International Adoption of the Tallinn Manual : Examining Legality and Repercussions of the Stuxnet Worm

Steve Jarvis

Boston University, CS 591: Cybersecurity and Policy
December 13, 2014

Contents

1 Introduction

Recent years have witnessed a shift of the earth's battlefield. For better or worse, militaries can largely trade in their guns for laptops and their soldiers for hackers. The nations of the world are connecting critical services and infrastructure to cyberspace, and doing so with minimal technical or legal protections in place. This puts them at great risk of attack. As the offensive capabilities and risks continually increase in cyberspace, so too must the protections.

In the wake of the Second World War, the international community recognized the necessity of establishing agreements and rules governing international conflict. The United Nations was organized in 1942 and the Geneva Conventions in 1949.[1] These organizations founded treaties that define international laws for entering into conflict (*jus ad bellum*) and behavior during conflict (*jus in bello*), respectively. To this day, those laws protect States from unjust attack and offer aid and support when the laws are broken and a nation is victimized.

The agreements by these groups were established a full half-century before the public Internet was in its infancy, and therefore the laws consider only kinetic warfare.[2] The growing prevalence of cyber operations is pushing the boundaries of what might be considered harmful or forceful behavior, and the international community has little means to deal with such events. Cyber operations rarely have a direct or obvious kinetic counterpart for comparison, and without established guidelines or limitations, States continue to progress their offensive cyber arms race. Cyber operations are limited only by technical capabilities rather than legal or ethical standards.

The Tallinn Manual was created to fill this void in international law by translating

1. "History of the United Nations," 2013, accessed November 2, 2014, `http://www.un.org/en/aboutun/history/`; Phillip Spoerri, "The Geneva Conventions of 1949: origins and current significance," International Committee of the Red Cross (ICRC), December 2009, accessed November 2, 2014, `https://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-120809.htm`

2. "Kinetic" is used throughout to describe traditional military action, one that involves physical movement and attack.

the established kinetic laws to this modern, cyber battlefield.[3] The need for such a set of laws grows more apparent with each passing year, as defensive capabilities remain relatively stagnant while offensive arsenals and dependence on cyberspace increase dramatically.

The goal of this report is to examine whether the Tallinn Manual is a suitable guide for use in establishing agreements on permissible cyberspace operations in the international community. To make this determination, its applicability to real life actions, particularly the Stuxnet worm, will be explored, as well as the Tallinn Manual's political hurdles. If successful, the Tallinn Manual could be the basis of an official adoption of cyberspace laws and help to ensure the safety and security of all States and their citizens in coming years.

2 The Current International Law

Today, 193 of 196 countries of the world are members of the United Nations (Kosovo, Taiwan, and Vatican City are the only non members).[4] These countries enjoy agreements protecting their sovereignty and freedom from unsolicited acts of physical aggression. These laws do not explicitly exclude cyber acts of aggression, but the nature of international law is permissive; if an act isn't explicitly stated illegal, then it is considered legal.[5] Since there are no laws established for cyber operations and little or no clear correlation to kinetic laws exists, there is no obvious illegal cyber operation between nations.

States have developed differing opinions on how established laws effect cyber operations. The different interpretations result in dissension among States and incompat-

3. Micael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), 18. See paragraph 2.

4. "Members," United Nations, 2002, accessed November 18, 2014, `http://www.un.org/en/members/`

5. "The Lotus Case (France vs Turkey)," Public International Law: An introduction to public international law for students, 1927, accessed November 23, 2014, `http://ruwanthikagunaratne.wordpress.com/2012/07/27/lotus-case-summary/`

ible policies. This lack of cohesion has serious results: there are no accepted answers on whether it is possible to exert a use of force or launch an armed attack online, how to qualify such attacks if they are a possibility, or what repercussions would be appropriate if those attacks were executed.[6]

The United Nations Security Council rules on kinetic uses of force involving members of the United Nations. The same cannot be afforded to nations victim of a cyber attack, since there are effectively no relevant laws. There can be no legitimate and organized repercussion from the international community.

3 Why The International Community Needs to Establish Cyber Agreements

In 2007, Estonia chose to relocate a bronze statue of a Soviet soldier to quell a dispute between Estonian nationalists, who saw the statue as a symbol of oppression, and a Russian ethnic group, who considered the statue's take down offensive. Following the statue's move, Russia initiated perhaps the largest distributed denial of service (DDOS) attack seen to date. Estonia is one of the most cyber connected nations in the world, and the attack disabled banking, news websites, the government's online services, telephony and credit card verification systems. Estonia's communications and commerce were rendered effectively useless for weeks.[7]

The events in Estonia demonstrate the capabilities of even simple cyber attacks, and the serious detrimental effects for States as connected as Estonia prove the con-

6. *Charter of the United Nations* (United Nations, October 1945), accessed October 11, 2014, `http://www.un.org/en/documents/charter/`; Matthew C Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* 36, no. 2 (2013), accessed October 11, 2014, `http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf`, 431-435. See the United Nations charter for definitions of a use of force and armed attack, specifically Articles 2(4) and 51.

