CCDCOE Report Launch and Panel Discussion

Cybersecurity of 5G Networks

31 October 2022

Research presentation by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) hosted at the European School of Management and Technology Berlin (ESMT), followed by panel discussion.

As NATO member states coordinate a strategic response towards the Russian invasion of Ukraine, the transatlantic alliance's technological vulnerabilities are becoming more apparent. In the context of emerging technologies and increasing cyberattacks, NATO should step up its efforts in improving cyber resilience and securing supply chains for critical digital technologies. Cyber defence of the military structures in Europe depends also on the unhindered functionality of civilian information infrastructures, especially on telecommunication service providers and their key equipment suppliers.

Faced with an unprecedented frequency of malicious cyber activities, NATO allies are more reliant on robust and safe 5G networks than ever before. In the renewed geopolitical context, cyber resilience in European countries deserves special attention. There are significant technological risks involved, not only for the military and government networks, but also for private corporations, which may inadvertently expose their valuable data used for the development of smart mobility, industry 4.0, eHealth, etc.

In 2020, the NATO CCDCOE launched a two-year project on 5G supply chain and network security. The project addresses the technical, strategic, legal, and policy issues of new-generation telecommunication infrastructure for NATO allies and close partners. Its recently launched report "Military Movement: Risks from 5G Networks" examines a potential NATO military movement scenario in 2030 and associated interactions with 5G technology in relation to seaports and road transportation. Smart seaports and digitalised transportation corridors were chosen as the most likely use-case environments for 5G applications in the given time horizon.

Mitigating cyber risks requires reliable 5G networks provided by trustworthy vendors and service providers, which fulfill all relevant standards set out in the EU toolbox for 5G security. By building relationships between the public and private sector on 5G networks and ensuring the interoperability of networks and technologies, NATO can promote synergies between the similar efforts of the EU, the transatlantic partners and the private sector.

The report launch in Berlin is taking place in the context of current profound changes in German security and foreign policy. Working with international partners, academic experts and private sector stakeholders, Germany is preparing a new national security strategy and advancing its military capabilities. Berlin is willing to set a new tone following Chancellor Olaf Scholz' speech on the beginning of a *Zeitenwende* in German security policy, the implementation of which has already started.

Agenda

15:30 – 16:00	Arrival of participants and registration
16:00 – 16:05	Welcome intervention by Christian-Marc Liflländer, Head of NATO Cyber Defence and Hybrid Policy Section
16:05 – 16:15	Opening remarks by Piret Pernik, Senior Researcher, CCDCOE
16:15 – 16:35	Key conclusions of the report "Military Movement: Risks from 5G Networks" by Mattias Männi, 5G Program manager, CCDCOE and Urmas Ruuto, Chief of Technology Branch, CCDCOE
16:35 – 17:40	Panel discussion on the impact of 5G technology on cyber resilience and military mobility in Europe **Moderator** - Prof. Dr. Paul Timmers, Research Associate, University of Oxford and Adjunct Professor, European University Cyprus **Panelists** - Prof. Dr. Gabi Dreo Rodosek, Founding Director of the Research Institute CODE, Bundeswehr University Munich - David Antunes, Programme Manager Cyber Defence, European Defence Agency - Dr. Valentin Weber, Cyber Research Fellow, German Council of Foreign Relations - Dr. Daniel Massey, Program Lead - Operate Through 5G to NextG Initiative, U.S. Department of Defense
17:40 – 17:55	Discussion with the audience
17:55 – 18:00	Closing remarks by Felix Kroll, Cyber Policy Coordination Staff, German Federal Foreign Office
18:00 – 20:00	Networking reception at the ESMT

The in-person event will be hosted at the ESMT Berlin at Schlossplatz 1, Berlin