CYBER SECURITY SUMMIT
Security solutions through collaboration™

Webinar Series — November 2020
Rapporteur Report

Cyber Norms in a Changing World

Cyber Security Summit International Webinar Series
November 24, 2020

Speaker: Eneken Tikk, Executive Producer at the Cyber Policy Institute, Finland

Moderator: Sean Costigan, Director & Co-Founder, ITL Security

Report Author: Simon Bracey-Lane, Research Fellow, Institute for Statecraft

Speaker Bio:

Eneken Tikk is the Executive Producer of the Cyber Policy Institute in Jyväskylä, Finland and associate researcher at Helsinki University. She began her career as a lawyer with interest in ICTs and public international law and has been part of developing Estonian data protection, public e-services and cybersecurity legislation. Dr. Tikk was a member of the team that started the NATO CCD COE, where she established and led the legal and policy branch. Eneken leads the Cyber Conflict Portal project at CPI and is the Editor-in-Chief of the International Journal on Digital Peace and Security. Eneken also leads the 1internat10nal Law project focused on critical research on international law and cybersecurity. Eneken is co-editor of the Routledge Handbook on International Cybersecurity (2020).

Introduction:

From the twentieth chapter of Deuteronomy forming the basis of Medieval laws of war[1] to the Geneva convention, quantifying acceptable actions in conflict is an ancient human tradition. But our world is changing faster than many of our institutions can adapt. As our world changes, so have the rules surrounding diplomacy, trade, industry and warfare. One of the most significant changes to our societies has been the rise of cyber space and the conflict that has come to dominate it. The following Rapporteur report outlines the discussion surrounding the generation of shared standards and rules for cyber space, or 'Cyber Norms.'

What are Cyber Norms?

These are not mechanisms for how nations resolve international technical issues or combat malicious activities. Instead, it is how diplomats are seeking to develop universal values for the international cyber community to strive towards. They are an ambition set of recommendations to foster greater transparency and cooperation. To render assistance in mitigation, enable effective criminal proceedings and identify instances of when a state's territory or infrastructure has been used to attack other states.

[1] J Barker, Agincourt: Henry V and the battle that made England, London 2005, pg., 143

What are Cyber Norms intended to achieve and what are the chances they will be adopted?

These shared standards are driven by a desire to create a world better equipped to both prevent and mitigate the impact of cyber incidents. This is coupled with an effort towards achieving an open, secure and stable cyberspace.

They are also a mechanism to develop a universally held consensus towards what responsible state cyber activity should be. These recommendations can be broken down into the following four points:

- **Protection of critical infrastructure:** States would adhere to a set of rules that protect critical infrastructure. Widespread implementation of these norms would lower the chances of attacks like Stuxnet, the attack on Saudi Aramco or the crippling of the Ukrainian electric grid. This is particularly relevant following the uptick in attacks on hospitals and on COVID-19 vaccine research and supply chains.
- **Enshrinement online human rights:** If enshrined with the same vigor offline human rights have been, we can ensure widespread condemnation and deterrence from internet shutdowns and any breaches of personal data.
- **Due Diligence:** Pressure to ensure vigilance on domestic infrastructure, making sure members of the international community are not unwittingly facilitating harm to other nations. This would go a great distance in challenging Distributed Denial of Service (DDOS) attacks.
- **Transparent Reporting:** Instituting international code of forthright transparency could reduce things like the number of zero-day attacks experienced around the world.

While positive, these recommendations are limited and lack the scope to comprehensively challenge all elements of cyber conflict. They do not address electoral interference, or disinformation operations and are predominantly technically focused. This is a weakness as states wage Hybrid Warfare, the fluid combination of tools to undermine and disrupt rival nations below the threshold of clear warfare. To focus on one element of the mosaic is to simply see a small colored tile rather than see the whole picture.

Debate also emerges about what services and processes can be considered critical. Can trust services, like certification organizations and anti-doping agencies or other international organizations be considered critical infrastructure? Is tourism a critical sector to every international partner? Would these norms be broad and compelling enough to dissuade indiscriminate attacks on platforms such as Google Play or all IoT devices.

The capacity of individual nations is another obstacle to the effectiveness of these recommendations. Many countries that want to assist in providing information and support in cross border criminal investigations might not have the right capabilities. This leads to a situation of willing, but unprepared international partners.

Lastly, we cannot expect adversarial nations or even close competitors to cooperate or exchange information on *all* aspects of malicious and hostile cyber activities. The reality is that governments who frequently conduct or condone malicious cyber operations are unlikely to report vulnerabilities of value to them.

Conclusion:

Many dismiss the utility of cyber norms. In their current form they are abstract, unbinding and unlikely to be implemented soon or in the near future by key states that frequently engage in cyber operations. However, we cannot expect our diplomats to do the work of our technical communities, manufacturers or users. Each sector has a part to play in this effort. It is important, regardless of the obstacles, that attempts are made to challenge conflict. Cyber Norms promote dialogue, open mindedness and international collaboration. These recommendations represent a potential to do a great deal of good. It represents a step towards creating an open, secure and stable cyberspace.

Thank you to our sponsor

CWT