7. Richard Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About it* (New York: HarperCollins Publishers, 2010), ISBN: 978-0-06-196224-0, 12-16.

cern is significant.[8]

The world's situation is growing more treacherous as States increase their reliance on cyberspace. Critical infrastructure, including power grids, water treatment plants, financial institutions and health care equipment, is coming online and reliant on the Internet for communication and proper operation. Citizens and governments depend on these services to maintain a healthy and safe standard of living. This infrastructure, and by extension the cyberspace that enables its proper operation, has a direct effect on a State's sovereignty and deserves the same protections the physical world is granted. For this same reason, the United States' National Research Council agreed that attacks which have a significant effect on a State's infrastructure should be considered armed attacks, even without direct injury, violence, or death.[9]

The new realm of cyberspace provides a battleground States of the world are just beginning to explore. New attacks are constantly developed and far outpace States' abilities to defend against them. It is crucial that the international community does what it can by establishing agreements protecting States' cyberspace, just as it did protecting States from traditional attacks.

4 Overview of the Tallinn Manual

The Tallinn Manual was an effort to address this growing concern over the threats posed via cyberspace. Many nations, including the United Kingdom, the United States, Russia, and Canada, cite national cyber security as an utmost priority.[10] The Tallinn Manual's aim was to fill the void in the international laws on conflict by determining the correlation between cyber operations and kinetic counterparts.

8. Clarke and Knake, *Cyber War*, 13. In at least 2007, Estonia ranked ahead of even the United States with regards to Internet use for daily tasks.

9. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities" (2009), accessed November 29, 2014, `http://www3.nd.edu/~cpence/eewt/Owens2009.pdf`, 254.

10. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 16-17

Ultimately, the stated goal of the Tallinn Manual is to provide non-binding guidance on which cyber operations are within the bounds of the law.[11]

The North Atlantic Treaty Organization (NATO) encouraged and supported the project. Michael Schmitt, a professor at the United States Naval War College and editor of the Tallinn Manual, led an international group of legal experts from many NATO States in discussion regarding the complications of cyber operations and how to apply established laws to this new dimension.[12] The result is a set of twenty-five rules and many additional thoughts, issues and sticking points in the form of commentary throughout the document. The rules cover such issues as defining a violation of sovereignty and jurisdiction, categorizing and defining a use of force and cyber (armed) attack, and special considerations for civilians.[13] All of the conclusions reached by the Tallinn Manual are inspired by established international law, often specifically the United Nations Charter and the Geneva Conventions, and the reasoning is often thoroughly assessed in the embedded commentary.

The three-year effort concluded in 2012 and continues to stand alone in its thoroughness in considering a modern world and outpaced laws. While the self-declared intentions were to construct a non-binding document, practice has proven the Tallinn Manual unparalleled in its applicability and usefulness. Timothy Edgar, the first Director of Privacy and Civil Liberties for the White House National Security Staff, states that "... in reality, if you want to determine the legality of a cyber operation, you reach for the Tallinn Manual."[14]

To determine if the Tallinn Manual is technically useful in addition to being legally sound, it will be examined in the context of a real life cyber operation: the Stuxnet worm.

11. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 16. See paragraph 1.
12. ibid., 17. The group of experts will be referred to throughout as simply the "Experts".
13. ibid. See rules 1, 2, 10-11, 30 and 32, respectively.
14. Timothy Edgar, "Cyberwar (1): the use of force in cyberspace," *presentation. Boston University, Cybersecurity and Policy.* (2014)

5 Details of the Stuxnet Worm

Stuxnet was a revolutionary cyber attack executed in 2010 that sabotaged the programmable logic controllers (PLCs) at Iran's nuclear enrichment facility at Natanz. The intent was to delay Iran's potential development of nuclear weapons, and it did this by causing the centrifuges that separate nuclear material to spin out of control and ultimately destroy themselves.[15]

Despite the destructive chaos actually happening in the system, the Stuxnet malware continuously delivered positive reports to the operators, providing assurance that all operations were going safely and as planned. The human operators capable of intervention had no indication there was an issue, much less one so dire. Stuxnet was the first operation consisting of only a computer program to cause destruction and setback to a sovereign State's military; it was a weapon made entirely of code.

To consider Stuxnet an act of aggression by another nation it first has to be known that it was, in fact, the product of a State, and not the effort of a private group of citizens or hacktivists. Very early on there was strong evidence pointing towards a State backing. Stuxnet's level of technical difficulty was uncontested by any cyber attack prior (and maybe since), and in addition to being very complex, it was also extremely expensive.[16] More recently however, solid claims have surfaced proving it was executed by a nation state, particularly a collaboration between the United States and Israel.[17] Stuxnet is now widely accepted to have been orchestrated by a

15. "Stuxnet 0.5: Distrupting Uranium Processing at Natanz," last modified January 2014, accessed October 11, 2014, http://www.symantec.com/connect/blogs/stuxnet-05-disrupting-uranium-processing-natanz; David Kushner, "The Real Story of Stuxnet: How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program," IEEE Spectrum, February 2013, accessed October 11, 2014, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/

16. Ben Flanagan, "Former CIA chief speaks out on Iran Stuxnet attack," The National, December 2011, accessed October 11, 2014, http://www.thenational.ae/business/industry-insights/technology/former-cia-chief-speaks-out-on-iran-stuxnet-attack. The cost of Stuxnet is estimated to be around one million U.S. dollars.

