FACT SHEET

Moving Towards Tallinn:
Drafting the Shape of Cyber Warfare

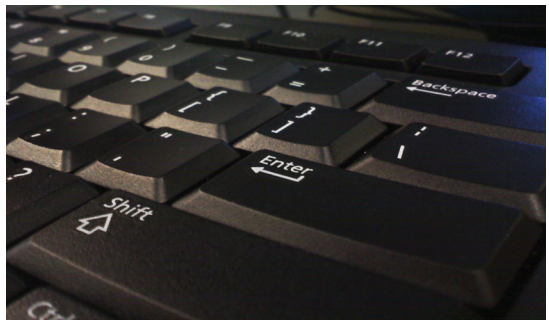
Ashley S. Boyle

September 2012

Introduction

On September 3, 2012, the NATO Cooperative Cyber Defence Centre of Excellence[1] (CCD COE) released a draft of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[2] The document was written at the request of the CCD COE by an International Group of Experts (IGE) comprised of legal and technical experts from academic and professional backgrounds.

The resulting 215-page draft is a peer-reviewed but unofficial document that examines whether and how existing international legal frameworks governing the use of interstate force apply in the cyber environment.



Despite its nonbinding status, the Tallinn Manual is the first of its kind to attempt to delineate the threshold dividing cyber war from cyber crime and formalize international rules of engagement in cyberspace.

Recent high-profile cyber operations have underscored the need for explicit codes of conduct in international cyberspace. To this end, the US has increased its efforts to develop comprehensive cyber policies for US cyber activity in both the domestic and international spaces.

The Tallinn Manual provides a litmus test on how experts from the international community foresee international law applying to the cyber environment.

It is an opportunity for the US to take stock of expert opinions on the matter and use this understanding to craft its own strong, effective, but minimally-intrusive cyber policies to achieve national security objectives both at home and abroad.

To aid understanding of this document, the American Security Project has compiled this condensed fact sheet with key findings from the Tallinn Manual.

Ashley Boyle is an Adjunct Fellow at the American Security Project

Part A: International Cyber Security Law concerns "those aspects of general international law that relate to the hostile use of cyberspace, but are not formally an aspect of either the *jus ad bellum* or *jus in bello*."[3]

- **Chapter I: States and Cyberspace** details how States, cyber infrastructure and cyber operations are related in order to determine State sovereignty, jurisdiction, and control over cyber infrastructure as well as State responsibility in regards to cyber operations.[4] Due to the technical challenges present in identifying perpetrators of and assigning responsibility for cyber operations, the IGE dedicates significant focus to these issues.

    - **Rule 1 – Sovereignty:** A State exercises control over the cyber infrastructure and cyber activities housed inside its sovereign territory.[5]

        - The IGE did not achieve consensus on whether malware that does not cause physical damage (such as that designed for surveillance or activity logging) meets threshold requirements to constitute a violation of sovereignty.[6] The IGE notes that there is a developing opinion that actions by non-State actors "may also violate a State's sovereignty."[7]

    - **Rule 2 – Jurisdiction:** A State has jurisdiction over individuals engaging in cyber activity conducted within its territory as well as over domestic cyber infrastructure. A State may also have extraterritorial jurisdiction where provided for by international law.[8]

        - On the issue of mobility: "any State from which the individual has operated enjoys jurisdiction because the individual, and the devices involved, were located on its territory when so used."[9]

    - **Rule 5 – Control of Cyber Infrastructure:** A State may not knowingly allow its cyber infrastructure to be used in such a manner that "adversely and unlawfully affect[s] other States."[10] A State may self-deny network services to its citizens when the timing and signature of an attack cannot be verified such as to prevent it from occurring.[11] This rule applies conditionally in instances in which an attack is routed through a State's cyber infrastructure, predicated upon the awareness of the transit State.[12]

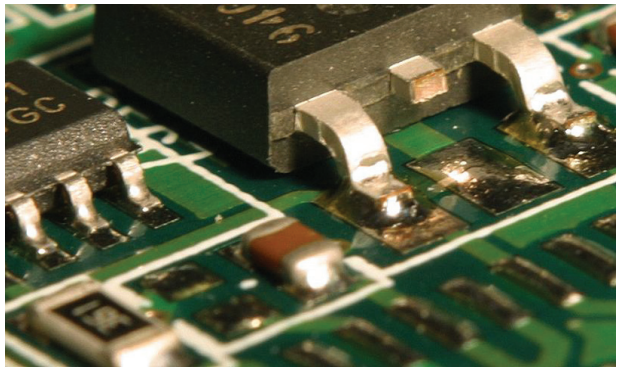
    - **Rule 6 – Legal Responsibility of States:** A State bears responsibility for any cyber attack attributed to it that violates international obligations.[13] This assignment of responsibility also applies to any individual, entity, or non-State actor acting with "governmental authority."[14]

