Applicability and Adoption of the Tallinn Manual

Considering Legality and Repercussions of the Stuxnet Worm

Steve Jarvis

November 29, 2014

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. The offensive capabilities and risks are continually increasing 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 for international conflict. The United Nations was organized in 1942 and the Geneva Conventions in 1949.[1] [2] These organizations founded treaties that defined 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 unwarranted kinetic 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 as such, the laws consider only kinetic warfare. 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, 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 the established, kinetic laws to this modern, cyber battlefield.[3] The need

1. United Nations, "History of the United Nations," 2013, accessed November 2, 2014, `http://www.un.org/en/aboutun/history/`

2. Phillip Spoerri, "The Geneva Conventions of 1949: origins and current significance," 2009, accessed November 2, 2014, `https://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-120809.htm`

3. Micael N. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare* (2013). See page 18, paragraph 2.

for such a set of laws grows more apparent with each passing year.

The goal of this report is to examine whether the Tallinn Manual is suitable for official adoption by the international community. To make this determination, its applicability to real life actions, particularly the Stuxnet worm, will be considered, as well as the Tallinn Manual's political hurdles. If successful, the Tallinn Manual's official adoption could help to ensure the safety and security of all states in coming years.

The Current International Law

Today, 193 of 196 countries of the world are members of the United Nations. 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's considered legal.[4] Since there are no laws established for cyber operations and little or no correlation to kinetic laws, there can be no repercussion from the international community.

Differing interpretations of how established laws regulate cyber activity results in dissension among states and incompatible policies. For example, there are no accepted answers on what constitutes illegal activity, whether it's even possible to exert a use of force or launch an armed attack online, or what repercussions would be appropriate if it is possible.[5]

With no consensus on what constitutes permissible cyber activity, there can be no agreement on suitable international laws or treaties to govern behavior. By extension, there are also no means to reprimand states or enforce acceptable behavior in cyberspace.

4. Lotus Case, "The Lotus Case (France vs Turkey)," 1927, accessed November 23, 2014, http://ruwanthikagunaratne.wordpress.com/2012/07/27/lotus-case-summary/

5. 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), http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf, 431-435.

Why The International Community Needs to Adopt Cyber Agreements

In 2007, Estonia chose to relocate a bronze statue of a Soviet soldier to quell the dispute between Estonian nationalists, who saw the statue as a symbol of oppression, and a Russian ethnic group, who considered its 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.[6]

The events in Estonia demonstrate the capabilities of even simple cyber attacks, and the serious detrimental effects for states connected as Estonia prove the concern is significant.[7]

The world's situation is only growing more dire as states become more reliant on cyberspace. The worlds' critical infrastructure, including power grids, water treatment plants, financial institutions and health care equipment, is growing increasingly connected or reliant on the Internet. Citizens and governments rely 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.

The new realm of cyberspace provides a battleground the states of the world are just beginning to explore. New attacks are constantly developed and far outpace states' abilities to defend against them. It's crucial that the international community establish rules protecting states' cyberspace.

6. Richard Clarke, *Cyber War. The Next Threat to National Security and What to do About it.* (2010), 12-16.

7. ibid., 13. In at least 2007, Estonia ranked ahead of even the United States with regards to Internet use for every day tasks.

The Tallinn Manual

The Tallinn Manual was an effort to address growing concern over the threats posed over cyberspace. National cyber security is an issue many countries cite as an utmost priority, including the United Kingdom, the United States, Russia and Canada.[8] The goal of the Tallinn Manual was to fill the void in the international community by correlating existing international laws on conflict to cyberspace and provide some non-binding guidance on what operations are within the bounds of the law.[9]

The North Atlantic Treaty Organization (NATO) encouraged and supported the project. Michael Schmitt 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. The result is a set of 25 Rules and many additional thoughts, issues and sticking points in the form of commentary throughout the document. The rules cover such things as defining a violation of sovereignty and jurisdiction, categorizing a use of force, defining a cyber (armed) attack, and special considerations for civilians.[10] All of the conclusions reached by the Tallinn Manual are inspired by established international law, often specifically the United Nations Charter or 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 stated intentions were to construct a non-binding document, practice has proved 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, said that "[...] in reality, if you want to determine the legality of a cyber operation, you reach for the Tallinn Manual."[11]

8. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, 16-17
9. ibid., 16, para. 1.
10. ibid. See Rules 1, 2, 10-11, 30 and 32, respectively.
11. Timothy Edgar, "Cyberwar (1): the use of force in cyberspace," *presentation. Boston University, Cybersecurity and Policy.* (2014)

The Stuxnet Worm

Stuxnet was a revolutionary cyber attack in 2010 that sabotaged the programmable logic controllers (PLCs) at Iran's Natanz nuclear enrichment facility. 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.[12] [13]

Despite the destructive chaos actually happening in the system, the Stuxnet malware would continuously deliver positive reports to the operators, assuring them that operation was going safely and as planned. The human operators capable of intervening 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.

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 a private group of citizens or hacktivists. There were almost immediately strong points made that pointed towards a state backing. Stuxnet's level of technical difficulty was uncontested by any cyber attack prior (and maybe since), and it was not only very complex, it was also extremely expensive.[14] More recently however, solid evidence has surfaced proving it was in fact executed by a nation-state, particularly a collaboration between the United States and Israel.[15] Stuxnet is now widely accepted to have been orchestrated by a nation-state, which qualifies it as a politically motivated operation and subject to the international laws of conflict.

Stuxnet exists amidst many controversial cyber operations over the past decade,

12. Symantec, "Stuxnet 0.5: Distrupting Uranium Processing at Natanz," 2013, accessed October 11, 2014, http://www.symantec.com/connect/blogs/stuxnet-05-disrupting-uranium-processing-natanz

13. David Kushner, "The Real Story of Stuxnet," 2013, accessed October 11, 2014, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/

14. Ben Flanagan, "Former CIA Chief Speaks Out on Iran Stuxnet Attack," 2011, accessed October 11, 2014, http://www.thenational.ae/business/industry-insights/technology/former-cia-chief-speaks-out-on-iran-stuxnet-attack

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

yet it still deserves much focus when considering cyber operations and international law on armed conflict, because it offers, arguably, the most likely candidate of a cyber-only operation to be considered a use of force or an armed attack as define in the Charter of the United Nations. Prime alternative operations include Flame Malware and Russia's cyber attack on Georgia.[16] [17] Flame was used for only espionage, and that is generally considered legal under international law.[18] 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.[19] These operations raise many interesting questions of their own, but the overall conclusions are unsurprising and generally uncontroversial.

The enrichment facility at Natanz was not connected to the Internet. Despite these precautions taken against cyber attack, the facility proved to still be vulnerable. Stuxnet was likely initially introduced to the target environment by an infected USB drive.[20] The route to its final target is unknown, but it's likely the virus crossed an unknown number of state boundaries through the Internet infrastructure..

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 could have been accomplished with a kinetic attack.[21]

16. Richard Steinnon, "Flame's MD5 collision is the most worrisome security discovery of 2012," 2013, accessed October 21, 2014, `http://www.forbes.com/sites/richardstiennon/2012/06/14/%20flames-md5-collision-is-the-most-worrisome-security-discovery-of-2012/`

17. David J. Smith, "Russian Cyber Strategy and the War Against Georgia," 2014, accessed October 11, 2014, `http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia`

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

19. ibid., page 94, para. 6 and ibid. See rule 20.

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

21. 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), `http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf`

As is 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 computers in more than a dozen countries.[22] Eugene Kapersky, founder of the Russian security company Kapersky Labs, claimed the virus even infected the Russian nuclear facilities. He is not alone in these claims, either, with as many as 15 other industrial complexes around the world believed to have been infected by Stuxnet.[23]

The distinction here between civilian and nuclear or industrial facility infection is significant, 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.[24] Infected civilians would not only be unaware, they would be at no risk of danger whatsoever. The infected industrial facilities, however, would likely suffer grave damage, just as Iran's facility is believed to have experienced at Natanz.[25]

Where Traditional Law is Not Enough

Cyber operations like Stuxnet are unlike any with which the world has yet dealt. The executions of these attacks raise many questions where guidance from a suitable guide 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?