17. Lee Ferran and Kirit Radia, "Edward Snowden: U.S., Israel 'Co-Wrote' Cyber Super Weapon Stuxnet," ABC News, July 2013, accessed November 23, 2014, http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cyber-super-weapon-stuxnet/

nation state, which qualifies it as a politically motivated operation and subject to international laws of conflict.

The enrichment facility at Natanz was not connected to the Internet and relied on a private, "air-gapped" network.[18] Despite these precautions taken against potential cyber attack, the facility proved to still be vulnerable. Stuxnet was likely introduced to the target environment by an infected USB drive.[19] The route to Natanz is unknown, but it is likely the virus crossed through the Internet infrastructure of a number of neutral States.

The damage was intended to stifle development of military operations by damaging Iran's ability to enrich uranium. The precise effects are unknown, as Iran made no official comment on whether it suffered damage from Stuxnet. However, it is widely held that their nuclear program did suffer significant setbacks, on the order of what might have been accomplished with a kinetic attack.[20]

As with many worms, and almost by their very design, Stuxnet proved difficult to control. It leaked into the wild and infected an untold number of civilian and State owned computers in more than a dozen countries.[21] Eugene Kapersky, founder of the Russian security company Kapersky Labs, claimed the virus even infected Russian nuclear facilities. He is not alone in these claims either, with as many as fifteen other industrial complexes around the world believed to have been infected by Stuxnet.[22]

The distinction between civilian and nuclear or industrial facility infection is sig-

18. "Air gap" is a term commonly used to describe a network that is physically separate from unsecured networks.

19. Aleksandr Matrosov et al., "Stuxnet Under the Microscope: Revision 1.31," ESET, 2010, accessed November 16, 2014, `http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf`, 8.

20. David Albright; Paul Brannan; Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?," *Institute for Science and International Security* (2010), accessed November 23, 2014, `http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf`

21. Matrosov et al., "Stuxnet Under the Microscope," 15.

22. Chris von Eitzen, "Stuxnet also found at industrial plants in Germany," The H, September 2010, accessed November 18, 2014, `http://www.h-online.com/security/news/item/Stuxnet-also-found-at-industrial-plants-in-Germany-1081469.html`

nificant, not only due to concerns regarding civilian targeting, but because of the nature of Stuxnet itself. Stuxnet was designed to recognize the hardware on which it was running, and if it wasn't on specific Siemen's PLCs it would sit dormant.[23] Civilians with infected computers would not only be unaware, they would be at no risk of danger whatsoever. The infected industrial facilities, however, were likely to suffer grave damage, just as Iran's facility is believed to have experienced at Natanz.[24]

5.1 Why Stuxnet Deserves the Focus

Stuxnet exists amidst many controversial cyber operations over the past decade, and it still deserves much focus when considering cyber operations and international law on armed conflict. It offers, arguably, the most likely candidate of a cyber-only operation to be considered a use of force or an armed attack. It exists on a level of complexity and intent all its own. Prime alternative operations include the Flame Malware and Russia's cyber attack on Georgia.[25] Flame was used for only espionage, and that is generally considered legal under international law.[26] Russia's cyber attack on Georgia in 2008, conversely, was used to further a kinetic attack and falls clearly into the category of an armed attack.[27] These operations raise many interesting questions of their own, but the overall conclusions are unsurprising and generally uncontroversial.

23. Eitzen, "Stuxnet also found at industrial plants in Germany"

24. Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?"

25. Richard Steinnon, "Flame's MD5 collision is the most worrisome security discovery of 2012," Forbes, June 2012, accessed October 21, 2014, `http://www.forbes.com/sites/richardstiennon/2012/06/14/%20flames-md5-collision-is-the-most-worrisome-security-discovery-of-2012/`; David J. Smith, "Russian Cyber Strategy and the War Against Georgia," Atlantic Council, January 2014, accessed October 11, 2014, `http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia`

26. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. See rule 6, comment 4.

27. ibid., 94. See paragraph 6. Also see rule 20.

6 Where Traditional Law is Not Enough

Cyber operations like Stuxnet are unlike any with which the world has previously dealt. The executions of these attacks raise many questions where guidance from a suitable source is desired to determine which laws, if any, were broken, how severely they were broken, and what response might be warranted. There are a handful of significant issues raised by Stuxnet which warrant specific consideration:

1. Was Stuxnet a use of force, as defined by international laws of conflict?
2. If it was a use of force, does it also qualify as an armed attack?
3. Did the operation lack sufficient discrimination and direction?
4. Which States can be held accountable in such an event?
5. If international laws were broken, what response is warranted by the victim State? How might the aggressor be reprimanded, and how should the rebuke be enforced?