    - **Rule 7 – Cyber Operations Launched from Governmental Cyber Infrastructure:** That an attack "has been launched or otherwise originates from government cyber infrastructure" is insufficient evidence for holding that State responsible for the attack. It does, however, indicate the State is associated with the cyber operation.[15]

- **Rule 8 – Cyber Operations Routed Through a State:** That a cyber operation was routed through a State's cyber infrastructure is not sufficient evidence for attributing the operation to or associating it with that State through which it was routed.[16]

- **Rule 9 – Countermeasures:** If State has been injured by "an internationally wrongful act," it may employ "proportionate countermeasures" against the State responsible for the cyber attack, which may include the use of cyber operations.[17]

- **Chapter II: The Use of Force** governs when the resort to and use of force is legally permissible (*jus ad bellum*). A State is prohibited from the threat or use of force[18] unless authorized by the United Nations Security Council (UNSC) under Chapter VII[19] or permitted under Article 51 of the UN Charter.[20] Therefore, a State targeted by a cyber operation that breaches the threshold of armed force[21] "may exercise its inherent right of self-defence [sic]."[22] Similarly, if the UNSC finds a cyber operation to be "a threat to the peace, breach of the peace, or act of aggression," it may authorize measures that can include cyber operations.[23]



  - The IGE notes that State practice is "only beginning to clarify the application to cyber operations of the *jus ad bellum*, citing the lack of standard definitions and thresholds as impediments to greater clarity on the matter.[24]

Part B: The Law of Cyber Armed Conflict

- **Chapter III: The Law of Armed Conflict Generally –** The law of armed conflict (*jus in bello*) is applicable in the cyber environment and thus cyber operations are subject to it.[25]

- **Chapter IV: Conduct of Hostilities –** Governs the means and methods that may or may not be employed during the conduct of hostilities (*jus in bello*).[26]

- **Section 2: Attacks Generally –** Finds that "the law of armed conflict applies to the targeting of any person or object during armed conflict irrespective of the means or methods of warfare employed."[27] Therefore, such principles as those of distinction and the prohibition of unnecessary suffering apply to cyber operations as they do to kinetic operations.[28]

- **Rule 30 – Definition of Cyber Attack:** A cyber operation, either offensive or defensive in nature, breaches the attack threshold when it "is reasonably expected to cause injury or death to persons or damage or destruction to objects."[29]

- **Section 3: Attacks against Persons** – Civilians may not be targeted by a cyber attack as long as they are not participants in hostilities.[30] Where there is to doubt as to the status of an individual, he will be counted as a civilian.[31]

- **Section 4: Attacks against Objects –** Specifies which tangible objects may be targeted by attacks.[32] Civilian objects may never be the target of cyber attacks, and computers, networks, or cyber infrastructure may only be targeted if they are military objectives.[33] A military objective "are those objects which by their nature, location, purpose, or use, make an effective contribution to military action" which offer a military advantage in their capture, destruction, or neutralization.[34]

- **Chapter V: Certain Persons, Objects, and Activities –** Specific persons, objects, and activities may not be targeted by a cyber attack, including: medical and religious targets; UN targets; detained persons; children; journalists; "objects indispensable to the survival of the civilian population"; and diplomatic archives or communications. Additionally, collective punishment is prohibited,[35] and humanitarian assistance efforts may not be interfered with or targeted.[36]

- **Chapter VII: Neutrality** – The concept of neutrality applies to cyberspace and cyber operations. Based upon Hague Conventions V and XII, as well as other international legal norms, neutrality maintains that "neutral cyber infrastructure" is that which exists within a neutral State (a State not party to the conflict) or has the nationality of a neutral State.[37]

Ashley Boyle is an Adjunct Fellow at the American Security Project focusing on asymmetric operations, political transition, and defense technology