22. Aleksandr Matrosov, "Stuxnet Under the Microscope," page 15.
23. Chris von Eitzen, "Stuxnet Also Found At Industrial Plants in Germany," 2010, accessed November 18, 2014, `http://www.h-online.com/security/news/item/Stuxnet-also-found-at-industrial-plants-in-Germany-1081469.html`
24. ibid.
25. Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?"

4. Which states can be held accountable in such an event?
5. If international laws were broken, what retaliation is appropriate, and how might it be enforced?

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 laws would be that prohibiting a use of force, set forth by Article 2(4) of the United Nations Charter. It 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.[26]

Regarding only kinetic law, Stuxnet's classification as a use of force is not clear, however. Though the distinction is not defined in the Charter, 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.

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 a use of force to be effectively the same as an armed attack.[27] Supposing the international community accepts the view that a cyber attack does coincide a use of force, this issue is the same as that of a use of force, but any consensus for a further definition of the term is unlikely.

26. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See Rule 11.
27. ibid., page 17, para. 3.

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.[28] This definition is rather limiting and seems to exclude any cyber attacks by its very nature. Similarly, most all traditional definitions of armed conflict require some kind of physical violence.[29] There have been no cyber-only attacks to date that fit this description, and it very well may be impossible simply by definition.

Furthermore, the any conclusion to this issue is likely more complex than a simple "yes or no" answer. The infections of civilian machines could be categorized differently than infections of state-owned infrastructure. Civilian infections were not necessarily harmful, and mere infection may not equate to a cyber attack in either case, even when the victim is civilian.

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's not clear the same applies to malware, which often has less directly devastating results.[30] With malware there is little danger of immediate harm relative to indiscriminate kinetic attacks, such as chemical warfare or the bombing of a hospital.

The stakes are far higher in the case of industry systems infected with Stuxnet, however. Infection at locations operating the targeted Siemens machines are subject to the same risk and harm as the intended target, Iran.

28. **usVsNicaraguq**

29. Kenneth W. Dam William A. Owens 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`, page 253, para. 2.

30. Geneva Convention, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)* (1977), `https://www.icrc.org/ihl/WebART/470-750065`

Accountability

It seems obvious that, if decided to be in violation of any laws, the sponsors of the malware and its authors could 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.[31] Is it legal to move malware through the infrastructure of neutral states, and can those states be held responsible for allowing it?

Retaliation and Defense

Equally important is the issue of enforcement and reprimanding states who are deemed in violation of any accepted law. The United Nations Charter allows for a use of force as self defense in Article 51, but some question whether a military response to a cyber attack is reasonable.[32]

A kinetic operation 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, and this has potentially devastating consequences for victim states.[33] [34] 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, or when a final decision cannot be reached at all.

31. Hague Convention, *Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land.* (1907), https://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=71929FBD2655E558C12563CD002D67AE. See Articles 2 and 5.

32. United Nations, *Charter of the United Nations* (1945), http://www.un.org/en/documents/charter/index.shtml. See Article 51.

33. Andrew Johnson, "Ban Ki Moon Laments 'Embarrassing Paralysis' of U.N. Security Council," September 2013, accessed November 29, 2014, http://www.nationalreview.com/corner/357974/ban-ki-moon-laments-embarrassing-paralysis-un-security-council-andrew-johnson

34. Michele Kelemen, "U.N. Security Council Deadlocked over Kosovo," December 2007, accessed November 29, 2014, http://www.npr.org/templates/story/story.php?storyId=17441680

Using the Tallinn Manual to Analyze the Stuxnet Worm

Now we turn to the Tallinn Manual to resolve the issues applying the existing laws to cyberspace,. We'd like to determine whether the Tallinn Manual is an effective tool in practice by finding whether it proves useful when evaluating Stuxnet.

