

Applicability and Adoption of the Tallinn Manual

Considering Legality and Repercussions of the Stuxnet Worm

Steve Jarvis

November 23, 2014

Introduction

Recent years have seen the battlefield of earth changing. 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 with minimal technical or legal protections in place. The offensive capabilities and risks are continually increasing, 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 1942¹ and the Geneva Conventions in 1949.² These organizations founded treaties that defined international laws for entering into conflict (*jus ad bellum*) and behavior during conflict (*jus in bello*), respectively.

The agreements by these groups were established a full half century before the public internet was in its infancy, and as such, considered only kinetic warfare. The recent 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 push the boundaries. Cyber operations are limited by technical capabilities rather than legal or ethical standards.

The Tallinn Manual aims to fill the void of defined international law when it comes to cyber activity by translating the established kinetic laws to this modern battlefield.³

The goal of this report is to examine whether the Tallinn Manual is suitable for adoption in the international community. To make this determination, its applicability to real life actions, particularly the Stuxnet worm, will be considered,

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.

as well as the Tallinn Manual's political hurdles. If successful, the Tallinn Manual's adoption could help to ensure the safety and security of all states in coming years.

Our Current Situation

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 legal.⁴

Differing interpretations of how established laws regulate cyber activity results in dissension among states. There are no established answers on what constitutes illegal activity, whether it's possible to exert a use of force or launch an armed attack online, or what repercussions would be appropriate if it is possible, to name a few.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.

Why This Needs to Change

The world's situation is only growing more dire as states grow increasingly more reliant on cyberspace. The world's critical infrastructure, including power grids, water treatment plants, financial institutions and health care equipment, is growing increasingly more connected reliant on the Internet. Citizens and governments rely on these services to maintain a healthy and safe standard of living. This in-

4. **TODO see citation 14 of tallinn**

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>, pages 431-435.

frastructure, and by extension the cyberspace that enables its proper operation, has a direct effect on a state's sovereignty and deserves the same protections to which the physical world is privy.

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. The international community needs to establish rules protecting states' cyberspace.

The Tallinn Manual

The Tallinn Manual was an effort to fill the void in international law when it comes to cyberspace. It was the effort of an international group of legal experts, upon encouragement from the North Atlantic Treaty Organization (NATO), to correlate existing international laws on conflict to cyberspace.⁶ The intent was to give meaning to the laws established by the United Nations and Geneva Conventions in cyberspace.

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 with a clarity unachieved by any other attempts. 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 effort concluded in 2012 and continues to stand alone in its thoroughness considering a modern world and outpaced laws.

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

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

was to delay Iran's potential development of nuclear weapons, and it did this by causing the centrifuges that spin uranium to spin out of control and ultimately destroy themselves.^{7 8}

Despite the destructive chaos actually happening in the system, all the while the hardware would deliver positive reports to the operators, assuring them that operation was going safely and as planned, so the human operators capable of intervening had no indication there was an issue, much less one so dire.

To consider Stuxnet an act of aggression by another nation, though, it has to be known that it was in fact the product of a nation and not a private group of citizens or hacktivists.⁹ Stuxnet's level of technical difficulty was uncontested by any cyber attack prior (and maybe since). Stuxnet was not only extremely complex, it was also highly expensive.¹⁰ This evidence supports the theory that the attack was orchestrated by a nation-state, which qualifies it as a politically motivated operation. More recently, more concrete evidence has surfaced that it was in fact executed by a nation-state, particularly a collaboration between the United States and Israel.¹¹

Stuxnet exists amidst many controversial cyber operations over the past decade, yet it still deserves the 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. Prime alternative operations include Flame Malware¹² and Russia's cyber attack on Georgia.¹³ Flame was used for only espionage, and that is generally considered legal

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

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

9. **TODO**

10. 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>

11. **TODO** <http://abcnews.go.com/blogs/headlines/2013/07/edward-snowden-u-s-israel-co-wrote-cy>

12. Richard Stiennon, "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/>

13. David J. Smith, "Russian Cyber Strategy and the War Against Georgia," 2014, accessed

under international law.¹⁴ 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.¹⁵ 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, it proved to still be vulnerable. Stuxnet is believed to have been initially introduced to the target environment by an infected USB drive.¹⁶ En route to its final target, though, the virus crossed an unknown number of state boundaries.

