
PRIYANKA R. DEV*

SUMMARY

INTRODUCTION ............................................................................................................... 380

I. CURRENT SOURCES OF LAW AND AUTHORITY ON CYBER LAW OF ARMED CONFLICT .............................................................. 382

II. BACKGROUND PRINCIPLES FROM KINETIC LAW OF ARMED CONFLICT THRESHOLDS .......................................................................................... 384

III. THEORIES ON WHAT CONSTITUTES A CYBER “USE OF FORCE” .......... 386
    A. Expanding the Existing Article 2(4) Definition of “Use of Force” .......... 386
    B. Creating a New Threshold Below “Use of Force” ................................... 390

IV. THEORIES ON WHAT CONSTITUTES A CYBER “ARMED ATTACK” .......... 393

V. THE NEED FOR MORE DEFINED LAWFULNESS THRESHOLDS: LESSONS FROM STUXNET ................................................................. 395

CONCLUSION ................................................................................................................... 398

* Priyanka R. Dev is a Candidate for the degree of Juris Doctor in 2015 at the University of Texas School of Law and the Director of Development of the TEXAS INTERNATIONAL LAW JOURNAL.
INTRODUCTION

There is little disagreement that computer technology has dramatically altered the nature of international conflict. Today, governments can utilize social media to topple regimes, use silent signals instead of people to commit espionage, and wage wars with the simple click of a button. And no State, corporation, or other organization—despite its resources or its military reputation—is immune from the threat of another. In early 2012, the websites of several big U.S. banking institutions fell prey to cyber intrusion when Iranian hackers launched a series of distributed denial of service (DDoS) attacks and captured computer clouds at data centers around the world, turning them into networks of slave computers, or botnets, positioned to flood and interrupt cyber traffic to and from the banking websites. After the attacks, the Iranian group that took credit for them warned the world through online postings: “From now on, none of the U.S. banks will be safe from our attacks.” In light of incidents like this, U.S. defense officials view cyber attacks to be the “single greatest threat” to U.S. national security.

As the dangers of cyber actions evolve in the wake of technological developments, so too should the way States and organizations apply traditional law of armed conflict (LOAC) principles to cyber actions. Traditional kinetic LOAC principles simply do not fit this new wave of warfare. The limitations of applying traditional LOAC to cyber acts have left nation States misguided and confused, forcing them to rely on subjective views of what is lawful rather than apply an objective, internationally-accepted assessment of lawfulness before implementing a cyber act. In the absence of formal guidance from the United Nations, the organization that typically formalizes LOAC rules into transnational binding treaties, scholars have offered informal rules of cyber conduct in the form of the

2. See James E. McGhee, Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy, 2 J.L. & CYBER WARFARE 64, 64 (2013) ("[F]ocused cyber threats have resulted in exposed intellectual property, research and development, military plans, proprietary information and extortion.").
3. Bradley Raboin, Corresponding Evolution: International Law and the Emergence of Cyber Warfare, 31 J. NAT’L ASS’N ADMIN. L. JUDICIARY 602, 603 (2011) ("Now, with merely a computer and an Internet connection, an entire nation’s infrastructure, both military and civilian, may be critically affected.").
5. QassamCyberFighters, Phase/2,w/4; Operation Ababil, PASTEBIN (Jan. 1 2013), pastebin.com/dwu47giH.
7. See Michael N. Schmitt, Cyber Operations and the Jus Ad Bellum Revisited, 56 VILL. L. REV. 569, 571 (2011) [hereinafter Schmitt, Cyber Operations] ("[T]he existing legal norms do not offer a clear and comprehensive framework within which states can shape policy responses to the threat of hostile cyber operations . . . . [T]ernational law as traditionally understood departs at times from what the international community would presumably demand in the cyber context.").
Texas International Law Journal Volume 50, Issue 2

“USE OF FORCE” AND “ARMED ATTACK” IN CYBER CONFLICT

Tallinn Manual—but their response lacks the enforceability mechanisms that boost the legitimacy of and reciprocity for LOAC. While most States nonetheless urge support for the black letter rules in the Tallinn Manual, at least one—namely, Russia—rejects the Tallinn Manual based on its view that traditional LOAC is ill-fitted to deal with cyber conduct and awaits a more formal international response. Whether or not one believes that traditional LOAC can be appropriately applied to the cyber warfare realm, most everyone agrees that an official U.N. Treaty approach—if it comes at all—could take years.

Given this state of limbo, this paper synthesizes and assesses the various ways in which the traditional combat thresholds of a U.N. Article 2(4) “use of force” and an Article 51 “armed attack” have been applied to cyber conduct, ultimately highlighting the problems that arise from literally extending these established Charter principles to cyber acts. Part I introduces the existing sources of law around this issue but reveals the gaping hole that the United Nations has left with regard to cyber rules. Part II discusses, in detail, what amounts to an Article 2(4) use of force in the cyber context and, in light of the difficulties that arise from literally extending the term, suggests a new approach that better accounts for cyber damages. Part III discusses how scholars have defined an armed attack in the cyber context, pointing out the great problems of the existing ambiguity about when a state can legitimately respond in self-defense under Article 51. Part IV finally applies these working definitions as well as my proposed suggestions to a recent potentially unlawful cyber action. In exploring what types of actions currently do and, in the future, should trigger these important LOAC thresholds, this paper aims to bring some clarity to an area of cyber conflict law that even pioneering cyber conflict experts admit is filled with impractical, ill-defined principle thresholds.

9. See generally TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

10. See Elena Chernenko, Russia Warns Against NATO Document Legitimizing Cyberwars, RUS. BEYOND THE HEADLINES (May 29, 2013), http://rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html (concluding that, based on statements by Russian Defense Ministry leaders, Russian authorities have taken a “guarded view” of the Tallinn Manual in part because they think its publication legitimizes the concept of cyberwars).

11. See id. (explaining that an agreement between the United States and Russia on cyberwar policy is unlikely to occur anytime soon); cf. Derek Jinks, Remarks at Texas International Law Journal Symposium Intangible Weaponry & Invisible Enemies: Applying International Law to Cyber Warfare, (Mar. 7, 2014), available at https://www.youtube.com/watch?v=bgM3EIYIYos (commenting that the secretiveness of States is one insurmountable problem preventing the international community from adopting a treaty resolving the rules governing cyberwarfare).

12. See Schmitt, Cyber Operations, supra note 7, at 571 (“Unfortunately, the existing legal norms do not offer a clear and comprehensive framework within which states can shape policy responses to the threat of hostile cyber operations.”); TALLINN MANUAL intro. (“[T]he scope and manner of international law’s applicability to cyber operations, whether in offence or defence, has remained unsettled since their advent.”).
I. CURRENT SOURCES OF LAW AND AUTHORITY ON CYBER LAW OF ARMED CONFLICT

While the United Nation’s response to cyber conflict and its dealing with the gaping hole in cyber LOAC has been nearly negligible, there do exist several sources of authority, including the Tallinn Manual, individual nation state policy, and scholarly frameworks, which can help governments navigate their cyber conduct.

