The “Tallinn Manual” Sets Forth the Rules for Cyber Warfighters

By Michael N. Schmitt and Liis Vihul

For Issue #3, May 2014

Last Updated: Thursday May 08, 2014 01:18

Cyberspace has undoubtedly become an operational domain for States, a reality prominently acknowledged by the United States on repeated occasions. Indeed, according to Admiral Michael S. Rogers, the new U.S. Cyber Command Commander and National Security Agency Director, all major combatant commands will soon have dedicated cyber attack forces. Other States, such as the United Kingdom, the Netherlands and France have similarly announced that they are developing offensive cyber capabilities. At the same time, non-State actors possess relatively easy access to cyber attack tools and therefore represent a considerable national security threat to countries. Cyber war is here to stay.

In the face of this reality, there is an increased need for understanding when and how international law governs cyber operations, both defensive and offensive, a point echoed by Admiral Rogers’ assurance that U.S. Cyber Command will strictly adhere to the law in carrying out its operations. Along the same lines, last year fifteen nations, including the United States, adopted a consensus report under the auspices of the United Nations asserting that “[c]ommon understandings on how [existing international law] shall apply to State behaviour and the use of ICTs by States requires further study.”

As States formulate national positions on international law and cyber operations, they are highly likely to be influenced by the authoritative “Tallinn Manual on the International Law Applicable to Cyber Warfare”. Stirred to action by the cyber attacks targeting Estonia in 2007 and those against Georgia during its 2008 armed conflict with the Russian Federation, the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence convened a 20-person International Group of Experts to undertake a 3-year project exploring how international law governs cyber confrontations. The assembled “International Group of Experts” consisted of distinguished scholars and accomplished practitioners, all serving in their private capacity to ensure objectivity. They were, however, joined by observers from NATO Allied Command Transformation, U.S. Cyber Command, and the International Committee of the Red Cross. Each organization, albeit from different perspectives, had particular institutional interest in the project’s outcome and was able to provide valuable insights into the law and current activities in cyberspace.

The Manual is designed as reference tool for States in the planning and execution of cyber operations, as well as fashioning responses to harmful cyber operations. It is not meant to be US or NATO-centric, since all States are today exposed and vulnerable to hostile cyber targeting. Indeed, most States possess no significant offensive cyber capabilities, but nevertheless need to understand how international law facilitates and limits defensive cyber measures. Importantly, considering its intended use by practicing legal advisors who have to base their legal analysis on the existing law, the "Tallinn Manual" limits its analysis
only to such law, and refrains from proposing how the law should develop in the future. Likewise, it offers no policy or operational suggestions, leaving such matters to policy-makers and operators.

Despite early claims to the contrary, consensus has emerged that international law applies to activities in and through cyberspace. The “Tallinn Manual” focuses its attention on two aspects of international law: the jus ad bellum (the law that governs when States may resort to force as an instrument of their national policy); and the jus in bello (the law of war that regulates how hostilities may be conducted during an armed conflict).

In the jus ad bellum, the principal legal issues concern the prohibition of the “use of force” set forth in Article 2(4) of the UN Charter and right of States to self-defense in the face of an “armed attack” enshrined in Article 51. With respect to cyber operations, States must therefore ask two questions. Are their cyber operations or those directed against them an unlawful use of force? May they respond to cyber operations against them with a cyber or kinetic use of force because it is so severe that it qualifies as an “armed attack” in the sense of Article 51?

The non-kinetic consequences of most cyber operations challenge traditional interpretations of both concepts. If another State’s cyber operations injure or kill persons, or damage or destroy objects, they are unambiguously uses of force. However, when physical consequences are lacking, States operate in a fog of law. There are convincing arguments for regarding cyber operations that cause significant non-physical harm as in violation of the use of force prohibition. An example is the targeting of Saudi Arabia’s national oil company, Saudi Aramco, with the Shamoon malware in 2012. The operations rendered 30,000 of the company's computers non-functional. Although it might appear to make no sense to differentiate between a kinetic operation that destroys computers and a cyber operation that makes them unusable, the law remains unsettled. Thus, the Manual usefully sets forth a menu of indicators as to how States may resolve the question in their operations and policy.

The most grave uses of force can qualify as armed attacks against which the victim State can use force in self-defense. Unfortunately, international law provides no clear guidance on the definition of an armed attack. The “Tallinn Manual” concluded that a cyber operation that causes direct or indirect physical damage or injury qualifies, but came to no conclusion as to whether one that had serious non-physical consequences (such as collapse of a financial system) was an armed attack. State practice over the next decade should help clarify matters.

The United States has taken a unique position on uses of force. For the United States, any use of force is also an armed attack and therefore justifies a forceful response. The administration has warned that “if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.” It has not openly indicated whether, and if so, what type of, non-physical damage could amount to a use of force.

As recent conflicts between both the Russian Federation and Georgia and the Russian Federation and Ukraine demonstrate, cyber operations are likely going to play a role in most future wars. All belligerent cyber operations must be conducted in accordance with the jus in bello. This means, for example, that cyber attacks must not be directed at the civilian population as such, individual civilians or civilian objects. Members of the armed forces that conduct cyber attacks, but fail to wear a uniform or other indication of their status, lose their entitlement to combatant immunity and prisoner of war status. Additionally, belligerent cyber operations may not be conducted from neutral territory with the exception of simple transmission of data across such territory.

Cyber operations that fall below the armed attack threshold and therefore do not permit the exercise of self-defense are the subject matter of the Tallinn Manual’s follow-on project, “Tallinn 2.0”. On a daily basis, States are faced with various cyber activities that raise the question of their lawfulness, but do not constitute armed attacks or even uses of
force. For the United States, the most pressing issue seems to be foreign industrial espionage. Such espionage puts its private companies at a competitive disadvantage and weakens its military wherewithal by enabling other States to enhance their military technologies with less research and development effort and cost. For other States, large-scale surveillance of cyber communications is one of the most topical concerns, prompting the discussion of its legal permissibility. The legal norms at the heart of such discussions are the sovereignty; the prohibition of intervention in the internal and external affairs of other States; the legal requirement that States may not knowingly allow their territories to be used to the detriment of other States and its application in the cyber context; and the precise parameters of international human rights norms in the cyber environment. These are examples of topics that “Tallinn 2.0” will address. Once the project concludes in 2016, the second expanded edition of the Tallinn Manual will be published. It will then cover the entire spectrum of international law applicable to State cyber operations both in times of peace and war.

http://www.ccdcoe.org/249.html

Michael N. Schmitt is the Tallinn Manual Project Director; Charles H. Stockton Professor and Chairman, International Law Department, United States Naval War College; Professor of Public International Law, University of Exeter Law School; Senior Fellow NATO Cooperative Cyber Defence Centre of Excellence.

Liis Vihul is the Tallinn Manual Project Manager; Senior Analyst, NATO Cooperative Cyber Defence Centre of Excellence.


4 The Defence Cyber Strategy (Netherlands) at 11.


6 Admiral Rogers’ testimony at a Senate Armed Services Committee on his nomination to run the National Security Agency. Available at: http://www.nytimes.com/2014/03/12/world/europe/nsa-nominee-reports-cyberattacks-on-ukraine-government.html?_r=1

7 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98 adopted by Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, UK and USA.


Material contained herein is made available for the purpose of peer review and discussion, and does not necessarily reflect the views of the Department of the Navy or the Department of Defense.