Applicability and Adoption of the Tallinn Manual

Considering Legality and Repercussions of the Stuxnet Worm

Steve Jarvis

November 16, 2014

Introduction

In the wake of the second World War, the international community recognized the necessity of establishing agreements for international conflict. The United Nations was organized in 1942[1] and the Geneva Conventions in 1949.[2] These communities founded treaties that defined international laws for entering into conflict (*jus ad bellum*) and behavior during conflict (*jus in bello*).

Those agreements were established with only kinetic warfare in mind. The growing prevalence of cyber operations is pushing the boundaries of acceptable international behavior, and the international community has little means to deal with it. Cyber actions rarely have a direct or obvious kinetic counterpart with which to compare, and without established norms, states continue to push the boundaries, limited by technical capabilities rather than legal or ethical standards. The Tallinn Manual aims to fill the void of defined international law or agreements when it comes to cyber activity.[3]

The goal of this report is to examine whether the Tallinn Manual is suitable for adoption in the international community by considering its applicability to real life actions, particularly the Stuxnet worm. Its adoption could help to ensure the safety and security of all in the coming years.

Our Current Situation

As aforementioned, the established international law deals only with kinetic warfare. There is no international policy establishing how states can operate militarily online. Differing interpretations of established laws results in dissension among states, with no clear answers on how to classify illegal online activity, whether it's

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), page 18, para 2.

possible to launch an armed attack in cyber space[4], or whether it's the position of the UN to interfere in the online space.

The diverged viewpoints run wide. With no consensus on what constitutes permissible cyber activity, there can be no agreement on suitable international laws or treaties. By extension, there are also no means to reprimand states or enforce acceptable behavior in cyberspace. This must be overcome in order to apply the international continuity provided by traditional agreements to the age of the internet.

Why This Needs to Change

States of the world are growing increasingly more reliant on the internet. The worlds' critical infrastructure, including power grids, water treatment operations, financial institutions and health care equipment, is growing increasingly more reliant on the Internet. Citizens and governments rely on these services to maintain a healthy and safe standard of living. Sometimes critical infrastructure is connected directly to the public Internet. 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 as the physical world surrounding. The international community needs to establish rules protecting states' cyberspace.

The Tallinn Manual

The Tallinn Manual was created to fill the void in international law when it comes to cyberspace. It was the effort of an international group of experts, upon encouragement from the North Atlantic Treaty Organization (NATO), to correlate existing international laws on conflict, largely the Geneva Conventions and United

4. 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`, pages 431-435.

Nations Charter, to cyberspace.[5]

Over a period of three years, legal experts from many NATO states discussed the complications of cyber operations and how to apply the 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 Stuxnet Worm

Stuxnet was a cyber attack in 2010 to sabotage the programmable logic controllers (PLCs) at the Iran nuclear enrichment facility and delay Iran's potential development of nuclear weapons.[6] It did this by causing the centrifuges that spin uranium to spin out of control and ultimately destroy themselves.[7] All the while, the hardware would send positive reports that operation was going safely and as planned, so the human operators had no indication there was an issue, much less one so dire.

Stuxnet was not only extremely technically complex, it was also extremely expensive.[8] As such, it's believed to have been conducted by a nation-state, which qualifies it as a politically motivated operation.

There have been many controversial cyber operations in the past decade. Stuxnet deserves the focus when considering regulation because it offers, arguably, the most complex situation and is the most likely candidate of a cyber-only operation to be considered a use of force or an armed attack. Prime alternative operations include

5. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, page 16, para 1

6. 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`

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

8. 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`

Flame Malware[9] and Russia's cyber attack on Georgia.[10] Flame was used for only espionage, and that is generally considered legal under international law.[11] Russia's cyber attack on Georgia, conversely, was used to further a kinetic attack and falls clearly into the category of armed conflict.[12] These conclusions are unsurprising and do not feel controversial.

The enrichment facility at Natanz was not connected to the Internet. Despite these precautions taken against cyber attack, it proved to still be vulnerable. It is believed to have been initially introduced to the target environment by an infected USB drive.[13] En route to its final target, though, it is unknown how many state boundaries this cyber weapon crossed.