The authority that comes closest to an international response is the Tallinn Manual on the International Law Applicable to Cyber Warfare. The Tallinn Manual, published in 2013 by a group of twenty renowned Western law scholars and practitioners (referred to as “The International Group of Experts”), contains ninety-five black letter rules about how States are to operate in a cyber warfare context; the actual rules reflect the consensus on current customary international law as agreed upon by a majority of the scholars after consultation with treaty law, national military manuals, and studies by international humanitarian law agencies—to name a few of the sources. The comment sections that follow each rule also contain minority viewpoints that were not integrated into the main rule. Three organizations—the International Committee of the Red Cross (ICRC), the North Atlantic Treaty Organization (NATO), and United States Cyber Command—stood in as “observers” to the project, which suggests that the project had a greater international voice than it actually did; but the rules do not necessarily reflect the positions of these internationally acclaimed organizations. Moreover, while the Tallinn Manual seems generally well received, the International Group of Experts did not include representatives from many of the countries that one might expect or wish to be included in a treatise on cyber warfare given their cyber capabilities, including Russia, China, and other eastern States. And while the writers have already received criticism regarding this lack of diversity, they did note that the

13. See TALLINN MANUAL intro. (explaining that “[t]here are no Treaty provisions that directly deal with ‘cyber warfare’.”).
15. See generally TALLINN MANUAL.
16. Id. intro.
17. Id.
18. Id.
19. Id.
21. The International Group of Experts did not include representatives from states located east of the former Iron Curtain. TALLINN MANUAL intro. Int’l Grp. of Experts (listing experts from institutions in the United States, the United Kingdom, Germany, Belgium, Canada, Australia, the Netherlands, Sweden, and Switzerland). The Tallinn Manual scholars respond to this criticism openly and honestly. They respond that the substantive differences regarding this interpretation of international law between the Western and Eastern worlds are not at all significant; because of this, the Eastern lack of representation on the committee does not affect the substance of the Tallinn Manual. Michael Schmitt, Remarks at Intangible Weaponry & Invisible Enemies: Applying International Law to Cyber Warfare, Texas International Law Journal Symposium (Mar. 6 2014), available at https://www.youtube.com/watch?v=MsqSLLPhtwo [hereinafter Schmitt, Remarks at Texas International Law Journal Symposium].
The Tallinn Manual was a work in progress and that, over time, state practice may alter the rules and norms articulated.\textsuperscript{23} The writers even started a second edition not long after the first was published; unfortunately, it does not appear that any Eastern scholars are involved in the forthcoming set of revisions either.\textsuperscript{24} The biggest limitation of the Tallinn Manual, despite its extremely comprehensive approach to defining a set of cyber LOAC, is that, as a scholarly project, it derives authority solely from academia rather than the sovereign authorities that have in the past served as a means of legitimating and enforcing LOAC principles.\textsuperscript{25} The Tallinn Manual, therefore, despite its honorable contributions and its potential to lay the groundwork for a more formal U.N. Treaty, merely offers States persuasive secondary authority.\textsuperscript{26}

Many States have unsurprisingly developed internal policies for cyber operations to help determine when another government’s cyber actions have crossed a threshold of unlawfulness and, perhaps more importantly, when a lawful response to foreign state action is justified.\textsuperscript{27} The United States, for instance, draws operational guidance from internal policy guidelines set by the executive branch.\textsuperscript{28} Admittedly, analyzing individual state perspectives rather than a truly international response as to what types of cyber conduct constitute uses of force or armed attacks is inherently unhelpful in establishing an objective, worldwide threshold.\textsuperscript{29} However,
these internal policies still serve as important sources of law for individual state policy and may help guide any future U.N. or international response.

Even scholarly work by cyber experts, though it lacks any mechanism for enforcement, is important to consider as a source of guiding law around cyber actions; it could also serve States and ultimately the United Nations with innovative solutions for assessing cyber acts. In a field that is constantly evolving, scholarly work on cyber conduct can provide a platform of ideas, conceptualizations, and innovative guidance for States to draw from before integrating certain standards into policy. While much of the scholarship on cyber uses of force and armed attacks was properly incorporated into and thereby supplanted by the Tallinn Manual, it is nonetheless important to note that there are still new ideas emerging from scholarly work that should be integrated into whatever final approach is ultimately taken by the United Nations or another binding authority.

II. BACKGROUND PRINCIPLES FROM KINETIC LAW OF ARMED CONFLICT THRESHOLDS

First, it is essential to discern what the terms “use of force” and “armed attack” traditionally entail and, perhaps most importantly, to distinguish between the two. The use of force threshold draws meaning from Article 2(4) of the U.N. Charter, which states the following: “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) therefore recognizes that the principle of national sovereignty underscores all our LOAC rules; out of this language, it has become generally accepted that it is when a State’s conduct rises to the threshold of a use of force that LOAC is triggered. Traditionally, an unlawful use of force justifies some countermeasures, such as economic sanctions or U.N. intervention, but it does not

30. See generally, e.g., Schmitt, Cyber Operations, supra note 7.
31. For example, Michael N. Schmitt’s seven-factor approach to determining whether an act was an Article 2(4) use of force, originally articulated in an article for The Columbia Journal of Transnational Law, was integrated into the Tallinn Manual at Comment 9 to Rule 11. Tallinn Manual r. 11 cmt. 9 (citing Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Colum. J. Transnat’l L. 885, 914 (1999)).
32. Some contend that the concepts of “use of force” and “armed attack” are essentially indistinguishable. See Tallinn Manual r. 11 cmt. 7 (acknowledging the view contrary to the Tallinn Manual’s rules that “the distinction between the two concepts is either so narrow as to be insignificant or non-existent,” and as a result, “any illegal use of force can qualify as an armed attack”). But, for purposes here, the two concepts will be referred to separately and refer to two different thresholds of activity, as is in line with current customary international law. Id.
34. See M.P. Ferreira-Snyman, The Evolution of State Sovereignty: A Historical Overview, 12 Fundamina 1, 24 (2006) (“[T]he ban on the use of force by the Charter is today understood not so much as a limitation of sovereignty, but as a necessary prerequisite for a de facto enjoyment of sovereign equality by states. Therefore, a state’s sovereign equality depends on a comprehensive prohibition of the use of force and an effective mechanism to implement and enforce this prohibition.”)
35. See Michael N. Schmitt, “Attack” as a Term of Art in International Law: The Cyber Operations Context, in 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283, 286 (C. Csosseck et al. eds., 2012) [hereinafter Schmitt, “Attack” as a Term of Art] (“[A]n ‘armed attack’ is an action that gives States the right to a response rising to the level of a ‘use of force,’ as that term is understood in the jus ad bellum.”).
justify a typical counterattack, even if it is in proportion to the initial use of force.\textsuperscript{36} It is also generally accepted that not all types of pressure, including political or economic, are sufficient to amount to unlawful Article 2(4) uses of force.\textsuperscript{37}

