Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Jaak Tarien, *Connections QJ* 19, no. 1 (2020): 5-7
https://doi.org/10.11610/Connections.19.1.01

Policy Highlights

National Cyber Defence Policies and the Role of International Cooperation

Colonel Jaak Tarien

Director of the NATO Cooperative Cyber Defence Centre of Excellence

Digitalization has made our societies vulnerable to cyber threats – from electric grids to elections. This is also true for militaries, and cyber defence has become a natural task for all defence organizations. Cyber threats cannot be considered as new threats anymore. However, the cyber threat landscape is changing rapidly, and will continue to do so. Malicious viruses, hackers, hacking, etc., are still part of this landscape, but cyber weapons and cyberattacks originating from nation states are the primary security concerns today. Malicious actors are quick to learn from each other and their tools proliferate. How should we respond? The creation of more secure cyberspace is possible only through cooperation. As there are no traditional borders in cyberspace, NATO Allies and Partners share the same responsibilities, as well as opportunities.

Cooperation in the area of cyber defence was, as it clearly appears from the name, the primary motivator behind the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) by six NATO nations in 2008. As of today, the Centre is staffed and financed by 25 countries altogether. Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Turkey, the United Kingdom and the United States are signed up as Sponsoring Nations of the NATO CCD COE. Austria, Finland and Sweden are Contributing Participants, a status eligible for non-NATO nations. The Centre continues to attract new members: Japan, Croatia, Montenegro, Slovenia and Switzerland are in the process of joining the Centre. In addition, Canada, Luxembourg and Australia have announced their intention of accession.

The NATO CCD COE, focusing on research, training and exercises, offers various training courses at a technical, operational, and strategic level for its member nations. In addition, the International Law of Cyber Operations Course is prepared for legal advisors. The Centre conducts a yearly international Red Team vs Blue Team exercise *Locked Shields* for cybersecurity experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. *Locked Shields* also includes a strategic element that covers decision-making, legal, and communication aspects. More than 1500 experts from 30 nations took part in *Locked Shields* 2019. *Crossed Swords*, another annual exercise, is a technical red-teaming cyber exercise targeting penetration testers, digital forensics experts and situational awareness experts. The annual conference CyCon—International Conference on Cyber Conflict—is the Centre's contribution to the broader cybersecurity community. CyCon promotes research and development on the technical, legal, policy, strategy, and military perspectives of cyber defence and security. One of the internationally recognized research accomplishments for the Centre has been the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations."[1] The Tallinn Manual 2.0 is the most comprehensive analysis of how existing international law applies to cyberspace. Finally, since 2018 the Centre is responsible for identifying and coordinating education and training solutions in cyber defence for all NATO bodies across the Alliance. As the Centre's heart is its international staff, cyber experts with various backgrounds, then all our deliverables are practical examples of the value and benefits of international cooperation.

The importance of cyberspace for our societies and economies will only grow. It is still transforming – connecting increasingly more people and devices, new emerging technologies allow new functionalities. But the future of cyberspace is in our hands. This growth and development are only possible if security and safety of, and in, cyberspace are provided. This means that our national policies, strategies, and laws need continuous review and adaptation. Cybersecurity will remain a challenge for all governments and globally. We will see discussions on roles and responsibilities of different state institutions, including military, on how to best respond to this challenge.

In this issue of "Connections," perspectives from Austria, Germany, Israel, Switzerland, the UK and the US are all valuable reference materials for other nations.

The more ambitious goal—more secure and safe cyberspace as a whole—is only possible through international cooperation. NATO and the EU, and other organizations, have a significant role here. Yes, international cooperation in cybersecurity is a sensitive and complex issue, and there are limits. However, the very basis for this cooperation is trust, information sharing and the ability to learn from each other. If we succeed with this, then the door for further cooper-

[1] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second edition (Cambridge, UK: Cambridge University Press 2017).

ation is open. The current issue of "Connections" is another step toward opening this door further.

Disclaimer

The views expressed are solely those of the contributing author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgement

Journal *Connections: The Quarterly Journal*, Vol. 19, 2020 is supported by the United States government.

About the Author

Colonel **Jaak Tarien** is the Director of the NATO Cooperative Cyber Defence Centre of Excellence, based in Estonia, since September 2018. Prior to joining the Centre Colonel Tarien served as the Commander of the Estonian Air Force from August 2012 to July 2018. Among other assignments, he has also served as Staff Officer with NATO's Supreme Allied Command Transformation (ACT), as Deputy Director of the Regional Airspace Surveillance Coordination Centre and as the Commander of the Estonian team at the BALTNET Regional Airspace Surveillance Co-ordination Centre in Lithuania.

Colonel Tarien, a graduate of the United States Air Force Academy, earned his Master's degree from the Air Command and Staff College of the USAF Air University. He recently also acquired a Master of Science degree in National Resource Strategy at the US National Defence University.