Lieutenant Colonel Andrew C. Foltz, USAF, wrote this essay while a student at the Air War College. It won the Strategic Research Paper category of the 2012 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

One of the many seemingly intractable legal issues surrounding cyberspace involves whether and when peacetime cyber operations constitute a prohibited use of force under Article 2(4) of the United Nations (UN) Charter. 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. 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.

As discussed in this article, several analytic frameworks have been developed to help assess when cyber operations constitute a use of force. One conclusion these frameworks share is that cyber operations resulting in physical damage or injury will almost always be regarded as a use of force. Beginning with the Stuxnet and Schmitt Analysis, the Cyber “Use-of-Force” Debate

By ANDREW C. FOLTZ

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

Members of International Telecommunications Union and UN Institute for Training and Research confer on cyber security

Stuxnet, Schmitt Analysis, and the Cyber “Use-of-Force” Debate

Lieutenant Colonel Andrew C. Foltz, USAF, wrote this essay while a student at the Air War College. It won the Strategic Research Paper category of the 2012 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.
### Report Documentation Page

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

<table>
<thead>
<tr>
<th>1. REPORT DATE</th>
<th>2. REPORT TYPE</th>
<th>3. DATES COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td></td>
<td>00-00-2012 to 00-00-2012</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5a. CONTRACT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5b. GRANT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5c. PROGRAM ELEMENT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5d. PROJECT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5e. TASK NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5f. WORK UNIT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Defense University, Joint Force Quarterly, 260 Fifth Avenue (Building 64, Room 2504) Fort Lesley J. McNair, Washington, DC, 20319</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10. SPONSOR/MONITOR’S ACRONYM(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>11. SPONSOR/MONITOR’S REPORT NUMBER(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12. DISTRIBUTION/AVAILABILITY STATEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release; distribution unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13. SUPPLEMENTARY NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14. ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>15. SUBJECT TERMS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16. SECURITY CLASSIFICATION OF:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. REPORT unclassified</td>
</tr>
<tr>
<td>b. ABSTRACT unclassified</td>
</tr>
<tr>
<td>c. THIS PAGE unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>17. LIMITATION OF ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same as Report (SAR)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>18. NUMBER OF PAGES</th>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
in 2007, however, a string of cyber operations—including the 2007 Distributed Denial of Service (DDoS) attack on Estonia, the 2008 DDoS attack on 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. 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.5 Perhaps this is because it caused physical damage and, therefore, clearly constitutes a use of force under prevailing analytic frameworks. This appears to be the emerging consensus.6 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 article tests one of the more robust frameworks, known as the Schmitt Analysis, by applying it to Stuxnet. Developed in 1999 by Professor Michael Schmitt, it is one of the most academically rigorous and frequently cited frameworks for characterizing cyber operations. The Schmitt Analysis consists of seven factors that states are likely to consider when characterizing cyber activities: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility. A key feature of the framework is that it remains faithful to Article 2(4) of the UN Charter while at the same time effectively bridging key elements of competing analytic frameworks that do not exhibit such fidelity to the Charter. By focusing this evaluation on Schmitt’s model, I expect the results will have implications for the use-of-force debate more generally.

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

**Why the Use-of-Force Threshold Matters**

Cyberspace represents a strategic vulnerability for many states because it is inextricably tied in to 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.7 Even the most secure U.S. defense networks are not immune.8 The scope of the problem has become so great that some claim the United States is engaged in a cyber war, and that it is losing.9 The National Security Strategy of 2010 notes that “cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation.”10 The White House’s International Strategy for Cyberspace of 2011 goes further by proclaiming: “When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country,” to include a military response.11

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 determining which legal regime governs state behavior.12 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, non-state-sponsored cyber operations and operations not amounting to a use of force are traditionally governed by more constrained law enforcement regimes.13

The need for clarity has taken on greater importance now that the United States and many of its allies treat cyberspace as a military operational domain.14 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 UN Security Council authorization is required to conduct certain operations.

**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, nor does it appear a mechanical rule is likely to emerge any time soon.15 This section describes why 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.

**Use of Force Under the UN Charter.** Jus ad bellum16 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 UN Charter, which prohibits states from the “threat or use of force” in their international relations. 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 nonstate 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 provide 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 relations between states and employs thresholds quite distinct from the use-of-force standard. 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.

