Article 2(4) only regulates state conduct. Second, it suggests Stuxnet's creators were concerned about complying with LOAC, particularly the principles of military necessity, distinction and proportionality.[62] Thus, the responsible state apparently

[60] As Daniel B. Silver, former General Counsel to both the National Security Agency and Central Intelligence Agency, notes, the Schmitt Analysis "turns out to be somewhat illusory …. At bottom, it leads to a conclusion that probably can be reached by reference to only one criterion: whether the foreseeable consequence of a particular manifestation of [computer network attack] is physical injury or property damage comparable to that resulting from military weapons." Silver, "Computer Network Attack as a Use of Force," 92.

[61] Schmitt, "Cyber Operations in International Law," 156.

[62] The LOAC principle of military necessity authorizes the use of force to accomplish military missions. It helps commanders identify lawful military targets during hostilities. The principle of proportionality involves weighing the anticipated gains of military operations against the reasonably foreseeable consequences to protected persons and places; e.g. civilians. Some collateral damage is generally unavoidable and is, therefore, allowable—but only if the reasonably foreseeable collateral damage is not disproportionate compared to the military advantage likely to be

regarded Stuxnet as the equivalent of an armed attack and executed the operation as such. The implication is that—even in grey area operations that do not result in actual damage—the more a cyber attack appears to comply with LOAC, the more states will regard it as a use of force.

A third observation involves one of the most technically challenging aspects of cyber operations: attribution. For Article 2(4) and the principles of *jus ad bellum* to apply, the offending party must be identified and generally must be a state.[63] As noted above, without reliable attribution states generally must respond to cyber operations as a law enforcement problem. Yet each of the prevailing frameworks, including the Schmitt Analysis, treats attribution as a condition precedent to any use of force analysis.[64] In other words, without attribution, a Schmitt Analysis offers limited practical value. But if attribution can be established, it is questionable whether a Schmitt Analysis would be necessary because more influential indicators should be discernable, such as motive and intent.

Next, to the extent state attribution bears on the characterization of cyber operations, so too should the victim state's response. As the ICJ noted in *Nicaragua*: "it is the State which is the victim of an armed attack which must form and declare the view that it has been so attacked."[65] Although Iran has acknowledged the presence of Stuxnet in its systems, it has denied any significant damage resulting from the worm and it has never claimed that it was attacked. As U.S. Cyber Command's top lawyer, Colonel Gary Brown, has commented: "Iran's 'non-position' on the Stuxnet event has been frustrating to practitioners in the field of cyberspace

gained from the attack. The principle of distinction directs combatants to distinguish between combatant forces and noncombatants, to direct force only against legitimate military objectives, and to refrain from targeting protected persons and places. *Air Force Operations & The Law: A Guide for Air, Space & Cyber Forces*, The Judge Advocate General's School, Maxwell AFB, AL (2009), 13-20.

[63] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4 (2010), 77. For a discussion on the possible expansion of *jus ad bellum* to permit the use of force against terrorists, see Michael N. Schmitt, "Responding to Transnational Terrorism Under the *Jus Ad Bellum*: A Normative Framework," *Naval Law Review* 56, 2008: 1-42.

[64] Schmitt, interview with author.

[65] *Nicaragua*, para 195.

operations. Finally, there was a well-documented, unambiguous cyber attack to dissect! And yet there was little official discussion of the issue because Iran passed up its opportunity to complain of an unjustified attack."[66] Unfortunately, Professor Schmitt's framework does not address the implications of such state inaction. It remains to be seen what, if any, impact Iran's "non-position" has on the development of use of force norms in cyberspace.

A more significant observation relates to the premise for Professor Schmitt's framework; i.e., that states will principally rely upon existing norms, particularly Article 2(4), when making use of force determinations in cyberspace. As some commentators predicted—and Stuxnet demonstrated—Article 2(4) has proven to be a "weak constraint on offensive cyber-attacks."[67] This is due, in part, to the difficulty observing, measuring and attributing cyber operations. More importantly, it reflects the fact that international law is not static and that the principles of *jus ad bellum* are not the exclusive province of the U.N. Charter.[68] For example, current interpretations of Article 2(4) are based on the distribution of more traditional measures of power—such as military and economic capacity—yet the distribution of cyber capabilities and vulnerabilities does not mirror such traditional measures.[69] Consequently, states are likely to consider factors well beyond Article 2(4)'s use of force prohibition when characterizing the legality of cyber operations. Such additional considerations would likely include: relative cyber strengths and vulnerabilities; strategic risks and opportunities; scope of potential consequences; ability to control escalation; effectiveness of cyber deterrence; potential reactions by adversaries, allies and international bodies like the U.N.; domestic politics; state declaratory policies; emerging state practice (including state inaction); continuing problems with attribution; as well as other legal,

[66] Brown, "Why Iran Didn't Admit Stuxnet Was An Attack," 71.
[67] Waxman, "Cyber-Attacks and the Use of Force," 426.
[68] Graham, "Cyber Threats and the Law of War," 88.
[69] Waxman, "Cyber-Attacks and the Use of Force," 448-58.

political, and technical constraints.[70] Moreover, given the novelty of cyberspace and the relative distribution of cyber capabilities and vulnerabilities, different states will likely weigh their strategic risks and opportunities very differently.

