# Applicability of the Tallinn Manual

Steve Jarvis

October 17, 2014

- Introduction.
  - In a world growing progressively more online, international law currently has a limited means for ruling on criminal cyber action.
    - The United Nations Charter and Geneva Conventions deal, historically, with only kinetic warfare.
      - Cyber actions rarely have a direct or obvious kinetic counterpart with which to compare. This 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 more exclusive classification.[2]
      - With no consensus on what constitutes illegal cyber activity, there can be no agreement on suitable international laws.
  - The Tallinn Manual aims to fill the void of defined international law when it comes to cyber activity. [3]

1. Waxman 2013, pages 431-435
2. Schmitt 2013, page 17, para 3
3. Schmitt 2013, page 18, para 2

    * The Tallinn Manual was the effort of an international group of experts, upon encouragement from the North Atlantic Treaty Organization (NATO).[4]

- Challenges. Determine whether the Tallinn Manual is an effective tool beyond a theoretical use. Whether it retains usefulness when applied to a real life attack.

  - Consider, specifically, the actions and consequences of the Stuxnet Worm. Determine whether international law was broken, and if so, how severely.

    * Explain Stuxnet technically, briefly.

      · It was an attack to sabotage the programmable logic controllers (PLCs) at the Iran nuclear enrichment facility and significantly delay Iran's potential development of nuclear weapons.[5]

      · Stuxnet was not only extremely technically complex, it was also extremely expensive.[6]

    * Why Stuxnet deserves the focus.

      · Prime alternatives are 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.

4. Schmitt 2013, page 16, para 1
5. Symantec 2013
6. Flanagan 2011
7. **flameForbes2013**
8. Smith 2014
9. Schmitt 2013, rule 6, comment 4.
10. Schmitt 2013, page 94, para 6 and Schmitt 2013, rule 20.

        - Cause damage to and slow development of Iran's nuclear development.[11]
        - Iran refused to comment on whether it suffered damage from Stuxnet. Other reports conclude that their nuclear program likely did suffer significant setbacks.[12]
    * Legal issues related to Stuxnet, on which guidance is desired from the Tallinn Manual.
        - Intentional damage caused to a sovereign state's infrastructure. Was it illegal, a use of force, and/or armed?
        - The damage was intended to stifle development of military operations.
        - How severe of a response is warranted?
        - The worm leaked into the wild and civilians, Kapersky even claimed it's infected Russian nuclear facilities.[13]

- Description of Tallinn Manual as relevant to a real life problem.
    - Where the Tallinn Manual meets the needs of an international cyber conflict doctrine in the case of Stuxnet.
        * Unanimously determined to be in violation of international law and a use of force by the group of experts.[14]
        * The manual goes on to say that the experts were unanimous in determining cyber operations alone might qualify as armed conflict.[15] Tallinn Manual states:

11. Kushner 2013
12. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" 2010
13. Wire 2013
14. Zetter 2013
15. Schmitt 2013, rule 22, comment 15.

> 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.[16]

- Tallinn Manual also comments directly that the experts were divided on whether Stuxnet qualified as an "armed attack".[17] Some experts felt it was justified as anticipatory self-defense.[18]

* Indiscriminate methods of cyber war are prohibited.[19] The infection of civilians' computers does not violate this, because despite infection, the attack was performed only on specific Siemens systems (not civilian).[20]
    - If Kapersky's claims that Stuxnet later infected Russian nuclear sites are true, however, Stuxnet did violate this rule, since it proves it was not limited in its effects as required by the law of armed conflict.[21]

– Issues on which the Tallinn Manual was not conclusive.

* Who even gets to accuse a suspect? Who gets to persecute?
    - Tallinn Manual doesn't seem to mention a requirement of cyber combatants to identify themselves, and it's seems unlikely they would, anyway. Attribution is a big challenge.
* How might we determine what constitutes an armed cyber attack?
    - Tallinn Manual is clear that cyber operations could amount to an armed attack,[22] but provide no means to determine whether a specific operation crosses that threshold, or how an armed attack

16. Schmitt 2013, rule 22.
17. Schmitt 2013, rule 22, comments 14 and 15.
18. Schmitt 2013, rule 13, comment 13.
19. Schmitt 2013, rule 43.
20. Kushner 2013
21. Wire 2013 and Convention 1977
22. Schmitt 2013, rule 22.

relates to a use of force (though that is a standing problem with kinetic warfare, just the same.)

- 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 defining detail. Without application to real life international conflict, though, it isn't obvious the Manual could reasonably be made much more detailed.
    - For example, there is little guidance on determining if Stuxnet, or any operation, qualifies as an armed attack. Some views, seemingly including that of the United States,[23] suggest that a use of force and an armed attack may be one in the same online.
      - Even though one in the same, the US has a relatively specific definition of a "use of force".
      - If we can assume an armed attack accompanies any use of force and warrants a response under Article 51, then the Tallinn Manual provides a fairly complete template to determine whether an operation qualifies.[24]
      - TODO find out why they thought it was an armed attack.
  - 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 U.S. Constitution served as a starting point and was molded by hundreds of years of precedence.
  - The current members of the UN should be encouraged to sign a treaty adopting adherence to the Manual.

23. Waxman 2013, page 433, para 4.
24. Schmitt 2013, rule 11, particularly comment 9.

  - 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.
  - There should be an official means to make amendments to the Manual, as necessary.

- Analysis of the solution.
  - The solution is neither perfect 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 the Tallinn Manual offers that help. 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.
  - Ratifying additional amendments will likely always prove challenging, just as international concurrence tends to be, but it is still an important necessity as the cyber space continues to evolve in ways not yet considered.

- Conclusion
  - Manual needs refinement and official acceptance, but is a tool worthy of forming international law.
  - 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.

# References

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

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

"Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" 2010. *Institute for Science and International Security.* http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf.

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

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

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

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

Waxman, Matthew C. 2013. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *Yale Journal of International Law* 36 (2). http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf.

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

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