Applicability and Adoption of the Tallinn Manual

Considering Legality and Repercussions of the Stuxnet Worm

Steve Jarvis

October 26, 2014

- Introduction.
  - How can we effectively deal with the new world of international cyber operations?
  - International law currently has a limited means for dealing with criminal cyber action.
    - The United Nations (UN) Charter and Geneva Conventions deal, historically, with only kinetic warfare.
      - Cyber actions rarely have a direct or obvious kinetic counterpart with which to compare. Differing interpretations results in dissension among states, with no clear answers on how to classify a use of force or armed attack online, or even whether it's possible to launch an armed attack in cyber space.[1]
      - Some states adopt a broad view of what constitutes illegal force while others have developed a much narrower classification.[2]
      - With no consensus on what constitutes permissible cyber activity, there can be no agreement on suitable international laws or treaties.
  - The Tallinn Manual aims to fill the void of defined international law or agreements when it comes to cyber activity.[3]
    - The Tallinn Manual was the effort of an international group of experts, upon encouragement from the North Atlantic Treaty Organization (NATO), to correlate existing international laws to cyberspace.[4]
  - The goal of this report is to determine whether the Tallinn Manual is suitable for official adoption in the international community by examining its applicability to the Stuxnet worm.
- Describe the issue. Explain Stuxnet, why it is the chosen event for consideration, and where guidance is needed from a cyber operations guide such as the Tallinn Manual.
  - Consider the actions and consequences of the Stuxnet Worm. Determine which, if any, international law was broken, and if so, how severely.
    - Explain Stuxnet technically, briefly.

1. 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.

2. Micael N. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare* (2013), page 17, para 3.

3. ibid., page 18, para 2.

4. ibid., page 16, para 1

- Stuxnet was an attack to sabotage the programmable logic controllers (PLCs) at the Iran nuclear enrichment facility and delay Iran's potential development of nuclear weapons.[5]
- Stuxnet was not only extremely technically complex, it was also extremely expensive.[6] As such, it's believed to have been conducted by a nation-state.

* Why Stuxnet deserves the focus.
  - Stuxnet offers a more complex situation and is the most likely candidate for a cyber-only operation to be considered a use of force.
  - Prime alternative operations include Flame Malware[7] and Russia's cyber attack on Georgia.[8] Flame was used for only espionage, and that is generally considered legal under international law.[9] Russia's cyber attack on Georgia, conversely, was used to further a kinetic attack and falls clearly into the category of armed conflict.[10] These conclusions are unsurprising and do not feel controversial.
* What were Stuxnet's goals and what it accomplished.
  - Stuxnet aimed to damage to and slow development of Iran's nuclear development.[11]
  - Iran refused to comment on whether it suffered damage from Stuxnet. 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.[12]
* Legal issues related to Stuxnet, on which there exists little or no help from established international law and guidance is desired from the Tallinn Manual.

5. 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

6. 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

7. 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/

8. 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

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

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

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

12. "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

· Intentional damage caused to a sovereign state's infrastructure by a computer virus. Was it:

1. Illegal?
2. A use of force?[13]
3. An armed attack?[14]

· The damage was intended to stifle development of military operations. How severe of a response (if any) is warranted?

· The worm leaked into the wild and civilians, Kapersky even claimed it's infected Russian nuclear facilities.[15] What repercussions might this entail?

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

- Determine whether the Tallinn Manual is an effective tool in practice by finding whether it proves useful when applied to Stuxnet.
  - Where the Tallinn Manual meets the needs of an international cyber conflict doctrine.
    * Unanimously determined to be in violation of international law and a use of force by the group of experts.[17] Stuxnet directly violates at least Rule 1 of the Tallinn Manual.[18]
    * The manual goes on to say that the experts were unanimous in determining cyber operations alone might qualify as armed conflict.[19] 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.[20]

13. United Charter, *Charter of the United Nations* (1945), `http://www.un.org/en/documents/charter/index.shtml`. See Article 2(4).
14. ibid. See Article 51.
15. 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/`
16. 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.
17. 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/`
18. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare.* See Rule 1.
19. ibid. See Rule 22, comment 15.
20. ibid. See Rule 22.

    * Tallinn Manual also comments directly that the experts were divided on whether Stuxnet qualified as an "armed attack".[21] Some experts felt it was justified as anticipatory self-defense.[22]
    * Indiscriminate methods of cyber war are prohibited.[23] The infection of civilians' computers (might[24]) not violate this, because despite infection, the attack was performed only on specific Siemens systems (not civilian).[25]
        · If Kapersky's claims that Stuxnet later infected Russian nuclear sites are true[26]

– 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?
        · Tallinn Manual is clear that cyber operations alone could amount to an armed attack,[27] 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.[28]
        · 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)[29]), then the Tallinn Manual provides a fairly complete template to determine whether an operation qualifies.[30]
        · Schmitt claimed that:

21. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See Rule 22, comments 14 and 15.
22. ibid. See Rule 13, comment 13.
23. ibid. See Rule 43.
24. ibid. See Rule 1, comment 6.
25. Kushner, "The Real Story of Stuxnet"
26. 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.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. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, rule 22.
28. 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`
29. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." See page 433, para 4.
30. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See rule 11, esp. comment 9.

> [...]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.[31]

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.[32]

· 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.[33]

* Who can be held responsible in a cyber attack?
  · Iran obviously had jurisdiction in Stuxnet.[34] 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.[35] Tallinn Manual states it must not *knowingly* allow conflicting parties to use its infrastructure.[36] The experts were split on whether that permits neutral states to passively allow such transmission.[37]

– The conclusions of the Tallinn Manual feel reasonable.
  * Many of the issues not directly resolved are complex and likely need 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.

- 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.

31. Gollom, "Are there International Rules for Cyberwarfare? Existing laws apply to cyberweapons.," para 4.
32. 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/`
33. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See rule 15.
34. ibid. See Rule 2
35. Convention, *Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land*. See article 8.
36. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*. See rule 93.
37. ibid. See rule 93, comments 5 and 6.

  - 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 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.
  - 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.[38]
  - There should be 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 UN.

- 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.[39]

  - 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.

- 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.

38. Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare*, rule 18.
39. Gollom, "Are there International Rules for Cyberwarfare? Existing laws apply to cyberweapons.," para 23.

– 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 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/.

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.

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.

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/.