Perhaps these additional considerations explain why there has been so little academic debate about the legal implications of Stuxnet—notwithstanding the significant attention it has received as a technological watershed. Even though most states would probably agree that Stuxnet constituted a use of force under Article 2(4), they may be reluctant to characterize the attack as unlawful since, by targeting an illicit program in a pariah state, it was justifiable. In this regard, it is worth noting that Stuxnet's objective was consistent with multiple U.N. Security Council mandates and it promoted those mandates without resorting to *armed* force. Thus, it remains to be seen whether Stuxnet represents a new form of tacitly condoned cyber vigilanteism, or whether the perpetrator(s) will eventually be held in contempt. Either way, Iran's "non-position" has made it easy for the international community to sidestep the issue.

Conclusion

Overall, Professor Schmitt's analytic approach to characterizing cyber operations remains sound. Nonetheless, the Stuxnet analysis reveals several shortcomings with his framework, including: severity of the consequences as a potentially determinative factor; attribution as a condition precedent to a use of force analysis; and failure to account for a victim state's "non-position." The analysis of Stuxnet also reveals at least one additional factor states may consider when characterizing cyber operations—whether an attack appears to comply with LOAC. More importantly, the analysis suggests it is time to relax the model's strict adherence to Article 2(4)'s instrument-based paradigm. By tying his framework to Article 2(4), Professor Schmitt

[70] Ibid. See also, Graham, "Cyber Threats and the Law of War," 89.

anticipated more consistent, predictable and relatively objective characterizations of force in cyberspace. However, state practice over the last decade suggests that states will treat Article 2(4) as just one of several factors to consider when characterizing cyber operations.[71] As Professor Schmitt himself acknowledged, as state practice emerges, other considerations and normative approaches—such as greater emphasis on consequences—may come to dominate the analysis.[72] In light of recent events in Estonia, Georgia and Iran, it appears that time has come.

The Schmitt Analysis of Stuxnet also has implications for the broader debate over the use of force in cyberspace. For one thing, the lack of discussion over the legal implications of Stuxnet demonstrates that states are unlikely to reach consensus on what constitutes a cyber use of force any time soon. The lack of a discernable threshold also means that state sponsored grey area cyber attacks are more likely.[73] Consequently, policymakers, cyber practitioners and their legal advisors must be prepared to operate in an ambiguous and contested legal environment, while at the same time shaping new norms of acceptable state conduct.[74] In the end, these evolving norms are not likely to be constrained by Article 2(4)'s narrow prohibition on the use of force. Rather, they will likely reflect the new realities and unique features of cyberspace, such as cyber's potentially devastating consequences, the non-traditional distribution of cyber capabilities and vulnerabilities, and the international community's response (or lack thereof) to seminal events like Stuxnet.

[71] See, e.g., Waxman, "Cyber-Attacks and the Use of Force," 448-58; and Sharp, *Cyberspace and the Use of Force.*
[72] Schmitt, "Thoughts on a Normative Framework," 917.
[73] As representatives from NATO's Cooperative Cyber Defence Centre of Excellence have noted: "it is the general murkiness, the lack of clear policies and procedures, the lack of direct evidence of the attacking entity's identity that may make such attacks even more attractive. In such a volatile environment, by deliberately remaining below the threshold of use of force and at the same time using national policy cover as shield against investigations and prosecution, an attacking entity may believe there is less likelihood of reprisal even if the attacker's identity is suspected." CCDCOE, *International Cyber Incidents: Legal Implications*, 103.
[74] See Waxman, "Cyber Attacks and the Use of Force," 426; and Silver, "Computer Network Attack as a Use of Force," 75.

Appendix:
The "Schmitt Factors"[75]

(1) Severity: Consequences involving physical harm to individuals or property will alone amount to a use of force. Those generating only minor inconvenience or irritation will never do so. Between the extremes, the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force. In this regard, the scale, scope and duration of the consequences will have great bearing on the appraisal of their severity. Severity is self-evidently the most significant factor in the analysis.