The perpetration of an armed attack provides States with a different legal threshold\textsuperscript{38} and draws its significance from U.N. Charter Article 51. Article 51 provides the following: “Nothing in the . . . Charter shall impair the inherent right of individual or collective self-defence if an \textit{armed attack} occurs against a Member of the United Nations . . . .”\textsuperscript{39} Under this provision, then, a state can lawfully and proportionately respond to an act that meets the threshold of unlawfulness of an armed attack.\textsuperscript{40} Under traditional LOAC, therefore, when State A commits an armed attack against State B, State B can lawfully respond \textit{proportionately} to State A’s act.\textsuperscript{41} Because an armed attack invokes a right to respond in a manner that could cause more harm in addition to that of the initial attack, it is generally accepted that an armed attack entails a higher threshold of unlawfulness than that of an Article 2(4) use of force, to which a state is not granted the right to lawfully respond through similar proportionate means.\textsuperscript{42} An armed attack also typically requires some sort of physical damage to persons or property in order to qualify as such.\textsuperscript{43}

There is general agreement that the U.N. Charter, even though it was conceived around kinetic principles, also applies to cyber conduct.\textsuperscript{44} Customary law, guided by the \textit{Nuclear Weapons Advisory Opinion} issued by the International Court of Justice (ICJ), demonstrates that Article 2(4) applies to “any use of force, regardless of the weapons employed.”\textsuperscript{45} It is likewise difficult to find scholarship that suggests that Article 51 armed attacks are not relevant in the cyber context.\textsuperscript{46} So, while it is fairly evident that the international community agrees that these concepts apply to and therefore place limits on a State’s right to act against another State through cyber means, there is still much ambiguity in the discussions about \textit{how} these concepts apply.

\begin{itemize}
\item \textsuperscript{36} \textit{Tallinn Manual} r. 9.
\item \textsuperscript{37} \textit{Id.} r. 11 cmt. 2.
\item \textsuperscript{38} Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 210 (June 27) (noting that there are “measures which do not constitute an armed attack but may nevertheless involve a use of force”).
\item \textsuperscript{39} U.N. Charter art. 51 (emphasis added).
\item \textsuperscript{40} See Schmitt, “\textit{Attack} as a Term of Art, supra” note 35, at 286 (stating that defensive force may be used in response to an armed attack when non-forceful means are likely to prove inefficient and when such defensive force is proportional to the attack incurred).
\item \textsuperscript{41} \textit{Id.}
\item \textsuperscript{42} \textit{Id.} at 285.
\item \textsuperscript{43} \textit{Tallinn Manual} r. 13 cmt. 9.
\item \textsuperscript{44} See, \textit{e.g.}, MARCO ROSCINI, \textit{CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW} 115 (2014) (stating that cyber attacks are “prohibited by Article 2(4) of the UN Charter”).
\item \textsuperscript{45} Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, para. 39 (July 8).
\item \textsuperscript{46} \textit{Cf.} Schmitt, \textit{Cyber Operations, supra} note 7, at 571, 589 (noting that the May 2010 U.S. National Security strategy considers cyber threats the most serious national challenge and arguing that cyber operations with sufficient consequence are armed attacks).
\end{itemize}
III. THEORIES ON WHAT CONSTITUTES A CYBER “USE OF FORCE”

The gamut of theories about how States should determine if a particular act qualifies as a use of force, though diverse, does not yet account for the crucial need to expand the analysis from a physical results-based approach to a more encompassing one that takes into account non-physical damage. Given that relatively few cyber acts result in the type of physical harm or damage that States traditionally accept as unlawful, States will ultimately be forced to adopt one of two solutions in order to proportionately apply the use of force threshold to cyber attacks: (A) expand the definition of an Article 2(4) use of force to account for the types of damages, like financial ones, that cannot be physically discerned and traditionally do not make an act more likely to be a use of force; or (B) create a new legal threshold below use of force that justifies a state response to a cyber act that is an invasion on national sovereignty but does not meet the threshold of a traditional Article 2(4) violation. I discuss these solutions in turn below.

A. Expanding the Existing Article 2(4) Definition of “Use of Force”

In order to best account for the full scope of potential damages but still recognize only the traditional Article 2(4) thresholds, States would have to broaden the accepted definition of an Article 2(4) use of force. Looking solely at an act’s physical effects to determinate if a cyber act qualifies as a use of force might be common sense, but this approach does not properly respond to the reality that there are non-physical effects of cyber attacks that are equally harmful to State sovereignty. What I coin the “common-sense approach” was best summarized by former U.S. State Department Legal Advisor Harold Koh, who suggested that if the effects of an action under kinetic law would constitute use of force, then the cyber equivalent is also a use of force. Koh’s explanation, however, does not seem to provide for the possibility that there are acts whose effects under kinetic law would not result in a use of force, but their cyber equivalents would meet the threshold. Koh’s explanation only makes clear that a cyber act which results in injury or death to persons or damage or destruction to objects is, by established definitions, an Article 2(4) use of force. Customary international law seems to be in consensus with the common-sense approach but similarly is unclear as to whether physical damage is required. The Tallinn Manual suggests that the writers saw this issue as a source of deep

48. See Koh, supra note 28 (stating that jus ad bellum rules to apply to uses of force in cyberspace and noting instances where the physical effects of cyber acts are comparable to physical kinetic acts).
49. Koh explained the common-sense approach with this simple example: If a line of malicious code from a distant computer somehow broke a dam and flooded a civilian population, it would constitute a use of force because the kinetic equivalent of a bomb exploding and leading to similar damage would also reach the threshold. Id.
50. Id.
51. See TALLINN MANUAL r. 11 (explaining that the scale and effects approach is used to determine whether there was a use of force).
contention.52 The comments to the Tallinn Manual indicate that its writers believed certain cyber acts that would not ordinarily result in the type of purely physical damage required under kinetic law should nonetheless constitute uses of force, in part because of the special nature of potential destruction through computers.53 Yet, as the writers often realized, lex lata, or the law as it stood at the time of their drafting the rules, did not allow for them to incorporate this understanding of use of force into the black letter law; instead, they were locked in to traditional definitions.54 Other scholars have commended the Tallinn Manual editors for synthesizing customary international law on this topic but also criticized—and I think properly so—the editors’ very limited definition of an Article 2(4) use of force.55