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.¹⁷

As is with many worms, and almost by design, Stuxnet proved difficult to control.¹⁸ It leaked into the wild and infected an untold number of civilian computers in more than a dozen countries.¹⁹ Eugene Kaspersky, founder of the Russian security company Kaspersky 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.²⁰

The distinction here between civilian and nuclear or industrial facility infection

October 11, 2014, <http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia>

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

15. *ibid.*, page 94, para 6 and *ibid.*, rule 20.

16. 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. See page 8.

17. "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

18. **TODO cite the design comment**

19. Aleksandr Matrosov, "Stuxnet Under the Microscope." See page 15.

20. 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>

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.²¹ 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.²²

Issues Where Traditional Law is Lacking

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 few issues raised by Stuxnet which warrant specific consideration:

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.²³

21. Eitzen, "Stuxnet Also Found At Industrial Plants in Germany"

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

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

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 adopt a generally all-encompassing definition of what constitutes an illegal use of force, while others operate with much narrower classifications that limit a use of force to be essentially the same as an armed attack.²⁴ Supposing the international community accepts the view that an armed attack always coincides 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 terms is unlikely.²⁵

Some popular definitions of an armed attack require it to be violent, political, and (TODO cite. this definition was in our reading one week). There have been no cyber-only attacks to date to fit this description, so is it even possible to launch an armed attack online? How might an armed cyber attack be quantified?

Discriminate Attack

The Stuxnet worm leaked into the wild and infected civilian and government devices. A failure to control weapons in kinetic warfare is outlawed as indiscriminate, but it's not certain the same applies to malware, in which there is little danger of harm relative to illegal kinetic attacks, such as chemical warfare.²⁶ The civilian infection was not necessarily harmful, and does mere infection equate to an attack in cyberspace? Whether it was harmful or not, are there expectations for special consideration of civilians in cyberspace?²⁷

24. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, page 17, para 3.

25. TODO

26. 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>

27. TODO

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

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.²⁸ Is it legal to move malware through the infrastructure of neutral states, and can those states be held responsible for allowing it?

Retaliation, Defense and Rebuke

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 could a military response to a computer hack be reasonable?²⁹

If Stuxnet or similar attacks are decided to fall short of a qualification as a use of force can there be any retaliation taken? Particularly, what if the victim state doesn't have the means to defend itself, yet the United Nations doesn't deem the operation a use of force? This was the case in the 2008 attacks Russia launched on Estonia, who suffered a completely debilitated Internet for two weeks and received no aid after a request to the United Nations Security Council.³⁰ Would an external state with sufficient capability have the United Nation's blessing to offer protection?

28. 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.

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

30. **TODO**

Applying the Tallinn Manual to 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.

Use of Force

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.”³¹ 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.³² 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.³³ Stuxnet also directly violates at least Rule 1 of the Tallinn Manual.³⁴

The manual goes on to say that the experts were unanimous in determining cyber operations alone might qualify as armed conflict.³⁵ 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.³⁶

Tallinn Manual also comments directly that the experts were divided on whether Stuxnet qualified as an “armed attack”.³⁷ Some experts felt it was justified as anticipatory self-defense.³⁸

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

32. *ibid.* See page 51.

33. Kim Zetter, “Legal Experts: Stuxnet Attack on Iran Was Illegal ‘Act of Force’,” 2013, accessed October 6, 2014, <http://www.wired.com/2013/03/stuxnet-act-of-force/>

34. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See Rule 1.