Regarding 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."[35] 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.[36] The group of experts unanimously concluded Stuxnet to be a use of force, and therefore in violation of Article 2(4) of the United Nations Charter.[37] Stuxnet also directly violates at least the sovereignty set forth in Rule 1 of the Tallinn Manual.[38]

The manual goes on to say that the experts were unanimous in determining cyber operations alone might qualify as armed conflict.[39] Tallinn Manual states:

> An armed conflict exists whenever there are here are hostilities, which may include or be limited to cyber operations, occurring between two or more States.[40]

Tallinn Manual also comments directly that the experts were divided on whether Stuxnet qualified as an "armed attack".[41] Some experts felt it was justified as anticipatory self-defense.[42]

35. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*
36. ibid. See page 51.
37. Kim Zetter, "Legal Experts: Stuxnet Attach on Iran Was Illegal 'Act of Force'," 2013, accessed October 6, 2014, `http://www.wired.com/2013/03/stuxnet-act-of-force/`
38. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See Rule 1.
39. ibid. See Rule 22, comment 15.
40. ibid. See Rule 22.
41. ibid. See Rule 22, comments 14 and 15.
42. ibid. See Rule 13, comment 13.

This finding alone is significant, because it enables retaliation under Article 51 to a cyber attack within the realm of possibility. This directly contradicts other interpretations of the Charter that reserve an armed attack for armed military operation.[43]

Indiscriminate methods of cyber war are prohibited.[44] The infection of civilians' computers (might[45]) not violate this, because despite infection, the attack was performed only on specific Siemens systems (not civilian).[46] That is assuming, of course, the mere installation of malware does not amount to an attack. It's not clear how the Tallinn Manual would categorize such a thing.

If Kapersky's claims[47] that Stuxnet later infected Russian nuclear sites are true, however, Stuxnet did violate this rule, since Stuxnet was decidedly a cyber attack and this would prove it was not limited in its effects as required by the law of armed conflict.[48]

There were also a number of issues on which the Tallinn Manual was not conclusive.

As mentioned, Tallinn Manual is clear that cyber operations alone could amount to an armed attack,[49] but provide little means to determine whether a specific operation crosses that threshold, or how an armed attack relates to a use of force (though that is a standing problem with kinetic warfare, just the same). Schmitt says these specifics were intentionally not included in the Tallinn Manual.[50]

Schmitt claimed that:

43. 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.com/sol3/papers.cfm?abstract_id=1083889`

44. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See Rule 43.

45. ibid. See Rule 1, comment 6.

46. Kushner, "The Real Story of Stuxnet"

47. 21st Century Wire, "More Stuxnet: US-Israeli Computer Virus Infected Russian Civilian Nuclear Power Plants," 2013, accessed October 11, 2014, `http://21stcenturywire.com/2013/11/13/more-stuxnet-us-israeli-made-virus-infected-russian-civilian-nuclear-power-plants/`

48. Convention, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*

49. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, rule 22.

50. Mike Gollom, "Are there International Rules for Cyberwarfare? Existing laws apply to cyberweapons.," 2013, accessed October 19, 2014, `http://www.cbc.ca/news/world/are-there-international-rules-for-cyberwarfare-1.1323638`

> [...]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.[51]

The Tallinn Manual does offer a definition for a cyber attack, 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."[52] 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. There was little physical damage done, compared traditional, kinetic force.[53]

There are also issues with immediacy that were not matters in kinetic warfare. Iran didn't know it was being attacked until the threat was over, and with no imminent or current attack there is no justification for an armed response under Article 51.[54]

Who can be held responsible in a cyber attack? Iran obviously had jurisdiction in Stuxnet.[55] What of neutral states whose infrastructure was used to transfer Stuxnet? Laws on kinetic warfare imply they can be held accountable for transferring munitions. The Hague Conventions itself limits a neutral state's obligation to restrict the combatant use of telephone or wireless cables.[56] Tallinn Manual states it must not *knowingly* allow conflicting parties to use its infrastructure.[57] The experts were split on whether that permits neutral states to passively allow such transmission.[58]

What self-defense is legal when it's unclear whether an operation could be clas-

51. Gollom, "Are there International Rules for Cyberwarfare? Existing laws apply to cyberweapons.," para 4.
52. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare.* See Rule 30.
53. John Leyden, "Cyberwar Playbook Says Stuxnet May Have Been 'Armed Attack'," 2013, accessed October 26, 2014, `http://www.theregister.co.uk/2013/03/27/stuxnet_cyberwar_rules/`
54. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare.* See rule 15.
55. ibid. See Rule 2
56. Convention, *Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land.* See article 8.
57. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare.* See rule 93.
58. ibid. See rule 93, comments 5 and 6.

sified as an "armed attack", or when the Security Council has not yet reached an agreement?