Ignoring non-physical damages in analyzing whether an act is an Article 2(4) use of force would be a great disservice to the unfortunate realities of cyber warfare; if the international community chooses to simply extend existing use of force definitions to cyber activity, it must adopt a broader conception of what damages to analyze. This common-sense approach does not consider the detrimental extent of non-physical damage that can result from cyber acts.56 For instance, under the common-sense approach, a cyber infiltration of State A by State B that resulted in total paralysis of State A’s stock market but no direct physical damage would not constitute a use of force; yet, a bomb attack in one tiny town in State A would not only qualify as a use of force, but perhaps also rise to the level of an Article 51 armed attack.57 The Tallinn Manual definition similarly legitimizes a strange policy: If State A, through some sort of cyber act, prevented fuel from being delivered to an airplane, which was necessary for State B to carry out a planned, pre-determined kinetic attack, the cyber act would still not constitute a use of force. Under

---

52. Even the Tallinn Manual editors could not agree on a definitive view. See id. intro. (“[T]he lack of agreed-upon definitions, criteria, and thresholds for application[] creates uncertainty when applying the jus ad bellum to the rapidly changing realities of cyber operations.”).

53. See id. r. 10–11 & cmts. (elaborating on the ways that cyber operations are similar and different from traditional uses of force).

54. See id. intro. (noting that the experts were bound to write the rules in line with lex lata rather than preferred policy, or lex ferenda). Tallinn Manual Rule 10 provides the following: “A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.” Id. r. 10. Rule 11 then goes on to define use of force, but this definition is reminiscent of the overly simplified analog that the U.S. State Department provided: “A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.” Id. r. 11; cf. Koh, supra note 28 (suggesting that a cyber action constitutes a use of force if the effects of an equivalent kinetic action would constitute a use of force).

55. See, e.g., McGhee, supra note 2, at 84 (“[The Tallinn Manual] spells out, with great particularity, its application and non-application to certain areas of law and conflict. Of note, the Group limits their discussion to use of force and armed conflict . . . . This ignores the overlap and fusion of electronic warfare and cyber warfare capabilities, an issue of great interest within the military Services.”).

56. For instance, cyber campaigns can disrupt services to a State by targeting key infrastructure, causing devastating economic effects. See, e.g., JAMES A. LEWIS, CTR. FOR STRATEGIC & INT’L STUDIES, THRESHOLDS FOR CYBERWAR 2 (Sept. 2010), available at http://csis.org/files/publication/101001_ieee_insert.pdf.

57. See Jay P. Kesan & Carol M. Hayes, Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace, 25 HARV. J.L. & TECH. 415, 516–17 (2012) (discussing that whether or not a cyber attack rises to the threshold of a use of force may depend upon whether one analyzes the attack in terms of its economic effects or by measuring whether the damage caused could have been created by a kinetic attack).
traditional LOAC definitions, the purely economic consequences of a cyber event escape consideration even though they could be as harmful to a nation state and result in proximate harm to the citizens’ persons and property.\textsuperscript{58} 

There are several other policy reasons why the threshold for a cyber use of force cannot be taken directly from kinetic LOAC as the Tallinn Manual suggests.\textsuperscript{59} First, cyber rules in general should expand to include consideration of more attenuated damage or harm when qualifying an act as a use of force.\textsuperscript{60} The physical damage or harm requirement is only appropriate in a kinetic context, where it is easier to discern when there are kinetic weapons involved.\textsuperscript{61} In the cyber context, where attribution itself presents a complication,\textsuperscript{62} the physical harm or damage presents a more attenuated, proximate cause rather than a direct cause.\textsuperscript{63} Moreover, while civilian populations are not necessarily affected by kinetic acts because they enjoy the protections of the traditional LOAC principle of distinction,\textsuperscript{64} cyber acts often affect civilian populations without harming them under traditional LOAC.\textsuperscript{65} These effects, because they are often secondary or tertiary consequences without a physical element, do not make an act any more unlawful, though they should.\textsuperscript{66} Further, traditional thresholds must also shift because of the nature of the weapon being used.\textsuperscript{67} While kinetic acts produce fairly instantaneous damage, using computers as weapons often results in more drawn-out, long-term effects;\textsuperscript{68} traditional LOAC allows States no way to incorporate these long-term effects into their analysis of lawfulness.\textsuperscript{69} A State’s lawfulness assessment is therefore dictated by how quickly a weapon can produce an effect rather than by how deeply the effects penetrate and cause more harm over time.\textsuperscript{70} 

The comments to the Tallinn Manual present a respectable solution to expanding the scope of the current definition of an Article 2(4) use of force. Though

\textsuperscript{58} See Tallinn Manual r. 11 cmt. 10 (discussing that highly invasive operations causing mere inconvenience are not categorized as a use of force, but “some may categorize massive cyber operations that cripple an economy as a use of force, even though economic coercion is presumptively lawful”).

\textsuperscript{59} Tallinn Manual r. 11.

\textsuperscript{60} See McGhee, supra note 2, at 72–73 (explaining that limiting use of force analysis to physical effects produces illogical results because both the physical effects of kinetic attacks and the economic effects of cyber attacks can create the same negative consequences for a population).

\textsuperscript{61} See id. at 72–73 (explaining that cyber operations can have the same overall effects as kinetic strikes “without causing lasting physical damage or damage at all”).

\textsuperscript{62} Id. at 78–79.

\textsuperscript{63} Id. at 74–75.

\textsuperscript{64} The principle of distinction, which “requires states to distinguish civilian and military personnel and restrict attacks to military objectives,” presents a challenge in the cyber warfare context. Oona A. Hathaway et al., The Law of Cyber-Attack, 100 CAL. L. REV. 817, 851–52 (2012).

\textsuperscript{65} See McGhee, supra note 2, at 72–73 (“Thus, two events that cause the exact same consequences would, in fact, be treated differently under [LOAC] rules . . . .”).

\textsuperscript{66} Id. at 74–75; see also Jody R. Westby, We Need New Rules of Engagement for Cyberwar, N.Y. TIMES (Mar. 1, 2013.), http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/we-need-new-rules-of-engagement-for-cyberwar (advocating for international law reform because cyber warfare does not fit neatly within the LOAC framework).

\textsuperscript{67} See generally Westby, supra note 66.

\textsuperscript{68} McGhee, supra note 2, at 73–75.

\textsuperscript{69} See id. at 88–91 (discussing the difficulties of evaluating lawfulness for States with regard to cyber attacks).