Endnotes

1. CCDCOE. "CCD COE," *NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Estonia*. 2011. http://ccdcoe.org/ [Accessed September 12, 2012].
2. Michael N. Schmitt et al. eds. "Tallinn Manual on the International Law Applicable to Cyber Warfare," NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, forthcoming 2013. September 2012 draft available: http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft?mode=window&backgroundColor=%23222222 [Accessed September 3, 2012]. Hereinafter *Tallinn Manual*.
3. *Tallinn Manual*, Part A: International Cyber Security Law.
4. *Tallinn Manual*, Comment 1, Chapter I: States and Cyberspace.
5. *Tallinn Manual*. Rule 1 – Sovereignty.
6. *Tallinn Manual*. Comment 6; Rule 1 – Sovereignty.
7. *Tallinn Manual*. Comment 14; Rule 1 – Sovereignty.
8. *Tallinn Manual*. Rule 2 – Jurisdiction.
9. *Tallinn Manual.* Comment 4; Rule 2 – Jurisdiction.
10. *Tallinn Manual*. Rule 5 – Control of Cyber Infrastructure.
11. *Tallinn Manual,* Comment 5; Rule 5 – Control of Cyber Infrastructure.
12. *Tallinn Manual*. Comment 2; Rule 8 – Cyber Operations Routed Through a State.
13. *Tallinn Manual*, Rule 6 – Legal Responsibility of States.
14. *Tallinn Manual*. Comments 8, 9; Rule 6 – Legal Responsibility of States.
15. *Tallinn Manual*. Rule 7 – Cyber Operations Launched from Governmental Cyber Infrastructure.
16. *Tallinn Manual*. Rule 8 – Cyber Operations Routed Through a State.
17. *Tallinn Manual*. Rule 9 – Countermeasures.
18. *Tallinn Manual.* Rule 10 – Prohibition of Threat or Use of Force.
19. United Nations. *Charter of the United Nations*. June 26, 1945. http://www.un.org/en/documents/charter/chapter7.shtml [Accessed September 5, 2012].
20. Ibid.
21. *Tallinn Manual*. Rule.11 – Definition of Use of Force.
22. *Tallinn Manual*. Rule 13 – Self-Defence Against Armed Attack.
23. *Tallinn Manual*. Rule 18 – United Nations Security Council.
24. *Tallinn Manual*. Chapter II: The Use of Force.
25. *Tallinn Manual.* Rule 20 – Applicability of the Law of Armed Conflict.
26. *Tallinn Manual*. Chapter IV: Conduct of Hostilities.
27. *Tallinn Manual*. Comment 1; Section 11 – Attacks Generally.
28. *Tallinn Manual*. Rule 31 – Distinction.
29. *Tallinn Manual.* Rule 30 – Definition of a Cyber Attack.
30. *Tallinn Manual.* Comment 4; Rule 32 – Prohibition on Attacking Civilians.
31. *Tallinn Manual*. Rule 33 – Doubt as to Status of Persons.
32. *Tallinn Manual.* Section IV: Attacks against Objects.
33. *Tallinn Manual*. Rule 37 – Prohibition on Attacking Civilian Objects.
34. *Tallinn Manual*. Rule 38 – Civilian Objects and Military Objects.
35. *Tallinn Manual*. Rule 85 – Collective Punishment.
36. *Tallinn Manual*. Rule; Rule 86 – Humanitarian Assistance.
37. *Tallinn Manual*. Comments 1, 5; Chapter VIII: Neutrality.

Building a New American Arsenal

The American Security Project (ASP) is a nonpartisan initiative to educate the American public about the changing nature of national security in the 21st century.

Gone are the days when a nation's strength could be measured by bombers and battleships. Security in this new era requires a New American Arsenal harnessing all of America's strengths: the force of our diplomacy; the might of our military; the vigor of our economy; and the power of our ideals.

We believe that America must lead other nations in the pursuit of our common goals and shared security. We must confront international challenges with all the tools at our disposal. We must address emerging problems before they become security crises. And to do this, we must forge a new bipartisan consensus at home.

ASP brings together prominent American leaders, current and former members of Congress, retired military officers, and former government officials. Staff direct research on a broad range of issues and engages and empowers the American public by taking its findings directly to them.

We live in a time when the threats to our security are as complex and diverse as terrorism, the spread of weapons of mass destruction, climate change, failed and failing states, disease, and pandemics. The same-old solutions and partisan bickering won't do. America needs an honest dialogue about security that is as robust as it is realistic.

ASP exists to promote that dialogue, to forge consensus, and to spur constructive action so that America meets the challenges to its security while seizing the opportunities the new century offers.

ASP

American Security Project

www.americansecurityproject.org