Each of these issues will be explored in depth with specific consideration for what makes the issue controversial under the current laws of conflict.

6.1 Use of Force

At perhaps the most fundamental, it is not clear whether Stuxnet was illegal under international law. To determine its legality there would need to be consensus that it did violate a law or laws already in place. One of the foremost (though certainly not only) laws would be that prohibiting a use of force, set forth by Article 2(4) of the United Nations Charter. Article 2(4) states:

> 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.[28]

28. *Charter of the United Nations.* See Article 2(4).

Regarding only this law, which was established for dealing with kinetic operations, Stuxnet's classification as a use of force is not clear. Though there is no distinction between cyber and kinetic operations mentioned, the traditional notion of force requires military force and violence, whereas Stuxnet, and nearly all cyber attacks, did not even include a physical presence, much less kinetic force. The interpretations of laws as established are insufficient to categorize Stuxnet as a use of force.

6.2 Armed Attack

Some States have adopted a generally all-encompassing definition of what constitutes an illegal use of kinetic force, while others operate with much narrower classifications that limit an armed attack to be effectively the same as a use of force.[29]

One of the most popular definitions of an armed attack is resultant of a 1986 case decided by the International Court of Justice between the United States and Nicaragua. The ruling classified an armed attack as one which is executed by armed forces sent directly by a State or on behalf of a State.[30] This definition is rather limiting and seems to explicitly exclude any cyber attacks by its very nature, since it makes numerous references to traditional arms. Similarly, most all traditional definitions of armed conflict require some level of physical violence matching or in excess of a use of force.[31] There have been no cyber-only attacks to date that fit this description, and it very well may be impossible simply by definition.

Furthermore, any conclusion to the issue of qualifying an armed attack is surely more complex than a simple black and white answer. The infections of civilian machines could be categorized differently than infections of State owned infrastructure.

29. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 17. See paragraph 3.

30. "Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)," International Court of Justice, June 1986, accessed November 29, 2014, `http://www.icj-cij.org/docket/?sum=367&code=nus&p1=3&p2=3&case=70&k=66&p3=5`. See paragraphs 187-201.

31. Owens, Dam, and Lin, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," 253. See paragraph 2.

Civilian infections were not necessarily harmful, and mere infection may not equate to a cyber attack in any case.

Determining when an operation crosses the threshold and becomes an armed attack is generally difficult, but as mentioned in section 3, it is crucial the international community has the means to classify attacks in cyberspace.

6.3 Discriminate Attack

Supposing the Stuxnet worm can be qualified as an armed attack, its spread throughout cyberspace raises questions of discrimination. A similar failure to control weapons in kinetic warfare is outlawed as indiscriminate, but it is not clear the same applies to malware, since it often has far less directly devastating results.[32] With malware there is little danger of immediate harm relative to indiscriminate kinetic attacks, such as acts of chemical warfare or the destruction of a hospital. Even without immediate harm, though, if a cyber operation can be classified as an attack, it is logical that it must be subject to the same laws of discrimination.

6.4 Accountability of Neutral States

If an operation is decided to be in violation of any laws, the sponsors of the malware and its authors should clearly be held responsible. There may be additional participants to consider, though. In kinetic warfare, belligerents cannot use neutral territory for transport of munitions, and it is a duty of the neutral State to ensure that is the case.[33] Application of those laws to cyberspace could require neutral States to take

32. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)* (International Committee of the Red Cross (ICRC), June 1977), accessed October 11, 2014, `https://www.icrc.org/ihl/WebART/470-750065`

33. *Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land* (International Committee of the Red Cross (ICRC), October 1907), accessed October 11, 2014, `https://www.icrc.org/ihl/INTRO/200?OpenDocument`. See Articles 2 and 5. The Hague Conventions are generally superseded by modern treaties, but are still cited as inspiration in many places of the Tallinn Manual.

measures preventing the transfer of malicious software or other facilitation of attacks via cyber infrastructure located within their territory. It is possible that a failure to stop the propagation of a cyber attack is, in itself, considered an attack.

6.5 Defense and Rebuke

Equally important is the issue of enforcement and reprimanding States who are deemed in violation of accepted law. The United Nations Charter allows for a use of force as self defense in Article 51, though it also requires any response to be proportional to the action which provoked it.[34] No cyber operation has been met with a military response to date, and in many cases such a response would seem excessive. For clarity on future policies, it is important to determine whether such a response could be deemed reasonable.

International conflict between members of the United Nations is subject to the United Nations Security Council for review and ruling. On multiple occasions, however, the Security Council has failed to reach a timely decision (or reach a decision at all), and this has potentially devastating consequences for victim States.[35] If a similar process is used for cyber operations it is important to consider what actions a State can take, within the bounds of the law, to protect itself in the time before an official ruling by the Security Council.