\textsuperscript{70} See id. at 73–74 (“Can semi-autonomous delayed effect cyber capabilities register on the immediacy criterion continuum for meeting use of force or armed attack?”).
in no way binding or said to constitute black letter law, the comments actually imagine a broader conceptualization of use of force, which seems more useful in the cyber context. First, the scholars suggest a focus on the scale and effects of an act. Comment 2 to Rule 11 notes that “mere economic or political coercion” should be insufficient. Comment 9 also enumerates a very broad set of factors, including the severity and quantifiable nature of the consequences of the act, which a state could and should consider when determining whether its cyber action may constitute a use of force. I list and summarize the factors below:

1. Severity
   Analyze the level of harm or damage that was caused to individuals and property, with an eye towards the scale, scope, and duration of consequences.

2. Immediacy
   Analyze whether the act had more immediate effects or consequences; if a violated state was given the opportunity to avoid or forestall the consequences (i.e., the consequences were less immediate), it is less likely that the act should constitute a use of force.

3. Directness
   Analyze how direct the causation between the initial act and resulting consequences is; the more direct, the more likely it should constitute a use of force.

4. Invasiveness
   Analyze the degree to which a network system was penetrated; the penetration of a classified system should fall closer to a use of force than that of a declassified system.

5. Measurability
   The more quantifiable and identifiable the consequences, the more likely the act is to constitute a use of force.

6. Presumptive Legitimacy
   Consider whether the act is presumptively unlawful; if the act is explicitly unlawful, then the act is more likely to constitute a use of force.

7. State Responsibility
   The greater the state involvement in the act, the greater the threat to international stability and the more likely the act is to constitute a use of force.

This model, though it contains a more expanded definition of use of force, might work fine in after-the-fact analysis, but because of the amount of detail required to perform a thorough analysis through the factors, it is not very helpful for operational, game-time decision making.

An alternative way to integrate the economic realities of computer network interruptions in setting the thresholds of cyber activity might be to adopt a dollar-
based approach to damages. 76 For instance, if instead of weighing factors, States quantified damages and losses to help determine whether an act constituted a use of force both before and after a cyber act, they would be forced to integrate the financial consequences of cyber activities into their operational decisions.

A 2013 incident in which the Syrian Electronic Army hacked into The Associated Press’s Twitter account, causing a huge hit to U.S. stock markets, may best highlight the usefulness of this dollar-based approach.77 On April 23, 2013, the Syrian Electronic Army allegedly hacked The Associated Press’s Twitter account to post untrue tweets telling the world that there had been an attack on the White House.78 In response to the false news, the Dow Jones plunged by 150 points, and the single “fake tweet erased $136 billion in equity market value.”79 Though the effects of the act were temporary (the stock market response was later described as a “perilous but short-lived nosedive”),80 the situation does suggest that the case of true economic harm should perhaps rise to the level of use of force; but the only way to incorporate financial harm into the use of force threshold is to accept it in lieu of physical damage.

Under a dollar-based approach, if the total value of loss to network connectivity and the immediate financial repercussions exceed the dollar amount threshold, the act would constitute a use of force; but if the dollar amount of damage falls below the threshold, there is no presumption of an Article 2(4) violation. I only propose this alternative to the physical damage requirements imposed under lex lata in order to suggest that the realities of economic harm, given the growing interdependence of world economies,81 have become increasingly severe. The corresponding response to this gaping hole in the rules of cyber conduct should integrate economic harm into the equation. But integrating economic harm by re-defining use of force still asks us to stretch traditional concepts82 that may not stretch that far.

B. Creating a New Threshold Below “Use of Force”

An alternative solution to better encapsulate non-physical cyber effects, rather than expanding ill-fitted traditional concepts, would be for the international

---

76. See Thomas Dübenörrer et al., An Economic Damage Model for Large-Scale Internet Attacks, in PROCEEDINGS OF THE THIRTEENTH IEEE INTERNATIONAL WORKSHOP ON ENABLING TECHNOLOGIES: INFRASTRUCTURE FOR COLLABORATIVE ENTERPRISES 223, 225 (2004) (discussing an economic damage model that proposes to measure damages caused by large-scale Internet attacks, such as Distributive Denial of Service (DDoS) attacks, by attempting to enumerate downtime loss, disaster recovery, liability, and customer loss).

77. Max Fisher, Syrian Hackers Claim AP Attack that Tipped Stock Market by $136 Billion: Is It Terrorism?, WASH. POST, Apr. 23, 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrain-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/. It should be noted that the Syrian Electronic Army never formally claimed responsibility for the act, but there is informal evidence that the group was the perpetrator. Id.

78. Id.


80. Fisher, supra note 77.


82. See TALLINN MANUAL r. 11 cmt. 10 (“[E]conomic coercion is presumptively lawful.”).
community to create a new threshold for actions that do not meet the traditional use of force threshold but nonetheless constitute a “breach of the peace” under Article 39 of the U.N. Charter. 83

This solution, however, still requires that we stretch existing language from the U.N. Charter. Article 39 of the Charter enables the Security Council to authorize countermeasures in response to a situation that constitutes a “threat to the peace, breach of the peace, or act of aggression.” 84 Under customary law, an Article 39 violation does not necessarily reach the requisite unlawfulness of an Article 2(4) use of force violation, but the question of what actions constitute a breach of the peace even in a kinetic context is still widely contested. 85 What constitutes a mere threat to the peace, though most agree it should be distinguished from an Article 2(4) use of force, is perhaps even more ill-defined. 86 The only formal guidance on what constitutes a breach of the peace appears in Prosecutor v. Tadić, an opinion of the International Criminal Tribunal for the Former Yugoslavia, but this guidance was too broad. 87 The court there stated that a threat to the peace should be assessed according to the “Purposes and Principles of the Charter”; 88 however, the purposes listed in Article 1 cover a broad base of policies from solving social problems to developing friendlier world relations. 89 Allowing these breaches of the peace violations to provide recourse to States affected by cyber acts would enable States to respond somehow when cyber operations harm individuals or property but not in a physical way. 90 There may still be disagreement as to whether intrusions of sovereignty that do not actually harm the target nation—those that are more akin to espionage—amount to an Article 39 violation, 91 but at least acknowledging the possibility of a cyber breach of the peace would allow States recourse to mitigating action. 92

Perhaps the seemingly broad language of Article 39 and the wide discretion given to the Security Council in Tadić provide a better starting point from which to extend traditional U.N. Treaty principles to fit cyber acts. Adopting this solution

