Merle Maigre : "Cyber defence is clearly a top priority for NATO"

Director of NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

© EDF

Merle Maigre

Since 2006 when Supreme Allied Commander Transformation approved the concept of a NATO Cyber Defence Centre, how has it been developing ?

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was founded in 2008, receiving accreditation from NATO the same year. For one example of the developments, ten years ago, the Tallinn-based CCDCOE was founded by seven nations and with James Mattis, current United States Secretary of Defense, signing the Memorandum of Understanding then on behalf of the Allied Command Transformation.

In 10 years, the Centre has grown from seven founding members in to 20-nations strong and capable international team. Our member nations include 17 NATO allies and 3 EU members. Our mission is to support NATO and our member nations with cyber defence research, training and exercises in 4 core areas : technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts, including legal scholars, policy and strategy specialists who join forces with technology researchers, all from military, government and industry backgrounds.

This unique and interdisciplinary setup has led to the launch of some highlights of CCDCOE that we are very proud of. In the beginning of this year the Centre launched *Tallinn Manual 2.0*, the most comprehensive guide on the application of international law to cyber operations. Since 2010 we are organising *Locked Shields*, the world's largest and most complex international live-fire cyber defence exercise. It focuses on training the technical experts, policy staffers, legal and media advisors who are responsible for national cyber security. The aim is to teach both military and civilians about the interdependencies from each other and various systems and networks. In addition, since the establishment of the Centre, we host every spring the annual conference on cyber conflict, *CyCon*, which unites more than 500 decision-makers and experts from government, academia and industry from all over the world. *CyCon* has developed into a community building event in cyber defence, bringing together the different experts of cyber defence – techies, lawyers, researchers, policy advisors, industry experts, government officials and military top brass.

CCDCOE is recognised not only in the worldwide cyber defence community, but also increasingly more among other key players who are not daily dealing with cyber security issues – such as ministers and other government officials, and military officers.

What are the main NATO strategic objectives relating to cyberspace ?

Cyber defence is clearly a top priority for NATO. Last year, NATO decided to establish cyber as a separate domain, meaning NATO will defend Allies against any threat : in cyberspace just as it has been doing on land, in the air or at sea.

“Locked Shields is the world’s largest and most complex international live-fire cyber defence exercise. It focuses on training the technical experts, policy staffers, legal and media advisors who are responsible for national cyber security”.

NATO recognises that international law applies in cyberspace and has reaffirmed its commitment to act in accordance with it. Last year, NATO Allies signed a *Cyber Defence Pledge* to strengthen their cyber defences as a matter of priority. NATO has developed some detailed metrics related to the *Cyber Defense Pledge* and regularly reports how each nation delivers on its cyber commitments based on these metrics. NATO is also strengthening the cyber component of its Command Structure. NATO Command Structure is the military backbone of the alliance.

NATO has constantly adapted its Command Structure over the past decades, to take account of a changing security environment. In a more unpredictable world, the Alliance has to adapt again.

In every military operation, in any foreseeable possible military mission or operation of NATO, there will be a cyber component. Therefore, cyber will also be part of the review and the adaptation of the command structure.

How is the Operations Branch working ? Is the Center involved in real operations ?

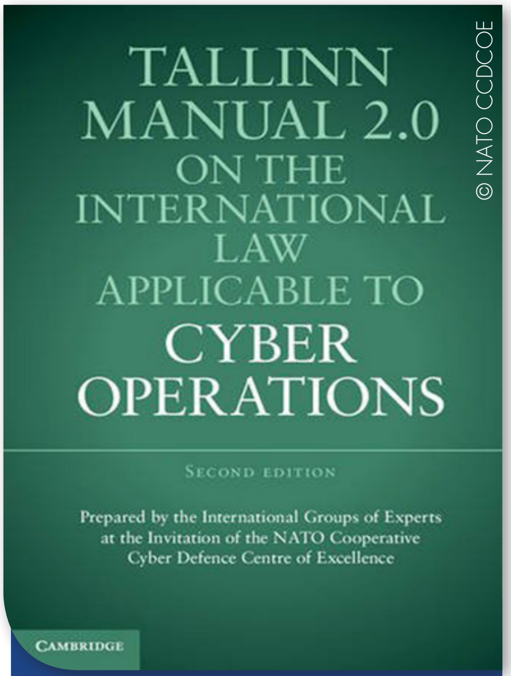
NATO CCDCOE is not an operational unit, our role is to provide advice, research, training and exercises. Operations Branch at the Centre analyses and provides solutions on how to best incorporate the cyber element in modern military operations.