(2) Immediacy: The sooner consequences manifest, the less opportunity States have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, States harbor a greater concern about immediate consequences than those which are delayed or build slowly over time.

(3) Directness: The greater the attenuation between the initial act and the resulting consequences, the less likely States will be to deem the actor responsible for violating the prohibition on the use of force. Whereas the immediacy factor focused on the temporal aspect of the consequences in question, directness examines the chain of causation. For instance, the eventual consequences of economic coercion (economic downturn) are determined by market forces, access to markets, and so forth. The causal connection between the initial acts and their effects tends to be indirect. In armed actions, by contrast, cause and effect are closely related—an explosion, for example, directly harms people or objects.

(4) Invasiveness: The more secure a targeted system, the greater the concern as to its penetration. By way of illustration, economic coercion may involve no intrusion at all (trade with the target state is simply cut off), whereas in combat the forces of one State cross into another in violation of its sovereignty. The former is undeniably not a use of force, whereas the latter always qualifies as such (absent legal justification, such as evacuation of nationals abroad during times of unrest). In the cyber context, this factor must be cautiously applied. In particular, cyber exploitation is a pervasive tool of modern espionage. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target-State's territory, as in the case of a warship or military aircraft which collects intelligence from within its territorial sea or airspace. Thus, actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force.

(5) Measurability: The more quantifiable and identifiable a set of consequences, the more a State's interest will be deemed to have been affected. On the one hand, international law does not view economic coercion as a use of force even though it may cause significant suffering. On the other, a military attack which causes only a limited degree of destruction clearly qualifies. It is difficult to identify or quantify the harm caused by the former (e.g., economic opportunity costs), while doing so is straightforward in the latter (x deaths, y buildings destroyed, etc).

[75] Schmitt, "Cyber Operations in International Law," 155-56.

(6) Presumptive legitimacy: [I]nternational law is generally prohibitory in nature. In other words, acts which are not forbidden are permitted; absent an express prohibition, an act is presumptively legitimate. For instance, it is well accepted that the international law governing the use of force does not prohibit propaganda, psychological warfare or espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate.

(7) Responsibility: The law of State responsibility … governs when a State will be responsible for cyber operations. But it must be understood that responsibility lies along a continuum from operations conducted by a State itself to those in which it is merely involved in some fashion. The closer the nexus between a State and the operations, the more likely other States will be to characterize them as uses of force, for the greater the risk posed to international stability.

Bibliography:

Air Force Operations & The Law: A Guide for Air, Space & Cyber Forces, 2d ed. The Judge Advocate General’s School. Maxwell AFB, AL, 2009.

Broad, William J., John Markoff and David E. Sanger. “Israeli Test on Worm Called Crucial in Iran Nuclear Delay.” New York Times, 15 January 2011.

Brown, Gary D. “Why Iran Didn’t Admit Stuxnet Was an Attack.” *Joint Forces Quarterly,* Issue 63 (4th Quarter 2011): 70-73.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What To Do About It*. New York, NY: Harper-Collins Publishers, 2010.

Duhaime.org Legal Dictionary, http://www.duhaime.org/LegalDictionary/O/OpinioJuris.aspx (accessed 12 December 2011).

Dunlap, Charles J., Jr. “Perspectives for Cyber Strategists on Law and Cyberwar.” *Strategic Studies Quarterly* (Spring 2011): 81-99.

Editorial. “Mike McConnell on how to win the cyber-war we're losing,.” *Washington Post*, 28February 2010. http://www.washingtonpost.com/wpdyn/content/article/2010/02/25/AR2010022502493.html?sid=ST2010031901063.

Falliere, Nicholas, Liam O Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Symantec, February 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Graham, David E. “Cyber Threats and the Law of War.” *Journal of International Law & Policy* 4 (2010): 87-102.

Hollis, Duncan B. “Why States Need an International Law for Information Operations.” *Lewis & Clark Law Review* 11 (2007): 1023-1061.

————. “New Tools, New Rules: International Law and Information Operations.” In *Ideas as Weapons: Influence and Perception in Modern Warfare*, edited by G.J. David Jr., and T.R. McKeldin III, 59-72. Dulles, VA: Potomac Books, Inc., 2009.

————. “An e-SOS for Cyberspace.” *Harvard International Law Journal* 52 (Summer 2011): 373-432.

————. “Could Deploying Stuxnet Be a War Crime?” *Opinio Juris* blog. 25 January 2011. http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/?utm_source=fe (accessed 1 December 2011).

Huntley, Todd C. “Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During A Time of Fundamental Change in the Nature of Warfare.” *The Naval Law Review* 60 (2010): 1-40.