---

83. U.N. Charter art. 39 (authorizing the Security Council to determine the existence of a “breach of the peace” and to make recommendations to restore international peace and security).
84. Id. (emphasis added). The Article actually allows the Security Council to make recommendations or decide what measures are to be taken based on a list of forceful and non-forceful options in Articles 41 and 42 in order to restore national peace and security. Id.
85. See Schmitt, Cyber Operations, supra note 7, at 583 (discussing the difficulty of characterizing non-physical harm as an Article 39 threat to the peace).
86. Id.
88. Id.
89. U.N. Charter art. 1, paras. 2–3; see also Schmitt, Cyber Operations, supra note 7, at 583–84 (describing the Purposes and Principles of the U.N. Charter as including “such intangibles as developing friendly relations and solving social problems”).
90. See Schmitt, Cyber Operations, supra note 7, at 584 (describing how the Security Council “may label any cyber operation a threat to the peace” even though a cyber attack is not a physical attack).
91. See id. (stating that “[t]here are no territorial limits on situations which may constitute threats to the peace” and that “a threat to the peace is whatever the [Security] Council deems it to be”).
92. See id. (explaining that the Security Council could authorize interruption of cyber communications as a measure that would maintain or restore peace and security in the event of a cyber threat or attack).
would allow States to avoid the well-defined, results-based approaches to harm under traditional Article 2(4) use of force analyses; there would be no need to broaden “harm” past the scope of its customary kinetic interpretation. Instead, States could have alternate recourse by charging certain cyber acts that breach sovereignty as unlawful breaches of peace and seek U.N. recourse or the authority to lawfully respond via minor countermeasures.

The 2012 Iranian attacks against U.S. banking institutions, and the subsequent U.S. response, demonstrate the need for and the usefulness of creating this third category. In response to the attacks, the Obama administration was precautionous and, instead of launching counter-botnets against Iranian computers that could trigger even worse counter-attacks, the United States convinced more than 100 other countries to “choke off” the intrusive computer traffic that stemmed from computer network nodes located in their respective countries. It was largely a defensive, rather than an offensive, move that was made out of fear towards the “unintended consequences” of cyber activity; officials later claimed they were wary of an “overly aggressive response that could invite escalatory attacks that might further paralyze the networks of American businesses.” But the response successfully hindered the Iranian attack, and because of this, officials refer to it as a “template” to respond in other similar cyber cases.

I urge here that this template is an all-too-cautious one, and if the United States had access to a more legitimate, treaty-based justification for a stronger response, perhaps based on a third category of cyber activity under Article 39, it would have been able to respond more proportionately. The highly defensive strategy it adopted, in the absence of more formal thresholds, will do little to prevent the possibility of future, similar attacks on the United States, without proper recourse against cyber acts, States are left vulnerable to repeated attacks. In the cyber realm just as much as in the kinetic one, a country’s ability to take proper countermeasures allows the country to demonstrate military power and deter further action. Even in the cyber world, the ability to outwardly exercise national sovereignty and instill fear through military power should not be thwarted just because these actions lack a physical element or face ill-defined thresholds.

93. Article 2(4) extends only to “those threats of a use of force that would otherwise be unlawful,” which would exclude cyber attacks and threats. Id. at 572.
94. McGhee, supra note 2, at 89 (“It would make little or no sense to allow states to use cyber in response to use of force and armed attacks, but to limit the tools available for lesser offenses.”); see also Michael Gervais, Cyber Attacks and the Laws of War, 1 J.L. & CYBER WARFARE 8, 60-62 (2012) (suggesting that, although States’ responses to low-intensity cyber attacks are constrained, they can and will respond to less severe attacks as they accumulate).
96. Id.
97. Id.
98. Id.
99. Id.
100. See id. (reporting that former U.S. defense officials critiqued the U.S. response to the 2012 Iranian cyber attacks as weak).
Of course, acknowledging a cyber breach of the peace under Article 39 would not subject every cyber act to scrutiny as being unlawful. Just as traditional espionage, for instance, is not considered an unlawful breach of the peace or national sovereignty, cyber LOAC should not expand so far as to treat cyber espionage that does not result in any disruption in networking as unlawful by itself. For an example of cyber conduct that is intrusive but not a breach of sovereignty, one can look to recent conduct by the United States Agency for International Development (USAID). News reports indicate that in April 2013, USAID launched and backed a Cuban Twitter-like social media website to encourage dissent against the sovereign Cuban government. Under the theories here, this act, without any quantifiable or physical harm, would not constitute either an Article 2(4) use of force or an unlawful act under the theoretical third threshold of Article 39. Defining common international standards for unlawful versus lawful activity in a cyber context will also help States ensure that their ongoing cyber espionage activities do not rise to or exceed the lawfulness threshold.

IV. THEORIES ON WHAT CONSTITUTES A CYBER “ARMED ATTACK”

Under customary international law, an armed attack as referenced in Article 51 constitutes a higher threshold of unlawfulness and only an armed attack, not an Article 2(4) use of force, legitimizes use of force in self-defense. Any use of force in self-defense is of course still subject to conventional notions of military necessity and proportionality.

Customary law appropriately incorporates both scale and effects into its conception of an Article 51 armed attack. Rule 13 of the Tallinn Manual states, “A

101. See Schmitt, Cyber Operations, supra note 7, at 576 (“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.”).

102. McGhee, supra note 2, at 89 (“[W]hen aren’t cyber operations subject to LOAC? The most obvious and relevant answer is, when the operation is conducted as espionage.”); see also, e.g., Gervais, supra note 94, at 89–90 (acknowledging that nations may engage in some ruse du guerre cyber tactics that do not violate LOAC).

103. Butler, supra note 1.

104. The International Court of Justice (ICJ) takes the position that there is a substantive distinction between a use of force and an armed attack and that not all uses of force warrant unilateral self-defense. Gervais, supra note 94, at 36 (citing Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 206 (June 27)). But even under kinetic law, there is some disagreement about what exactly triggers a State’s right to self-defense. See, e.g., id. at 35–36 (noting that some scholars argue that any use of force is per se an armed attack); Michael N. Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, 54 HARV. INT’L L.J. ONLINE 13, 21–22 (2012) [hereinafter Schmitt, International Law in Cyberspace] (discussing the disagreement between the U.S. government, which believes that any use of force constitutes an armed attack justifying self-defense, and the International Group of Experts, which agrees with the ICJ that there are separate thresholds for uses of force and armed attacks).