35. *ibid.* See Rule 22, comment 15.

36. *ibid.* See Rule 22.

37. *ibid.* See Rule 22, comments 14 and 15.

38. *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.³⁹

Indiscriminate methods of cyber war are prohibited.⁴⁰ The infection of civilians' computers (might⁴¹) not violate this, because despite infection, the attack was performed only on specific Siemens systems (not civilian).⁴² 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 claims⁴³ 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.⁴⁴

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?

As mentioned, Tallinn Manual is clear that cyber operations alone could amount to an armed attack,⁴⁵ 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.⁴⁶

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

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

41. *ibid.* See Rule 1, comment 6.

42. Kushner, "The Real Story of Stuxnet"

43. 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/>

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

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

46. 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>

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)⁴⁷), then the Tallinn Manual provides a fairly complete template to determine whether an operation qualifies.⁴⁸

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 needs to be actually repaired.⁴⁹

This seems to qualify Stuxnet as an armed attack, yet other experts still disagree it crossed the undefined threshold. There was little physical damage done, compared traditional, kinetic force.⁵⁰ 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 51.⁵¹

Who can be held responsible in a cyber attack? Iran obviously had jurisdiction in Stuxnet.⁵² 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.⁵³ Tallinn Manual states it must not *knowingly* allow conflicting parties to use its infrastructure.⁵⁴

47. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." See page 433, para 4.

48. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See rule 11, esp. comment 9.

49. Gollom, "Are there International Rules for Cyberwarfare? Existing laws apply to cyber-weapons," para 4.

50. 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/

51. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See rule 15.

52. *ibid.* See Rule 2

53. Convention, *Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land*. See article 8.

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

The experts were split on whether that permits neutral states to passively allow such transmission.⁵⁵

Adopting the Tallinn Manual

The Tallinn Manual does an outstanding job of applying existing international law to the age of the internet. There are sections of the rule set which lack some detail or specifics. This indecisiveness can also be regarded as a strength. Much of the gray area in the Tallinn Manual is equally undecided in kinetic conflict, terribly complex and 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.

Adoption of the Tallinn Manual raises more than only technical questions. Some of the greatest hurdles to adopting the Tallinn Manual are political. As a NATO sponsored project, the translation of existing law to the realm of the 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 be 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 sign a treaty adopting adherence to the rules set forth by the Manual.

55. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare* See rule 93, comments 5 and 6.

The treaty 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, just as the United States' Constitution served as a starting point for US law and was molded by hundreds of years of precedence.

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.⁵⁶

Given the rapid evolution 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.

Where Adoption Would Bring the International Community

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

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

be possible under the law as we found it.⁵⁷

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 taking measures to secure, regulate and police domestic networks, often at the expense of some traditional internet freedoms.⁵⁸ 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 establish such proposals. Richard Clarke,

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

58. **TODO cte EFF?**

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.⁵⁹

Conclusion

The Tallinn Manual offers help in an area which the international community much needs it in the coming years. It should be taken advantage of.

The Tallinn Manual is not without technical and political hurdles, but it is ultimately worthy of official acceptance in founding international law and standards.

An agreement 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 internet with help from the Tallinn Manual and subsequent discussions on permissible and responsible online operations and stewardship. It is the confidence to move forward.

59. TODO <http://www.sfgate.com/business/article/Former-White-House-aide-backs-some-Net-regu>

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.

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>.

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>.

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). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1083889.

"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/>.
- . "Members." 2002. Accessed November 18, 2014. <http://www.un.org/en/members/>.
- 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>.
- Steinon, 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: Disrupting Uranium Processing at Natanz." 2013. Accessed October 11, 2014. <http://www.symantec.com/connect/blogs/stuxnet-05-disrupting-uranium-processing-natanz>.
- 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 Attack on Iran Was Illegal 'Act of Force'." 2013. Accessed October 6, 2014. <http://www.wired.com/2013/03/stuxnet-act-of-force/>.