At present, we are analyzing the integration of cyber into military planning process and operations. Furthermore, we are supporting NATO with analyses on how to achieve battlefield effects in cyber defence.

“Tallinn Manual 2.0” on international law in Cyberspace is presented as an influential resource for legal advisers dealing with this domain of operations. How does this new edition make a difference with the previous 2013 edition ?

Authored by nineteen international law experts, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* is the updated and considerably expanded second edition of the 2013 Tallinn Manual on the International Law Applicable to Cyber Warfare. The focus of the first edition of the Tallinn Manual was on the most severe cyber operations, those that violate the prohibition of the use of force in international relations, entitle states to exercise the right of self-defence, and/or occur during armed conflict. Tallinn Manual 2.0 adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis, and that fall below the thresholds of the use of force or armed conflict.

As such, the 2017 edition covers a full spectrum of international law as applicable to cyber operations, ranging from peacetime legal regimes to the law of armed conflict. The analysis of a wide array of international law principles and regimes that regulate events in cyber space includes principles of general international law, such as the sovereignty and the various bases for the exercise of jurisdiction. The law of state responsibility, which includes the legal standards for attribution, is examined at length. Additionally, numerous specialised regimes of international law, including human rights law, air and space law, the law of the sea, and diplomatic and consular law are examined within the context of cyber operations.



TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS

Second edition

Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence

Cambridge

© NATO CCDCOE

"Tallinn Manual 2.0" 2017 edition covers a full spectrum of international law as applicable to cyber operations, ranging from peacetime legal regimes to the law of armed conflict.

How could the work done here in Tallinn, as regards International Law in Cyberspace, impact the national laws of the NATO nations ?

The analyses concluded by the authors of Tallinn Manual 2.0 and also the studies carried out by our legal scholars create a valuable basis for further debate and discussions on potential policy measures and approaches. In the end, it is up to the nations to enforce International Law, but an impressive body of work has already been done for the national legal and policy advisors who should offer guidance for the most appropriate legal framework or course of action.

What is the Strategy Branch dealing with ? What is its possible contribution to the global NATO strategy ?

The NATO CCDCOE acts as the custodian of NATO's cyber doctrine. The Centre coordinates and facilitates this process by inviting all the players to the table who are ultimately responsible for writing the doctrine. Doctrine drafted by nations that participate is then circulated to all NATO allies for further comment.

What kind of cooperation the NATO Center of Excellence is conducting with the European Union ?

The Centre recognizes the value of collaboration with a variety of partners in the private sector, academia and also EU. We welcome the participation of EU experts in our training courses and exercises. The liaison between CCDCOE and European Defence Agency has been established and is growing, also on the basis of the roadmap that we have developed. With EDA we jointly investigate the feasibility for the establishment of EDA-CCDCOE joint projects in the future.

Interview by Jean-François Morel

© NATO CCDCOE

A scene of "Locked Shields 2017". "The aim is to teach both military and civilians about the interdependencies from each other and various systems and networks".

Prior to taking command as director of CCDCOE in August 2017, Merle Maigre has been the Security Policy Adviser to the President of Estonia. She also served as the Policy Adviser in the Policy Planning Unit in the Private Office of NATO Secretary General Rasmussen in Brussels. She has also worked as a researcher at International Centre for Defence and Security.

Merle Maigre is a graduate of King's College London (M.A.), Middlebury College (B.A.), and Tartu University (B.A) ; she has also studied at the Johns Hopkins SAIS Bologna Center and the Paris Institute of Political Studies or Sciences-Po.