Adopting the Tallinn Manual

The Tallinn Manual does an exceptional job of applying existing international law to the age of the Internet. This is a great foundation, but dealing effectively with this era of cyber operations requires 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.[59] 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 states' sovereignty. This was apparent in Estonia, as victims were unable to access their own funds to purchase basic needs. Attacks that have a significant effect on a state's infrastructure should be considered armed attacks, even without direct injury, violence or death.[60]

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 definition of a 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.[61]

59. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See Rule 30.

60. William A. Owens and Lin, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," page 254.

61. Michael J. Norris, "The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace," 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`

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 which 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. When does an operation cross the threshold from an inconvenience to an attack? Is the mere installation of malware a violation of soveriegnty? When is a state sufficiently involved with the creation or distribution of an attack to warrant responsibility? Much of this lack of detail in the Tallinn Manual can actually be regarded as a strength through flexibility. Much of the corresponding gray area is equally undecided in kinetic conflict, terribly complex and, in cyberspace, likely to evolve at a rapid pace. 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 nature of the laws allow for interpretation and for a continued 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 Internet may be accompanied by a Western bias. Further, those states usually at odds with NATO will be unlikely to consider a set of rules built solely by NATO.

Some of the currently conflicting issues (responsibility of neutral states, 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, the current members of the United Nations should be encouraged to ratify a treaty adopting adherence to the rules set forth by the Manual.

The agreement should adopt the Tallinn Manual as a starting point for ruling on international cyber conflict and used as a bases 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 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 agreements, 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 retaliation, up to and including that under Article 51, is a potential outcome. This is also suggested in the Tallinn Manual itself.[62]

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 increasingly more reliant on the Internet. Schmitt implied he believes the standards for classifying armed attacks in cyberspace will evolve in coming years:

62. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, rule 18.

> 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.[63]

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 grows increasingly more 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.

The conclusions of the Tallinn Manual feel reasonable. Many of the issues not directly resolved are complex and likely require analysis on a case-by-case basis. The issues that were directly resolved are not only founded on accepted international law, but feel just when applied to the cyber world.

Achieving concurrence on acceptable cyber acts will likely prove challenging, but it is a necessary feature 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 cyber space in the spirit of previously established and accepted international laws.

Another notable, though indirect, potential effect 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.[64] For example, while the United States hasn't

63. Gollom, "Are there International Rules for Cyberwarfare? Existing laws apply to cyberweapons.," para 23.

64. John Perry Barlow, "A Declaration of the Independence of Cyberspace," 1996, accessed November 29, 2014, `https://projects.eff.org/~barlow/Declaration-Final.html`. The

passed significant regulation on networks and software to defend against cyber attacks, there are many arguments to establish such proposals. Richard Clarke, a leading adviser on cyber security in the US political space, is a proponent for greater regulations.

> [...] industry only responds when you threaten regulation. If industry doesn't respond (to the threat), you have to follow through.[65]

The openness of the Internet makes it a space unlike any other, and the immediate attention it gets from totalitarian states proves it is a strong tool for protecting human rights.[66] While an indirect effect, the potential preservation of this space should not be understated.

Conclusion

The Tallinn Manual offers help in an area which the international community much needs it in coming decades. There have been multiple recent occasions where cyber operations have wrecked havoc on states' infrastructure, and the potential consequences are likely to only 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 measures to protect themselves and others.

The Tallinn Manual is not without technical and political hurdles, but it is ultimately worthy of official acceptance in founding international law and standards. The collective international community has an opportunity to collaborate and work through the issues presented, ultimately offering a safer and fruitful cyberspace for all to utilize.

Electronic Frontier Foundation requested the sovereignty of cyberspace be respected by the world's governments. The effects of state infrastructure via the Internet have changed this landscape, but it may still be possible to preserve these ideals.