International Committee of the Red Cross. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* 4 (2003). Available at: http://www.icrc.org/eng/assets/files/other/ihlcontemp_armedconflicts_final_ang.pdf.

Korns, Stephen W., and Joshua E. Kastenberg. “Georgia’s Cyber Left Hook.” *Parameters* (Winter 2008-09): 60-76.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Arlington, VA: RAND Corporation, 2009.

Lin, Herbert S. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law & Policy* 4 (2010): 63-86.

Milevski, Lukas. “Stuxnet and Strategy: A Special Operation in Cyberspace?” *Joint Forces Quarterly*, Issue 63 (4th Quarter 2011): 64-69.

Nakashima, Ellen. "Cyber-Intruder Sparks Massive Federal Response — and Debate Over Dealing With Threats." *Washington Post*, 9 December 2011. http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

National Research Council of the National Academy of Science. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, edited by William A. Owens, Kenneth W. Dam, and Herbert S. Lin. Washington DC: National Academies Press, 2009.

Nicaragua v. United States. 1986 International Court of Justice Reports 226 (27 June 1986).

Porche III, Isaac R., Jerry M. Sollinger, and Shawn McKay. *A Cyberworm that Knows no Boundaries*. Washington DC: RAND Occasional Paper, 2011. http://www.rand.org/pubs/occasional_papers/OP342.html (accessed on 15 January 2012).

Richardson, John.   *Stuxnet as Cyber Warfare: Applying the Law of War to the Virtual Battlefield.* Social Science Research Network Working Paper, 2011. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888 (accessed on 15 August 2011).

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* 37, 1999: 885-937.

————. "The Sixteenth Waldemar A. Solf Lecture in International Law." *Military Law Review* 176, 2003: 364-421.

————. "Responding to Transnational Terrorism Under the *Jus Ad Bellum*: A Normative Framework." *Naval Law Review* 56, 2008: 1-42.

————.   "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 151-178. Washington DC: National Academies Press, 2010.

Schneier, Bruce. "The Threat of Cyberwar Has Been Grossly Exaggerated." *Schneier.com*, 7 July 2010, http://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html (accessed on 6 December 2011).

Senate, *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the Senate Armed Services Committee*, 11th Cong., 11th sess., 15 April 2010. http://armed-services.senate.gov/statemnt/2010/ 04%20April/Alexander%2004-15-10.pdf (accessed 28 November 2011).

Sharp, Walter G. *Cyberspace and the Use of Force*. Falls Church, VA: Aegis Research Corp., 1999.

Silver, Daniel B. "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter." In *Naval War College International Law Studies, Vol. 76, Computer Network Attack and International Law,* edited by Michael N. Schmitt and Brian T. O'Donnell, 73-98. Newport, RI: 2002.

Singel, Ryan. "Is the Hacking Threat to National Security Overblown?" *Wired.com*, 3 June 2009. http://www.wired.com/threatlevel/2009/06/cyberthreat/ (accessed on 6 December 2011).

The White House. *National Security Strategy.* Washington DC, May 2010.

————. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington DC, May 2011.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Implications.* NATO Cooperative Cyber Defence Centre. Tallin, Estonia, 2010.

United Nations. *Charter of the United Nations and Statute of the International Court of Justice*. San Francisco, CA: 1945.

United Nations Security Council. *Resolution 1737*. U.N. Doc. S/1737. 5612th meeting (2006).

————. *Resolution 1747*. U.N. Doc. S/1747. 5647th meeting (2007).

————. *Resolution 1803*. U.N. Doc. S/1803. 5848th meeting (2008).

————. *Resolution 1929*. U.N. Doc. S/1929. 6335th meeting (2010).

US Army War College. *Information Operations Primer*. Carlisle Barracks, PA (November 2011).

US Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington DC, July 2011.

————. *An Assessment of International Legal Issues in Information Operations*. Washington DC: Office of General Counsel, May 1999.

Waxman, Mathew C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *The Yale Journal of International Law* 36, 2011: 421-459.

Wingfield, Thomas C. *The Law of Information Conflict: National Security Law in Cyberspace*. Falls Church, VA: Aegis Research Corp., 2000.

————. "When is a Cyber Attack an 'Armed Attack?' Legal Thresholds for Distinguishing Military Activities in Cyberspace." Cyber Conflict Studies Association, 1 February 2006. Available at: http://www.docstoc.com/docs/445063/when-is-a-cyberconflict-an-armed-conflict.

————. "International Law and Information Operations." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 525-542. Washington DC: National Defense University Press, 2009.

Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired.com*, 11 July 2011. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/ (accessed 27 October 2011).