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 refused to comment on whether it suffered damage from Stuxnet. However, it's widely held that their nuclear program did suffer significant setbacks, on the order of what could have been accomplished with a kinetic attack.[14]

As is with many worms, Stuxnet proved difficult to control. It leaked into the wild and infected TODO potentially hundreds of thousands civilian computers and, Kapersky claimed, even infected the Russian nuclear facilities. The distinction between civilian and nuclear facility infection is significant here, 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

9. 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/`

10. 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`

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

12. ibid., page 94, para 6 and ibid., rule 20.

13. TODO, "TODO," TODO, accessed November 16, 2014, `http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf`. See page 8.

14. "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`

if it wasn't on specific Siemen's PLCs it would sit dormant.[15] Infected civilians would not only be unaware, they would be at no risk of danger whatsoever. The Russian nuclear facility, however, would likely suffer grave damage, just as Iran's facility at Natanz.

Cyber Issues Where Traditional Law is Lacking

Stuxnet and other cyber operations are unlike any ever seen. The execution of attacks such as Stuxnet raise many questions where guidance from a suitable guide is desired to determine which laws were broken, how severely they were broken, and what response might be warranted.

To start, 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 set forth by Article 2(4) of the UN Charter, which 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.[16]

Stuxnet's classification as a use of force is not clear, though. A traditional use of force involves military force, though that distinction is not defined in the Charter.

The Stuxnet worm leaked into the wild and infected civilian devices, Kapersky even claimed it infected Russian nuclear facilities.[17] A failure to control weapons in kinetic warfare is outlawed as indiscriminate, but it's not clear that's what this

15. TODO, "TODO." TODO

16. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See Rule 11.

17. 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/`

leak equates to.[18] The civilian infection was not necessarily harmful, and does mere infection equate to an attack in cyberspace?

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.[19] Is it legal to move malware through the infrastructure of neutral states, and can those states be held responsible for allowing it?

Equally important is the issue of enforcement and reprimanding states who are deemed in violation of any accepted law. The UN Charter allows for a use of force as self defense in Article 51, but could a military response to a computer hack be reasonable?[20]

Applying the Tallinn Manual to the Stuxnet Worm

Now that there have been sufficient, specific issues raised with the applicability of existing law to cyberspace we turn to the Tallinn Manual to help. 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."[21] 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

18. 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`

19. 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.

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

21. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*

which Stuxnet clearly violates.[22] The group of experts unanimously concluded Stuxnet to be a use of force, and therefore in violation of Article 2(4) of the UN Charter.[23] Stuxnet also directly violates at least Rule 1 of the Tallinn Manual.[24]

The manual goes on to say that the experts were unanimous in determining cyber operations alone might qualify as armed conflict.[25] 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.[26]

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.[27]

Tallinn Manual also comments directly that the experts were divided on whether Stuxnet qualified as an "armed attack".[28] Some experts felt it was justified as anticipatory self-defense.[29]

Indiscriminate methods of cyber war are prohibited.[30] The infection of civilians' computers (might[31]) not violate this, because despite infection, the attack was performed only on specific Siemens systems (not civilian).[32] 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[33] that Stuxnet later infected Russian nuclear sites are true,

22. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See page 51.
23. 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/`
24. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See Rule 1.
25. ibid. See Rule 22, comment 15.
26. ibid. See Rule 22.
27. **TODO that paper you downloaded from http://papers.ssrn.com/sol3/papers.cfm?abstract˙id=1**
28. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See Rule 22, comments 14 and 15.
29. ibid. See Rule 13, comment 13.
30. ibid. See Rule 43.
31. ibid. See Rule 1, comment 6.
32. Kushner, "The Real Story of Stuxnet"
33. Wire, "More Stuxnet: US-Israeli Computer Virus Infected Russian Civilian Nuclear Power Plants"

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.[34]

Issues on which the Tallinn Manual was not conclusive. What self-defense is legal when it's unclear whether an operation could be classified as an "armed attack", or when the Security Council has not yet reached an agreement?