34. *Charter of the United Nations*

35. Andrew Johnson, "Ban Ki Moon Laments 'Embarrassing Paralysis' of U.N. Security Council," National Review, September 2013, accessed November 29, 2014, `http://www.nationalreview.com/corner/357974/ban-ki-moon-laments-embarrassing-paralysis-un-security-council-andrew-johnson`; Michele Kelemen, "U.N. Security Council Deadlocked over Kosovo," NPR, December 2007, accessed November 29, 2014, `http://www.npr.org/templates/story/story.php?storyId=17441680`. These are two examples of Security Council deadlock where no decision was reached.

7 Applying the Tallinn Manual to Analyze the Stuxnet Worm

Now we turn to the Tallinn Manual to resolve these issues applying existing laws to cyberspace. The goal is to determine whether the Tallinn Manual is an effective tool in practice by exploring whether it proves useful when evaluating Stuxnet.

Regarding the legality of Stuxnet, the Tallinn Manual defines a cyber operation to be a use of force when the effects of the operation "are comparable to non-cyber operations rising to the level of a use of force."[36] It goes on to suggest a detailed rating scale for cyber operations in the comments, including such factors as severity, immediacy, directness, invasiveness and military character, most of which Stuxnet clearly violates.[37] The group of Experts considered Stuxnet specifically in their work, and unanimously concluded it to be a use of force. Therefore, the operation was in violation of international law by Article 2(4) of the United Nations Charter.[38]

The manual goes on to say that the Experts were unanimous in determining cyber operations alone might qualify as armed conflict:

> An armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, occurring between two or more States.[39]

This finding alone is significant, because it would bring responding to a cyber attack with a military use of force within the realm of possibility. This finding directly contradicts other interpretations of the Charter that reserve an armed attack for kinetic military operations.[40]

36. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 48. See rule 11.

37. ibid., 49-52. See comment 9.

38. Kim Zetter, "Legal Experts: Stuxnet Attach on Iran Was Illegal 'Act of Force'," Wired, March 2013, accessed October 6, 2014, `http://www.wired.com/2013/03/stuxnet-act-of-force/`

39. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 71. See rule 22.

40. Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Legal Studies Research Paper Series* 1023 (2008), accessed November 24, 2014, `http://papers.ssrn.`

The case of Stuxnet is specifically mentioned in the commentary of the Tallinn Manual regarding an armed attack. It is stated that the Experts were divided on whether Stuxnet should be categorized as an armed attack, mostly due to an insufficient level of damage caused.[41] Some Experts noted the attack may also have been justified as anticipatory self-defense.[42]

The Tallinn Manual definitively decides that indiscriminate methods of cyber war are prohibited, which is appropriate since it concluded that it is possible for cyber operations to reach the level of an armed attack.[43] It is undecided whether the mass infection of computers violates this, because the group of Experts was undecided on ruling the mere installation of malware to be a violation of sovereignty.[44] In the case of Stuxnet, infection alone was unremarkable and the attack was performed only on specific Siemens systems, so it is not clear whether even widespread infection would put Stuxnet in violation.[45]

If Kapersky's claims that Stuxnet later infected Russian nuclear sites are true, though, Stuxnet did violate the sovereignty of Russia and failed to be sufficiently discriminate with its target.[46]

The Tallinn Manual is not equally conclusive on all matters, though. As mentioned, Tallinn Manual is clear that cyber operations alone could amount to an armed attack, but provide little means to determine whether a specific operation crosses that threshold, or how an armed attack relates to a use of force.[47] These are standing prob-

com/sol3/papers.cfm?abstract_id=1083889. This is one such interpretation that reserves the category of armed attack for kinetic force.

41. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 71. See rule 22, comments 14 and 15. There commentary also cited uncertainty that the operation was the attributable to a State and not an independent group, but this has since been generally confirmed.

42. ibid., 56. See rule 13, comment 13.

43. ibid. See rule 43.

44. ibid., 25. See comment 6 of rule 1.

45. Kushner, "The Real Story of Stuxnet"

46. "More Stuxnet: US-Israeli Computer Virus Infected Russian Civilian Nuclear Power Plants," 21st Century Wire, November 2013, accessed October 11, 2014, http://21stcenturywire.com/2013/11/13/more-stuxnet-us-israeli-made-virus-infected-russian-civilian-nuclear-power-plants/

47. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 71. See rule

lems with kinetic conflict as well, and Schmitt says these specifics were intentionally not expanded upon in the Tallinn Manual, as to not alter the definitions provided by existing international law.[48]

Despite offering little means for identifying a specific threshold, there is a definition provided for a cyber (armed) attack. In an interview, Schmitt explained that

> ... the majority said that an attack, in the law of war, means you physically harm someone, you break something, you cause physical damage or you interfere in the functionality of an object such that it needs to be actually repaired.[49]

The Tallinn Manual offers a similar definition, which is a

> ... cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.[50]

Both Schmitt's comment and the consensus of the legal scholars seem to suggest Stuxnet was an armed attack, yet the Experts still disagree it crossed the threshold of damage. Many believe there was little physical damage done, compared to traditional, kinetic force.[51]

Iran had clear jurisdiction in Stuxnet.[52] It is now widely accepted that Stuxnet was the product of an effort between the United States and Israel, and if Iran were seeking a response they would surely be the primary subjects. Laws on kinetic warfare state that neutral States who fail to remain neutral can also be held accountable for transferring munitions. Regarding the transfer of malware, Tallinn Manual specifies

22.