105. Gervais, supra note 94, at 57; see also supra Part II.

State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects.107 This majority rule mandates that, when a State is to evaluate whether or not another State’s act was an armed attack, it is customary to take into account not only the effects of an action but also the scale of the action.108 The Tallinn Manual comments suggest that an armed attack requires a trans-border element109 and does not necessarily involve weapons.110 Rule 30 actually defines an armed attack as that which is reasonably expected to cause “injury or death to persons or damage or destruction to objects,”111 Comment 9 to Rule 13 admittedly states that “[t]he case of actions that do not result in injury, death, damage, or destruction, but which otherwise have extensive negative effects” is an “unsettled” classification.112

However, it is noteworthy that existing cyber definitions of armed attack at least adopt a more comprehensive approach and incorporate not only direct but also proximate effects in the analysis. Comment 10 to Rule 13 states that the majority of the International Group of Experts concluded that “all reasonably foreseeable consequences of the cyber operation” are to be considered when one is analyzing whether an act meets the threshold; this suggests a broader proximate view than direct causation.113 The Group, however, seemed divided as to whether an armed attack had to be intentional; the majority concluded that intention was irrelevant while the minority found intention to be required.114

James McGhee, an operational cyber law attorney for the U.S. Air Force, cautions against an overly-narrow approach to defining cyber attacks, suggesting that an odd outcome would result if one were to require direct physical damage for a cyber action to constitute an attack: A cyber event that blows out a power grid without any physical damage would not constitute a cyber attack, but a kinetic event that does the same thing would.115 Yet, even though the Tallinn Manual suggests a slightly broader approach, the law is in flux.116 As McGhee noted, these divisions within the law make it “possible to arrive at separate and contradictory answers of whether an event constitutes an attack.”117 And, as a result of the multi-faceted ambiguity and the numerous questions left unanswered, there have been no cyber acts that have been unanimously considered armed attacks by the international community.118

108. Id. cmt. 6.
109. Id. cmt. 2.
110. Id. cmt. 4.
111. Id. r. 30.
112. Id. r. 13 cmt. 9.
114. Id. cmt. 11.
115. McGhee, supra note 2, at 73.
117. McGhee, supra note 2, at 100.
The most recent wave of U.S. military policy adopted a surprisingly broad approach to the definition of cyber attack\textsuperscript{119}—one that proves useful in discerning a definition that incorporates all facets of “effects.”\textsuperscript{120} In Joint Publication 3-12, the U.S. Department of Defense (DoD) defined a cyberspace attack as “[c]yberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains.”\textsuperscript{121} This definition provides a good platform for States because it accounts for the special nature of computer networking\textsuperscript{122} and takes into account the devastating effects that harm other than physical harm can involve.\textsuperscript{123} However, the DOD’s definition might be problematic because it alone does not seem to delineate between various thresholds—for instance, what attacks constitute mere Article 2(4) uses of force versus Article 51 armed attacks. And, of course, because this definition originates with unilateral U.S. policy, it is unclear whether this definition is portable across the international community. Nonetheless, it provides a nice example of a step towards a more pragmatic solution in the current “hodge-podge of cyber concepts, definitions, rules, policy and law” that prevents proper development of international cyber warfare law.\textsuperscript{124}

V. \textbf{THE NEED FOR MORE DEFINED LAWFULNESS THRESHOLDS: LESSONS FROM STUXNET}

The various thresholds of unlawful cyber activity were tested most famously in the 2010 Stuxnet malware virus incident.\textsuperscript{125} There is some consensus in the international community that the 2010 Stuxnet operation was an armed attack, in part because, though the trigger occurred in cyber space, the virus ended up causing physical damage to targets.\textsuperscript{126} In June 2010, the world discovered that the Stuxnet

\begin{thebibliography}{99}
\bibitem{119} See McGhee, \textit{supra} note 2, at 94–97 (stating that “almost anything in cyber could constitute an attack” under the definition of “cyber attack” according to the military’s Joint Publication 3-12); \textit{see generally} JOINT CHIEFS OF STAFF, \textit{JOINT PUBLICATION 3-12 (R): CYBERSPACE OPERATIONS} [hereinafter JP 3-12].

\bibitem{120} See McGhee, \textit{supra} note 2, at 97 (“[T]he definition of cyber attack does not tell one whether those listed effects are the only effects allowed or whether more exist.”).

\bibitem{121} JP 3-12, \textit{supra} note 119, at II–5.

\bibitem{122} See McGhee, \textit{supra} note 2, at 100 (explaining that the definition of attack dictated by U.S. policy includes events which do not manifest physically—for instance, those that cause a change in data “to reflect something different to the observer than what is actually there”).

\bibitem{123} See id. at 72–73 (noting that a cyber event, such as the remote take down of a power grid, can lead to non-physical, yet devastating effects).

\bibitem{124} \textit{Id.} at 102.


virus, a wireless malware virus that was able to transcend public Internet, attacked programmed computers at Iran's largest nuclear facilities and caused large-scale breakdowns in Iran's nuclear operations.\textsuperscript{127} The malware worm, described as a “sophisticated computer program designed to penetrate and establish control over remote systems in a quasi-autonomous fashion,” targeted computer programming systems at Iran’s nuclear facilities—ultimately entirely reprogramming many of the systems struck.\textsuperscript{128} The bug invaded the computers, lurked for days or weeks, and ultimately sent instructions to speed the nuclear centrifuges up or slow them down so that they started spinning at supersonic speeds and ultimately self-destructed.\textsuperscript{129} One German expert that studied Stuxnet described it as a “military-grade cyber missile that was used to launch an ‘all-out cyber strike against the Iranian nuclear program.’”\textsuperscript{130} With the click of a button, a conglomerate of State and non-State actors, allegedly including the United States and Israel, managed to bring major breakdown to Iran's Natanz nuclear fuel enrichment plant, with some estimates indicating that the Stuxnet worm led to a 23\% decline in the number of operating centrifuges between mid-2009 and mid-2010.\textsuperscript{131}

The common-sense approach to the Article 2(4) use of force analysis, as well as customary law as reflected in the \textit{Tallinn Manual}, suggests that the incident was an Article 2(4) use of force.\textsuperscript{132} Because of the resulting physical damage, which would help constitute a use of force in a kinetic context, the direct application of this threshold to the Stuxnet incident points in the same direction. Even the factors laid out in the comments to the \textit{Tallinn Manual} support a similar conclusion:

1. **Severity**
   - Strong. Severe harm to property; weak harm to persons, but this factor allows for harm to property to constitute sufficiently strong consequence.

2. **Immediacy**
   - Strong. Stuxnet damaged the computers it struck immediately, without allowing the computer user or facility managers to prepare or mitigate the consequences.

3. **Directness**
   - Strong with regards to first-level damage. Much weaker with regard to secondary and tertiary systemic damage. Because the virus spread so easily [at times by itself], secondary and tertiary damages were exponential, but their importance is muted by this factor.

\textsuperscript{127} See James P. Farwell & Rafal Rohozinski, \textit{Stuxnet and the Future of Cyber War}, 53 \textit{SURVIVAL: GLOBAL POL. & STRATEGY} 23, 29 (2011) (examining Stuxnet’s effect on Iranian nuclear facilities, citing reports of temporarily-ceased uranium feeding, and speculating that a “decline in the number of operating [Iranian] centrifuges” for a period may be attributable to the virus attack).

\textsuperscript{128} \textit{Id.} at 24.

