18 July 2017

Geneva Conventions Apply to Cyberspace: No Need for a 'Digital Geneva Convention'

Calls for a new international treaty to regulate cyber operations between states are confusing the debate over norms and policy development in cyberspace according to the independent review of Tomáš Minárik and LTC Kris van der Meij, researchers at the NATO CCD COE, a NATO-affiliated cyber defence think-tank.

The following analysis does not represent the views of NATO.

The recent WannaCry and NotPetya cyber campaigns have prompted reactions from major ICT companies. Microsoft, in particular, has renewed its call for a Digital Geneva Convention that will oblige governments to protect civilians from nation-state attacks in times of peace. The initiative has gained the support of Deutsche Telekom, which has called for thinking on an intergovernmental level with respect to the possibility of a binding treaty prohibiting 'all kinds of cyber attacks'. This is unsurprising, since malicious cyber attacks are bad for the business of transnational ICT companies in that they reveal exploits of vulnerabilities in their products (such as EternalBlue) and encourage consumers to consider open-source or other alternatives.

However, calling for a 'Digital Geneva Convention' is both legally confusing and politically unrealistic.

"The original Geneva Conventions and the Additional Protocols thereto are part of international humanitarian law, or law of armed conflict. They are designed primarily for an armed conflict, such as the ongoing war between Russia and Ukraine. They apply to cyber operations that have a link to an armed conflict; however, they have a limited applicability outside the scope of an armed conflict," says Tomáš Minárik, researcher at NATO CCD COE Law Branch.

"Nevertheless, other rules of international law play a major role with respect to peacetime cyber activities, such as those found in the Council of Europe's Convention on Cybercrime or the customary law rules regarding the responsibility of States for unlawful activities that have been set forth in the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts," adds LTC Kris van der Meij from NATO CCD COE Law Branch.

Tallinn Manual 2.0: A Thorough Guide for State Action in Cyber Space

In 2009-2013, the first edition of the Tallinn Manual was prepared under the auspices of the NATO CCD COE, which examined the applicability of law of armed conflict (including the Geneva Conventions) to cyber operations in great detail. The second edition of the Tallinn Manual, also authored under the auspices of the NATO CCD COE in 2013-2017, added legal analysis of the more common cyber incidents: those that do not occur during an ongoing armed conflict, nor have the potential to trigger one.

These cyber incidents are currently of enormous relevance to states, businesses and regular users. Therefore, international efforts to advance norms to help prevent and defend against these incidents, such as the UN GGE, OSCE confidence-building measures, and Microsoft's initiative have to be applauded for focusing attention on the subject and attempting to identify and craft norms for peacetime cyber activities.

Better Focus on Gradual Progress than Unrealistic Universal Consensus

Microsoft has been perhaps the most vocal and long-standing critic of unfettered state-sponsored operations, with its long-term initiative of cybersecurity norms for nation-states and the global ICT industry. All of its proposals are reasonable; states would be well-advised to consider them in their own policy and norms development.

"Improving the cyber security of critical infrastructure, but also convincing states to extend the right to privacy extraterritorially, curbing indiscriminate online surveillance and data retention, and addressing international law violations by governments are important and realistic goals. However, they are achievable through gradual progress and do not require universal consensus. Devoting effort to a Digital Geneva Convention that has little chance of ratification by most countries would be counterproductive," concludes Minárik.

Given that certain states in the UN GGE were unable in 2017 to even agree on the simple statement that law of armed conflict applies to cyberspace (which logically follows on from the UN GGE's 2013 confirmation that international law applies to cyberspace), it is hard to imagine the adoption of a broadly multilateral cyber-specific treaty anytime soon. Indeed, even in the unlikely event of such a treaty coming to fruition, it is unclear if there is a technically viable mechanism by which it could be verified.

A basic international legal framework exists to protect civilians in war- and peacetime; if states cannot agree on new treaty law, they can still develop state practice on existing treaty law, which might in turn drive the further development of customary international law.

The NATO CCD COE follows the developments in international organisations active in cyber security on a dedicated website of the INCYDER project.

NATO Cooperative Cyber Defence Centre of Excellence is a Tallinn-based knowledge hub, research institution, and training and exercise centre. The international military organisation is a community of currently 20 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. NATO CCD COE is home of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. The Centre also organises the world's largest and most complex international technical cyber defence exercise Locked Shields.

The Centre is staffed and financed by its sponsoring nations and contributing participants. Belgium, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States are signed on as Sponsoring Nations of NATO CCD COE. Austria, Finland and Sweden have become Contributing Participants, a status eligible for non-NATO nations.

This brief reflects the independent views of NATO CCD COE researchers. This brief does not necessarily reflect the policy or the opinion of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre), Sponsoring Nations and Contributing Participants of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

For further insight, please also learn about the analysis of WannaCry campaign by NATO CCD COE researchers and recent conclusions on NotPetya incident.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

A: Filtri tee 12, 10132 Tallinn,

Estonia T: +372 717 6800 F: +372

717 6808 E: ccdcoe -at- ccdcoe.org