How might we determine what constitutes an armed cyber attack? Some states adopt a broad view of what constitutes illegal force while others have developed a much narrower classification.[35]

Tallinn Manual is clear that cyber operations alone could amount to an armed attack,[36] 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.[37]

If we can assume an armed attack accompanies any use of force and warrants a response under Article 51 (similar to the apparent view of the United States (US)[38]), then the Tallinn Manual provides a fairly complete template to determine whether an operation qualifies.[39]

Schmitt claimed 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

34. Convention, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*
35. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, page 17, para 3.
36. ibid., rule 22.
37. 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`
38. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." See page 433, para 4.
39. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See rule 11, esp. comment 9.

needs to be actually repaired.[40]

This seems to qualify Stuxnet as an armed attack, yet other experts still disagreed it crossed the undefined threshold. There was little physical damage done, compared traditional, kinetic force.[41] 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.[42]

Who can be held responsible in a cyber attack? Iran obviously had jurisdiction in Stuxnet.[43] Attribution is still a significant challenge though.

What of neutral states whose infrastructure was used to transfer Stuxnet? Laws on kinetic warfare imply they can be held accountable, but cyberwar feels different in this regard. The Hague Conventions itself limits a neutral state's obligation to restrict the combatant use of telephone or wireless cables.[44] Tallinn Manual states it must not *knowingly* allow conflicting parties to use its infrastructure.[45] The experts were split on whether that permits neutral states to passively allow such transmission.[46]

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.

40. Gollom, "Are there International Rules for Cyberwarfare? Existing laws apply to cyberweapons.," para 4.
41. 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/`
42. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare.* See rule 15.
43. ibid. See Rule 2
44. Convention, *Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land.* See article 8.
45. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare.* See rule 93.
46. ibid. See rule 93, comments 5 and 6.

Adopting the Tallinn Manual

Proposed solution for resolving international cyber conflict. The Tallinn Manual does an outstanding job of applying existing international law to the age of the internet, albeit lacking some detail. Much of the gray area is equally undecided in kinetic conflict, terribly complex and likely to evolve at a rapid pace. The Tallinn Manual should be adopted as a starting point for ruling on international cyber conflict and used to evolve international law, just as the US Constitution served as a starting point for US law and was molded by hundreds of years of precedence.

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 be solidified with time and applied as general rules.

Adoption of the Tallinn Manual raises more than only technical questions, as well. The Tallinn Manual was compiled by legal scholars of the NATO states and, while they worked with the best intentions and strived to maintain a universal view, it's possible they introduced some Western bias into the set of rules. Furthermore, Eastern states traditionally at odds with NATO are politically unlikely to accept a proposal supported solely by NATO.

To encourage all states to come together and form a truly worldly set of rules, those states who are not a part of NATO should be encouraged to participate in solidifying and finalizing the rules set forth in the Tallinn Manual, particularly those areas that are currently less decisive than they could be.

Once the evolution of the Tallinn Manual is made a global participation, the current members of the UN should be encouraged to sign a treaty adopting adherence to the Tallinn Manual.

Violation of the Tallinn Manual should be ruled on by the UN 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.[47]

There should be an official means to make lasting and binding amendments to

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

the Manual (or treaty), as deemed necessary by the Security Council and members of the UN.

Where Adoption Brings International Cyber Space

Analysis of the solution. 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:

> 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.[48]

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.

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.

48. Gollom, "Are there International Rules for Cyberwarfare? Existing laws apply to cyber-weapons.," para 23.

Conclusion

Conclusion The Tallinn Manual is worthy of official acceptance in founding international law and standards. The international community can look forward to a healthy, global internet with help from the Tallinn Manual and subsequent discussions on permissible and responsible online operations and stewardship. The efforts of the Tallinn Manual will give us confidence in the international arena that we, collectively, are continuing to act in cyber space in the spirit of already established and accepted international laws. It is the confidence to move forward.

Bibliography

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

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.

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.

"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.

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

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.

TODO. "TODO." TODO. Accessed November 16, 2014. http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.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.

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/.