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

66. **TODO turkey comes to mind**

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. Alternatives to agreements on fair and permitted use might include strict regulation and policing by independent states. This would not only be the demise of a cherished characteristic of cyberspace, it would likely have drastic effects for the oppressed citizens of the world.

The international community can look forward to a healthy, global Internet with help from the Tallinn Manual and continued discussions on permissible and responsible online operations and stewardship.

Since the Tallinn Manual is inspired by already accepted international laws, it can confidently be regarded as the beginning of a path forward. It is a great work and should be taken advantage of.

Bibliography

Aleksandr Matrosov, et al. "Stuxnet Under the Microscope." 2010. Accessed November 16, 2014. http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

Barlow, John Perry. "A Declaration of the Independence of Cyberspace." 1996. Accessed November 29, 2014. https://projects.eff.org/~barlow/Declaration-Final.html.

Case, Lotus. "The Lotus Case (France vs Turkey)." 1927. Accessed November 23, 2014. http://ruwanthikagunaratne.wordpress.com/2012/07/27/lotus-case-summary/.

Clarke, Richard. *Cyber War. The Next Threat to National Security and What to do About it.* 2010.

Convention, Geneva. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I).* 1977. https://www.icrc.org/ihl/WebART/470-750065.

Convention, Hague. *Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land.* 1907. https://www.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=71929FBD2655E558C12563CD002D67AE.

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

Eitzen, Chris von. "Stuxnet Also Found At Industrial Plants in Germany." 2010. Accessed November 18, 2014. http://www.h-online.com/security/news/item/Stuxnet-also-found-at-industrial-plants-in-Germany-1081469.html.

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

Flanagan, Ben. "Former CIA Chief Speaks Out on Iran Stuxnet Attack." 2011. Accessed October 11, 2014. http://www.thenational.ae/business/industry-insights/technology/former-cia-chief-speaks-out-on-iran-stuxnet-attack.

Gollom, Mike. "Are there International Rules for Cyberwarfare? Existing laws apply to cyberweapons." 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.

Johnson, Andrew. "Ban Ki Moon Laments 'Embarrassing Paralysis' of U.N. Security Council." September 2013. Accessed November 29, 2014. http://www.nationalreview.com/corner/357974/ban-ki-moon-laments-embarrassing-paralysis-un-security-council-andrew-johnson.

Justice, International Court of. "CASE CONCERNING THE MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA)." 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.

Kelemen, Michele. "U.N. Security Council Deadlocked over Kosovo." December 2007. Accessed November 29, 2014. http://www.npr.org/templates/story/story.php?storyId=17441680.

Kirby, Carrie. "Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in cybersecurity." 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). http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.

Kushner, David. "The Real Story of Stuxnet." 2013. Accessed October 11, 2014. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/.

Leyden, John. "Cyberwar Playbook Says Stuxnet May Have Been 'Armed Attack'." 2013. Accessed October 26, 2014. http://www.theregister.co.uk/2013/03/27/stuxnet_cyberwar_rules/.

Nations, United. *Charter of the United Nations*. 1945. http://www.un.org/en/documents/charter/index.shtml.

———. "History of the United Nations." 2013. Accessed November 2, 2014. http://www.un.org/en/aboutun/history/.

———. "Members." 2002. Accessed November 18, 2014. http://www.un.org/en/members/.

Norris, Michael J. "The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace." 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.

Schmitt, Micael N. *Tallinn Manual on International Law Applicable to Cyber Warfare*. 2013.

Smith, David J. "Russian Cyber Strategy and the War Against Georgia." 2014. Accessed October 11, 2014. http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia.

Spoerri, Phillip. "The Geneva Conventions of 1949: origins and current significance." 2009. Accessed November 2, 2014. https://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-120809.htm.

Steinnon, Richard. "Flame's MD5 collision is the most worrisome security discovery of 2012." 2013. Accessed October 21, 2014. http://www.forbes.com/sites/richardstiennon/2012/06/14/%20flames-md5-collision-is-the-most-worrisome-security-discovery-of-2012/.

Symantec. "Stuxnet 0.5: Distrupting Uranium Processing at Natanz." 2013. 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). 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). http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf.

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.

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

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