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. First, the framers of the

Charter took an instrument-based, vice consequence-based, approach to the use of force prohibition. While acknowledging that states are most concerned about the consequences of coercive activities (that is, the degree of injury, deprivation, or destruction), the framers recognized that a consequence-based criterion was too subjective to distinguish lawful from unlawful state coercion. 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 shorthand. 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.” According to this approach, the Article 2(4) prohibition does not extend to all forms of state coercion. For example, the instruments of economic and political coercion are not prohibited. Less clear, but generally accepted, is that the prohibition is not limited to “armed” force—it may also encompass unarmed, nonmilitary physical force, such as releasing water from a dam. The International Court of Justice highlighted this point in Nicaragua v. United States (hereinafter Nicaragua), when it concluded that arming and training guerrillas amounted to a prohibited use of force, even though it did not rise to the level of an armed attack. 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. As discussed below, discerning a clear use-of-force threshold in this gray area—a difficult task even in traditional kinetic context—has proven particularly difficult in the cyber context.

Use of Force in Cyberspace. The difficulty of applying Article 2(4) in cyberspace is that the instrument-based paradigm does not cleanly translate to cyber operations, particularly for gray area operations that do not result in physical harm. 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. 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, these commentators call Article 2(4)’s instrument-based paradigm into question.

The perceived shortcomings of Article 2(4) have led many to propose a new treaty law to govern cyber operations. 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 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.

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. The advantage of this approach—which is generally favored by U.S. policymakers and military operators—is that it is fairly simple to apply and it acknowledges that states are principally concerned about consequences. 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 attack. This framework generally adheres to the Charter’s instrument-based approach, but it struggles to characterize hostile gray 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 target 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. This framework suffers from the inherent subjectivity of defining what constitutes “critical infrastructure and vital interests,” and because it expands the gray area to encompass activities such as computer network exploitation that are not currently prohibited by international law. Professor Schmitt’s framework represents the fourth major model.

Schmitt Analysis

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

- **Severity**: Cyber operations that threaten physical harm more closely approximate an armed attack. Relevant factors in the analysis include scope, duration, and intensity.
- **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.
- **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.
- **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.
- **Measurability**: States are more likely to view a cyber operation as a use of force if the consequences are easily identifiable and objectively quantifiable.
- **Presumptive legitimacy**: To the extent certain activities are legitimate outside of the cyber context, they remain so in the cyber domain, for example, espionage, psychological operations, and propaganda.
- **Responsibility**: The closer the nexus between the cyber operation and a state, the more likely it will be characterized as a use of force.35

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—that is, 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.36 Finally, the framework is more useful for post hoc forensic analysis of particular cyber attacks than for characterizing real-time operations.37

Professor Schmitt also acknowledged that his adherence to the Article 2(4) 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.38 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.”39 In the end, the Schmitt Analysis has generally stood the test of time and remains one of the most commonly referenced frameworks for characterizing the use of force in cyberspace.

**Characterizing Stuxnet**

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.40 According to analysts attending Defense Cyber Investigations Training
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.

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. First, Stuxnet’s designers required incredibly precise intelligence about Iran’s PLCs and frequency converters, as well as the performance parameters of its centrifuges. 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 signatures to gain access to targeted systems. Finally, Stuxnet appears to have been designed to avoid collateral damage. 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 percent of the infections were localized to Iran, and there are no reports of physical damage outside of Iran. Although no one has claimed responsibility for Stuxnet, it has the signature of a state operation. Most speculation and some anecdotal evidence points to Israel, with possible support from the United States and/or Germany.

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 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—it’s nuclear program. By setting Iran’s nuclear program back several years, the duration of Stuxnet’s consequences also supports characterizing it as a use of force—though this delay is due to 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 and 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. 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 does it appear to have crossed 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 interna-
tional community would likely not regard as a use of force.

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

**Presumptive legitimacy**: Stuxnet does not enjoy presumptive legitimacy. Short of UN 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 UN Security Council Resolutions. 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 strongly suggest state involvement. That said, it is possible that Stuxnet was created and launched by nonstate actors—such as Iranian dissidents working with freelance hackers—in which case it would not be subject to international laws governing the use of force.

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 probably involved state support.

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—that is, discerning the use of force threshold entails predicting how states will characterize cyber operations. That said, the analysis reveals several limitations with the framework, as well as opportunities for its expansion.

First, it appears that in any given Schmitt Analysis, the characterization of a cyber operation may be derived from 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 the Article 2(4) instrument-based paradigm. To illustrate the point, what if instead of damaging Iranian 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.”

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 that 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. Thus, the responsible state apparently regarded Stuxnet as the equivalent of an armed attack and executed the operation as such. Since an armed attack constitutes a use of force, the implication is that states are more likely to characterize cyber attacks as a use of force if they appear to comply with LOAC—even in gray area operations that do not result in actual damage.

