COUNCIL on FOREIGN RELATIONS

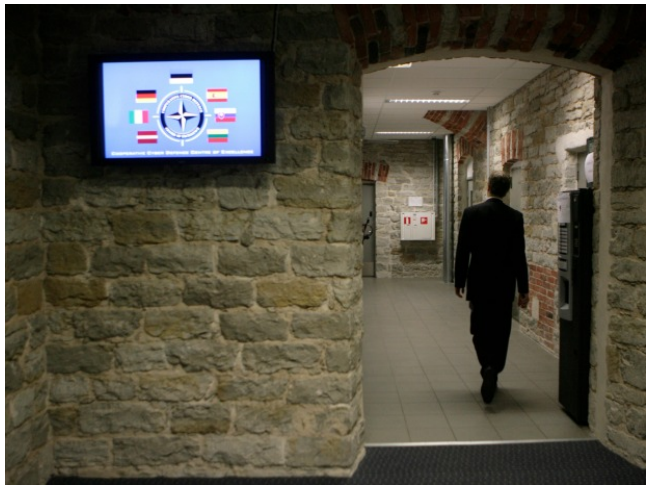
CFR PRESENTS

Net Politics

CFR experts investigate the impact of information and communication technologies on security, privacy, and international affairs.

International Perspectives on Regulating Military Cyber Activity

by **Guest Blogger**
June 3, 2015



A Cooperative Cyber Defence Centre of Excellence by NATO staff member walks through a closed operational area of the centre in Tallinn, Estonia on November 10, 2008. (Ints Kalnins/Reuters).

Ashley Deeks is an associate professor at the University of Virginia Law School. She formerly served in the State Department's Office of the Legal Adviser and was an international affairs fellow at the Council on Foreign Relations.

This past week, the **NATO Cooperative Cyber Defense Center of Excellence** put on its annual **Cyber Conflict (CyCon)** conference in Tallinn, Estonia. Rather than summarize some of the panels, which offered important insights into the most pressing issues in the cyber arena, this post looks across those panels to identify common themes that arose during the conference. At least one important refrain emerged: an anxiety about the lack of a robust, clear legal framework within which to conduct and evaluate cyber operations.

Grappling with the Rules—or Lack Thereof

This was not a legal conference. Indeed, part of its appeal is that it brings together a mix of technologists, military officials, academics, lawyers, and corporate officials. Nevertheless, one of the most noticeable themes I detected across panels was a strong interest in increasing the clarity of international law regulating cyber operations. Senior policy speakers such as Adm. Mike Rodgers and NATO Assistant Secretary General Sorin Ducaru repeatedly referred to the importance of operating in accordance with the law. Many at the conference seemed to view legal rules as promoting stability and, therefore, security.

Yet comments such as these embodied a tension: while policymakers agreed on the importance of acting in accordance with legal rules, others pressed for increased clarity about what, exactly, those rules are. Indeed, one workshop at the conference was devoted to exploring the options for cyber norm development. And the conference's international law-related panels were standing room only: there was obvious interest in hearing ideas about how to apply or tweak existing international law to fit the cyber context.

Questions at the conference about the cyber rules of the road sorted themselves into three buckets: who creates the rules; what the rules should look like; and how procedurally to develop these rules.

Who Will Create the Rules?

States, of course, are the primary (and some say only) creators of international law. Whether by concluding treaties or creating customary law by engaging in extensive state practice over time, states generally dictate what the rules of the road will be. But one confounding factor, at least in today's cyber world, is that the large majority of state practice is done secretly and rarely sees the light of day. Far more than many other areas of geopolitical activity, states' actual conduct in the cyber arena remains unknown and, to a large extent, unknowable to other states.

For this reason, products such as the Tallinn Manuals are garnering intense interest. **The first Tallinn Manual**, produced by an

independent group of experts mostly drawn from NATO member states, came out in 2013. The Manual proffered what the experts saw as the current state of the law relevant to cyber operations that involved a state's resort to force or a state's conduct of armed conflict. Version 2.0 picks up where the first version left off, and will set forth the experts' views on what international law applies to cyber activity that falls below the level of armed conflict or the use of force—activity such as cyber espionage or denial of service attacks. Because the Manuals have been crafted by recognized experts, and because the Manuals provide a systematic examination of what the rules seem to be today, many actors are treating the Manual as the closest thing to an authoritative source on the current state of the law.

What Should the Rules Look Like?

As to the content of the rules, another tension manifested itself. On the one hand, many hope to use existing international law as the key source of cyber rules. But several speakers highlighted that existing rules require some modifications in order to fit neatly with cyber activity. For example, international law allows a state to undertake "countermeasures" against another state that has committed an international law violation against it. But before a state takes a countermeasure, it is supposed to request that the law-breaking state stop the violation and, if the violation continues, to inform the violating state of the impending countermeasures. Those notice requirements may make less sense in the cyber context, given the speed at which cyber activities take place. Likewise, a state may act in self-defense when an armed attack is "imminent," but how should a state assess the imminence of an attack when it discovers a logic bomb on its system and cannot tell what action might trigger a severe and near-instantaneous attack?

These and other examples discussed at CyCon reveal the need for states to fine-tune existing rules, to the extent that major cyber players even accept that the existing rules are the proper baseline from which to work. Russia and China may reject this proposition.

By What Process Should We Establish those Rules?

On the third question—that of process, and how to develop the rules—there is an apparent divide among states, and between some states and NGOs. Some NATO members with robust cyber capabilities seem content to assert that they are acting lawfully, on the basis of

relatively general international rules, but seem disinclined to provide detail about how they are applying those rules. Smaller states, academics, and NGOs seem to be pressing for a more detailed legal framework. A Chinese speaker raised questions about the Tallinn process, based on a concern that it was a Western project that failed to account for the views of other actors. In short, stark differences remain about what process, if any, states should use to reach firmer consensus about the cyber rules of the road.

The Tallinn 2.0 process is just getting underway, with an estimated completion date of 2016. Those drafting the 2.0 Manual are actively engaging with non-Western states to ensure that the product accurately reflects the current legal positions not just of NATO members but of a range of states. Though such consultations might complicate the drafting, they are likely to pay off in the longer run if they provide the 2.0 Manual with additional legitimacy.

Pingbacks