\textsuperscript{129} Foltz, \textit{supra} note 126, at 44.

\textsuperscript{130} Farwell & Rohozinski, \textit{supra} note 127, at 23.

\textsuperscript{131} \textit{Id.} at 29.

\textsuperscript{132} \textit{TALLINN MANUAL} r. 11 cmt. 8
4. Invasiveness  Strong suggests use of force. Stuxnet struck and completely controlled computer-programming systems.

5. Measurability  Medium. While the consequences are identifiable [network failure was traceable to Stuxnet], they were not quantifiable.

6. Presumptive Legitimacy  Weak/not applicable. No presumptive legitimacy or illegitimacy.

7. State Responsibility  Weak. Unclear the degree of state involvement.\textsuperscript{133}

However, while the Tallinn Manual rules and a strict application of traditional LOAC to Stuxnet suggest that the incident was an Article 2(4) use of force, the international community is still left utterly confused as to whether it rose to the threshold of armed attack.\textsuperscript{134} The Tallinn Manual charges us with looking at both the scale and effects of the act,\textsuperscript{135} but the Stuxnet incident reveals that some questions are still unresolved: From what chronological point of a large-scale attack does one assess whether the threshold of armed attack has been satisfied? Even among the proximate effects, what extent of effects does one take into account? Is it legitimate to treat the subversive nature of the attack as evidence of an armed attack rather than a less severe breach of the peace or use of force?

Some might even argue that Stuxnet was simply a pre-emptive cyber strike in self-defense in response to the threat of Iran’s nuclear program,\textsuperscript{136} yet, it does not seem that Iran’s activities were at all imminent, which would be required to constitute a lawful act of self-defense under Article 51.\textsuperscript{137} Even so, the lawfulness of Stuxnet as a preemptive cyber strike ultimately turns on whether the consequences of the act were proportional to the perceived threat—a determination drawn from traditional LOAC that back then and even now remains foggy at best.\textsuperscript{138}

While Stuxnet demonstrated the international community’s need for better tools to preemptively assess the lawfulness of States’ cyber actions and reactions, more recent news about the United States’ reaction to Iran’s intrusion on its financial

\textsuperscript{133} Id. r. 11 cmt. 9.

\textsuperscript{134} See Farwell & Rohozinski, supra note 127, at 32–33 (questioning whether action as a recourse to a cyber attack is allowed under Article 2(4) of the U.N. Charter).

\textsuperscript{135} TALLINN MANUAL r. 11.

\textsuperscript{136} Id. r. 13 cmt. 13 (“In light of the damage they caused to the Iranian centrifuges, some members of the International Group of Experts were of the view that the operations had reached the armed attack threshold (unless justifiable on the basis of anticipatory self-defence . . .)” (emphasis added)).

\textsuperscript{137} Id. r. 15.

\textsuperscript{138} A State may only resort to proportionate countermeasures to a perceived threat. Id. r. 9.

\textsuperscript{139} “The principle of proportionality stems from Article 51 of Additional Protocol I, which states that force is prohibited where it ‘may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.’” Gervais, supra note 94, at 84–85 (quoting Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51(5), June 8, 1977, 1125 U.N.T.S. 3). Some courts take the view that there is a “zone of proportionality” within which a State has discretion to act. Gervais, supra note 94, at 85–86 (citing HCJ 2056/04 Beit Sourik Vill. Council v. Gov’t of Isr. 58(5) PD 807 [2004] (Isr.)).
institutions in 2012\textsuperscript{140} only further underscores the fact that States are left misguided. The Obama administration’s response may have been altogether different if the United States had treaty protocols and more delineated principles to follow. If these cyber treaty protocols—hopefully elaborated sometime in our distant future—integrate consideration of the wide variety of intrusions on sovereignty that can occur as a result of cyber activity, States will be in a much better place to assess their own actions as well as those of intruders.

\textbf{CONCLUSION}

The latest cyber rumblings around the conflict in Crimea underscore that almost every modern conflict will involve some sort of cyber activity.\textsuperscript{141} A week after Russia supposedly entered the Crimea region, Ukrainian security alleged that unknown cyber attackers were interfering with the mobile phone services of Ukrainian Parliament members.\textsuperscript{142} In April 2014, reports indicate that Russian forces used hacking to intercept a U.S. surveillance drone that was over the Crimea region.\textsuperscript{143} Not only has warfare evolved, but it also continues to evolve, and these new types of cyber activities make international recognition of cyber lawfulness thresholds even more critical to a legitimate LOAC tradition.

Given this influx, “[s]tates contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community’s probable assessment of whether the operations violate the prohibition on the use of force.”\textsuperscript{144} In order to properly assess the international community’s reaction, a State must be able to reasonably determine if its plan meets the threshold of a breach of the peace or rises to the level of an Article 2(4) use of force, and, if the plan entails force, whether it is a proper use of force in self-defense to an armed attack under Article 51. The reciprocity and therefore the legitimacy of LOAC rests upon more delineated and accepted notions of lawful thresholds within the realm of cyber activities.

Even outside of preserving the LOAC tradition, it is incumbent upon organizations like the United Nations to meet the evolving nature of military operations, especially as States are increasingly contributing resources into developing cyber operations.\textsuperscript{145} In April 2014, the U.S. Army launched the Cyber Center for Excellence at Fort Gordon, the location where it plans to house all military doctrine writers for electronic warfare, signals, and cyber operations.\textsuperscript{146} The Army also recently published field manual FM 3-38, \textit{Cyber Electromagnetic Activities}, a response to the increasingly wireless nature of cyber operations and an

\textsuperscript{140} Perlroth & Hardy, supra note 4.


\textsuperscript{143} Porche, supra note 141.

\textsuperscript{144} TALLINN MANUAL r. 11 cmt. 8.

\textsuperscript{145} See, e.g., Porche, supra note 141, (describing cyberwarfare developments, including the increase in wireless cyberspace acts, and the United States’ operational military responses to these developments).

\textsuperscript{146} Id.
acknowledgement of the “broad and rapidly changing operational environment” that requires the Army to “leverage an electromagnetic spectrum that is increasingly competitive, congested, and contested.” The manual organizes infrastructure around cyber operations, setting up tactical cells that are to be filled with special personnel trained in electronic warfare. Moves like this indicate that military operations all over the world are increasingly and rightfully responding to the impact that technological developments have on modern warfare. But, despite international scholars’ and independent States’ best efforts at responding to the developments, it unfortunately may be years before other well-recognized international authorities with greater enforcement mechanisms like the United Nations attempt to fill the void through formal treaty powers. Until then, the customary protocols around the various activity thresholds should shift to meet the realities of our changing conflict landscapes.

147. FM 3-38, supra note 28, at v.  
148. See generally id.