48. Mike Gollom, "Are there international rules for cyberwarfare?," CBC News, March 2013, accessed October 19, 2014, `http://www.cbc.ca/news/world/are-there-international-rules-for-cyberwarfare-1.1323638`

49. ibid. See paragraph 4.

50. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. See rule 30.

51. John Leyden, "Cyberwar playbook says Stuxnet may have been 'armed attack': Would you rather be shot, blown up, stabbed - or hacked?," The Register, March 2013, accessed October 26, 2014, `http://www.theregister.co.uk/2013/03/27/stuxnet_cyberwar_rules/`

52. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 27. See rule 2.

that States must not *knowingly* allow conflicting parties to use their infrastructure.[53] The Experts were split on whether that permits neutral States to passively allow such transmission. Many felt that in order to claim there was an unknown transfer there must be a significant effort to ensure such activity is not taking place.[54] In the end, the Tallinn Manual provides no bottom line on the responsibility of neutral states or their accountability for passively transferring cyber munitions.

When considering a response, the issue of immediacy is more of a factor in cyberspace than in kinetic warfare. In the case of Stuxnet, Iran didn't know it was being attacked until the machinery was already damaged and the attack was effectively complete. With no imminent or current attack there is no justification for an armed response under Article 51. Conversely, a kinetic attack is generally immediately apparent to the victim and immediacy is rarely a consideration. Again, the Tallinn Manual did not change the definition of immediacy for cyberspace, only provided means to help determine whether cyber operations meet the established standards for immediacy.[55] With the conclusions drawn by the Tallinn Manual, Iran would only be able to respond with force if they believed the attack was part of a larger campaign and likely to continue.[56]

8 Why International Law Should Adopt the Tallinn Manual

While the Tallinn Manual was not conclusive across all issues, it does an exceptional job of applying existing international law to the age of the Internet. It provides a great foundation, but dealing effectively with this era of cyber operations requires

53. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 206. See rule 93.

54. ibid. See rule 93, particularly comments 5 and 6.

55. ibid., 60. See rule 15, especially comments 9 and 10.

56. ibid., 62-63. See comment 9 of rule 15 on immediacy.

more than just translations of laws from the kinetic era.

As an example of where more than a simple translation may be warranted, consider again the 2007 conflict between Russia and Estonia. The Tallinn Manual is unlikely to qualify that event as an armed attack, since there was no reasonable expectation of injury, death, or damage.[57] As States grow more dependent on cyberspace for the operation of critical infrastructure, however, there is no longer a requirement of physical destruction or violence to threaten a State's sovereignty. This was apparent in Estonia, as victims were unable to access their own funds or purchase basic needs.

Therefore, this conclusion of the Tallinn Manual is one that needs to be improved in order to catch up with the age of the Internet. Michael Norris suggests an amendment to the Tallinn Manual's definition of cyber attack to reconcile (difference emphasized):

> A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to, *or neutralization of*, objects.[58]

This amendment should not suggest that any disruption of service be regarded as a cyber attack, but needs to allow for protection in cases like the attack on Estonia, where there was a great effect on the nation's ability to operate effectively, yet without causing any physical damage. Narrowing the threshold that constitutes an armed attack remains an open issue.

Sections of the Tallinn Manual, and even this amended rule, could be seen as lacking some detail or specifics. For example, when does an operation cross the threshold from an inconvenience to an attack? Is the mere installation of malware a violation of sovereignty? When is a State sufficiently involved with the creation or distribution of an attack to warrant responsibility? Much of this lack of detail in

57. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*. See rule 30.

58. Michael J. Norris, "The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace," Student Pulse, 2013, accessed November 22, 2014, `http://www.studentpulse.com/articles/775/the-law-of-attack-in-cyberspace-considering-the-tallinn-manuals-definition-of-attack-in-the-digital-battlespace`

the Tallinn Manual can actually be regarded as a strength through flexibility. Any corresponding kinetic issues are often equally gray and require a case-by-case analysis. Cyberspace adds an additional layer of complexity and rapid advancement. Making a set of rules as specific and technically detailed as possible has the significant drawback of failing to keep up with innovation and potentially allowing for legal loopholes. The general nature of the laws allow for interpretation and for continual operation in the spirit of those laws rather than the literal letter.