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 responsible party must be identified as a state. 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. In other words, without attribution, a Schmitt Analysis offers limited practical value. But if state attribution can be established, it is questionable whether a Schmitt Analysis would be necessary because more revealing 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 International Court of Justice 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.” Although Iran has acknowledged the presence of Stuxnet in its systems, it has denied any significant damage and has never claimed that it was subject to an armed attack. 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 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.” 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 Professor Schmitt’s premise 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.” This is due, in part, to the difficulty of 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 UN Charter. Whereas contemporary interpretations of Article 2(4) reflect the distribution of traditional instruments of power—that is, political, military, and economic strength—the current array of cyber capabilities and vulnerabilities does not mirror the traditional distribution. Consequently, states with significant cyber capabilities or vulnerabilities—regardless of their political, military, or economic strength—are likely to consider factors well beyond Article 2(4) when characterizing the legality of cyber operations. Such additional considerations may 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 organizations; domestic politics; state declaratory policies; emerging state practice (including state inaction); attribution problems; and other legal, political, and technical constraints. Moreover, given the novelty of cyberspace, 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. Even though most states would probably agree that Stuxnet constituted a use of force under Article 2(4), they may be reluctant to agree that Stuxnet constituted a use of force any time soon. The lack of a discernable threshold also suggests that state-sponsored gray area cyber attacks are more likely. Consequently, policymak-

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 vigilante-ism, 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**

Although Professor Schmitt’s analytic approach to characterizing cyber operations remains sound, the analysis of Stuxnet reveals several shortcomings with his model. These include 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” toward a particular cyber operation. This analysis also reveals at least one additional factor states may consider when characterizing cyber operations—whether an attack appears to comply with LOAC.

More importantly, this analysis suggests the time has come to relax the model’s strict adherence to the Article 2(4) instrument-based paradigm. By tying his framework to Article 2(4), Professor Schmitt 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. 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.

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 suggests that state-sponsored gray area cyber attacks are more likely. Consequently, policymak-

**policymakers and cyber practitioners must be prepared to operate in an ambiguous and contested legal environment**

ers and 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. 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 nontraditional distribution of cyber capabilities and vulnerabilities, and the international community’s response (or lack thereof) to seminal events like Stuxnet.

**NOTES**


13 Dunlap, 84.


15 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) as just one of several factors to consider when characterizing cyber operations.
is used to judge whether State practice and adher-
legal obligation. In the international law context, it
is a software vulnerability
caused by adversaries. See also Schmitt, “Cyber
Network Attack and the Use of Force,” 2011; and
Hollis, “Why States Need an International Law for
Information Operations,” 1041.

25 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.
26 Schmitt, “Cyber Operations in International
Law,” 155.
27 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
28 Hollis, “Why States Need an International Law
for Information Operations,” 1040.

29 Ibid., 1041. Professor Schmitt highlighted this
dilemma: “The advent of cyber operations throw
the instrument-based approach into disarray
by creating the possibility of dramatically destabilizing effects caused by other than kinetic
actions.” Schmitt, “Cyber Operations in Interna-
tional Law,” 177.
States Need an International Law for Information
Operations,” 1053; and Silver, 78.
31 Sharp, 129–131; and Hollis, “Why States
Need an International Law for Information Opera-
tions,” 1041.

32 Schmitt, interview with 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.
33 Schmitt, “Computer Network Attack and the
Use of Force,” 914.

34 Schmitt’s responsibility factor is best
understood as a measure of the degree of state
attributes. Although in some cases it does not describe as such.
35 Professor Schmitt’s responsibility factor is best
understood as a measure of the degree of state
attributes, although in some cases it does not describe as such.
36 Schmitt, interview with author. See also,
Michael N. Schmitt, “The Sixteenth Waldemar A.
Solf Lecture in International Law,” Military Law
37 Schmitt, interview with author.
38 Schmitt, “Computer Network Attack and the
Use of Force,” 917.

39 See, for example, Lukas Milevski, “Stuxnet
and Strategy: A Special Operation in Cyberspace?”
Joint Force Quarterly 63 (4th Quarter 2011), 64; and
Porche, Sollinger, and McKay, 1.
40 See Kim Zetter, “How Digital Detectives
Deciphered Stuxnet, the Most Malevolent Malware
in History,” Wired.com, July 11, 2011; Porche,
Sollinger, and McKay; Nicolas Falliere, Liam O
Murchu, and Eric Chien, W32.Stuxnet Dossier
(Symantec, February 2011); and Hollis, “Could
Deploying Stuxnet Be a War Crime?”
41 Milevski, “Stuxnet and Strategy,” 66 citing
James P. Farwell and Rafał Rohożynski, “Stuxnet
and the Future of Cyber War,” Survival 53, no. 1
[January 2011], 24.

42 According to reports, representatives from
the International Atomic Energy Agency who had
inspected Natanz did not even have this level of
information. Ibid., 65.
43 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.
44 Richardson, 7.