Potential adoption of the Tallinn Manual raises more than only technical questions. Some of the greatest hurdles to a universal adoption of the Tallinn Manual are political. As a NATO sponsored project, the translation of existing law to the realm of a global cyberspace may be accompanied by a Western bias. Further, those States typically at odds with NATO will be unlikely to consider a set of rules compiled solely by NATO.

A subset of the currently undecided issues (whether neutral states can be held accountable for only negligence, whether installing malware is itself a violation of sovereignty, etc.) on which the Experts were divided could reasonably be more definitive and solidified with time and applied as general rules. Those States outside NATO, particularly those often in disagreement, should be encouraged to participate in solidifying and defining the rule set. This will help the Tallinn Manual to 1) be free of NATO bias and 2) be supported by all States, not just those who are members of NATO.

Once the evolution of the Tallinn Manual is made a global participation it will be more likely to garner universal backing. When it does and appropriate amendments are made, the current members of the United Nations should be encouraged to ratify a treaty adopting adherence to the rules set forth within the Tallinn Manual.

Any agreement should adopt the Tallinn Manual as a starting point for ruling on international cyber conflict and be used as a basis to continually evolve relevant

international law. Given the rapid growth of information technology, it should be a highest priority to establish an official means to make lasting and binding amendments to the Tallinn Manual (or treaty), as deemed necessary by the Security Council and members of the United Nations.

The United Nations already has an established means to judge violations of established law, and the same framework should be used for cyberspace agreements. Violation of the Tallinn Manual should be ruled on by the United Nations Security Council, at which point any response, up to and including a use of force under Article 51, is a potential outcome. This method of enforcement is also suggested by the Tallinn Manual itself.[59]

9 Where Adoption Brings the International Community

The solution is neither complete nor final, but as with all law, we must set up a solid base with which to work and progress over time. The established international law made preparation for the age of the Internet possible, and in the same way, the Tallinn Manual sets the stage for the tools we need in decades to come, as the world grows more reliant on the Internet.

The ability of a cyber operation to be classified as an armed attack, and by extension the possibility of responding with military force under Article 51, is quite significant and can lead to a severe escalation during times of conflict. This is appropriate, though, as the world's critical infrastructure becomes increasingly online and cyber weapons increase in ability and complexity constantly. It is an antiquated notion that military arms must explode, shoot, or even directly cause bloodshed. It

59. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 66. See rule 18.

is important that States are granted the means to protect their cyberspace.

When asked about threshold of attacks and the significant damage that can be inflicted through cyberspace, Schmitt implies he believes the standards for classifying armed attacks in cyberspace will also evolve in coming years:

> I anticipate that we'll see a lot of thresholds coming down that will allow States to respond more vibrantly to cyber attacks that might not be possible under the law as we found it.[60]

Overall, the conclusions of the Tallinn Manual feel just and reasonable. Many of the issues not directly resolved are complex and likely require analysis on a case-by-case basis over a number of years, all the while the laws will be consistently developed and solidified. Achieving concurrence on acceptable cyber acts will likely prove challenging, but it is a necessary aspect as the cyber space continues to evolve in ways not yet considered.

Despite any unintentional bias introduced by the Experts' NATO background, their effort to apply already agreed upon international law provides confidence in the international arena that the international community, collectively, is continuing to act in cyberspace in the spirit of previously established and accepted laws.

Another notable, though indirect, potential effect of an established treaty based on the rules of the Tallinn Manual is the preservation of an open Internet within and among sovereign States. As the States of the world realize the potential damage inflicted by attacks launched via cyberspace they are exploring measures to regulate and police domestic networks, often at the expense of some traditional Internet freedoms.[61] For example, while the United States hasn't passed significant regulation on networks and software to defend against cyber attacks, there are many arguments to

60. Gollom, "Are there international rules for cyberwarfare?" See paragraph 23.

61. John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, 1996, accessed November 29, 2014, `https://projects.eff.org/~barlow/Declaration-Final.html`. The Electronic Frontier Foundation requested the sovereignty of cyberspace be respected by the world's governments. The demands of State infrastructure on the Internet have changed this landscape, but it may still be possible to preserve these ideals.

establish such proposals. Richard Clarke, a leading adviser on cyber security in the United States political space, is a proponent for greater regulations and had this to say of regulating the private sector:

> ... industry only responds when you threaten regulation. If industry doesn't respond (to the threat), you have to follow through.[62]

The openness of the Internet makes it a space unlike any other, and the immediate censorship performed by totalitarian States proves it is a strong tool for protecting human rights.[63] So, while an indirect effect, the potential preservation of a healthy, open cyberspace should not be understated, and agreeing to the rules of the Tallinn Manual could help avoid heavy-handed regulations.

10 Conclusion

The Tallinn Manual offers help in an area that the international community needs in coming decades. There have been multiple recent occasions where cyber operations have wreaked havoc on States' infrastructure, and the potential consequences are likely to escalate as the world becomes more connected. The risks are heightened by the certainty that offensive measures are continuously advancing. It is crucial that States start taking the reasonable measures to protect themselves and their citizens.

An application of the Tallinn Manual to the events surrounding the Stuxnet Worm demonstrated that the work of Schmitt and the Experts have come a great way in correlating existing law to operations in cyberspace. The Tallinn Manual is not

62. Carrie Kirby, "Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in cybersecurity," SF Gate, 2005, accessed November 29, 2014, `http://www.sfgate.com/busin/ess/article/Former-White-House-aide-backs-some-Net-regulation-2729985.php`

63. Joel Hruska, "Turkey becomes first nation to block Google DNS, claims Twitter is groveling at its feet," Extreme Tech, 2014, accessed November 30, 2014, `http://www.extremetech.com/internet/179074-turkey-becomes-first-nation-to-block-google-dns-claims-twitter-is-groveling-at-its-feet`. Turkey's Prime Minister censored Twitter and blocked Google's DNS after news of a potential scandal began spreading online.

without technical and political hurdles, but it is ultimately worthy of serving as a basis in establishing the first international laws for cyberspace. The collective international community has an opportunity to collaborate to work through the issues presented, ultimately offering a safer and more fruitful cyberspace for all to utilize.

An agreement adhering to the rules of the Tallinn Manual would not only help provide protection to the infrastructure and sovereignty of participating States, it could encourage a continued free and open Internet. The international community can look forward to a healthy, global cyberspace with help from the Tallinn Manual and continued discussions on permissible and responsible cyber operations and online stewardship.

Since the Tallinn Manual is inspired by already accepted international laws, it can confidently be proposed as the beginning of a path forward. The Tallinn Manual provides a strong foundation of which the international community should take advantage.

Bibliography

"More Stuxnet: US-Israeli Computer Virus Infected Russian Civilian Nuclear Power Plants." 21st Century Wire. November 2013. Accessed October 11, 2014. http://21stcenturywire.com/2013/11/13/more-stuxnet-us-israeli-made-virus-infected-russian-civilian-nuclear-power-plants/.

Charter of the United Nations. United Nations, October 1945. Accessed October 11, 2014. http://www.un.org/en/documents/charter/.

Clarke, Richard, and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to do About it*. New York: HarperCollins Publishers, 2010. ISBN: 978-0-06-196224-0.

Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. International Committee of the Red Cross (ICRC), October 1907. Accessed October 11, 2014. https://www.icrc.org/ihl/INTRO/200?OpenDocument.

Edgar, Timothy. "Cyberwar (1): the use of force in cyberspace." *presentation. Boston University, Cybersecurity and Policy.* (2014).

Gollom, Mike. "Are there international rules for cyberwarfare?" CBC News. March 2013. Accessed October 19, 2014. http://www.cbc.ca/news/world/are-there-international-rules-for-cyberwarfare-1.1323638.

Hollis, Duncan B. "Why States Need an International Law for Information Operations." *Legal Studies Research Paper Series* 1023 (2008). Accessed November 24, 2014. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1083889.

Hruska, Joel. "Turkey becomes first nation to block Google DNS, claims Twitter is groveling at its feet." Extreme Tech. 2014. Accessed November 30, 2014. http://www.extremetech.com/internet/179074-turkey-becomes-first-nation-to-block-google-dns-claims-twitter-is-groveling-at-its-feet.

Kirby, Carrie. "Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in cybersecurity." SF Gate. 2005. Accessed November 29, 2014. http://www.sfgate.com/busin/ess/article/Former-White-House-aide-backs-some-Net-regulation-2729985.php.

Koh, Harold Hongju. "International Law in Cyberspace." *Harvard International Law Journal Online* 54 (2012). Accessed October 11, 2014. http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.

Norris, Michael J. "The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace." Student Pulse. 2013. Accessed November 22, 2014. http://www.studentpulse.com/articles/775/the-law-of-attack-in-cyberspace-considering-the-tallinn-manuals-definition-of-attack-in-the-digital-battlespace.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin. "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities" (2009). Accessed November 29, 2014. http://www3.nd.edu/~cpence/eewt/Owens2009.pdf.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I). International Committee of the Red Cross (ICRC), June 1977. Accessed October 11, 2014. https://www.icrc.org/ihl/WebART/470-750065.

Schmitt, Micael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York: Cambridge University Press, 2013.

"Stuxnet 0.5: Distrupting Uranium Processing at Natanz." last modified January 2014. Accessed October 11, 2014. http://www.symantec.com/connect/blogs/stuxnet-05-disrupting-uranium-processing-natanz.

Walrond, David Albright; Paul Brannan; Christina. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" *Institute for Science and International Security* (2010). Accessed November 23, 2014. http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf.

Waxman, Matthew C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *Yale Journal of International Law* 36, no. 2 (2013). Accessed October 11, 2014. http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf.

Zetter, Kim. "Legal Experts: Stuxnet Attach on Iran Was Illegal 'Act of Force'." Wired. March 2013. Accessed October 6, 2014. http://www.wired.com/2013/03/stuxnet-act-of-force/.