CCDCOE Report Launch and Panel Discussion

Cybersecurity of 5G Networks

Introduction

On October 31st, 2022, the CCDCOE Report Launch with an affiliated panel discussion on “Cybersecurity of 5G Networks” took place at ESMT Berlin. The introductory presentation of the research outputs and key conclusions of the report "Military Movement: Risks from 5G Networks" was followed by a panel discussion on the impact of 5G technology on cyber resilience and military mobility in Europe. The panel consisted of experts on 5G and cybersecurity from academia as well as policy makers to reflect the complexity of the topic. The event started with a welcome intervention by Christian-Marc Lifländer, Head of NATO Cyber Defence Section on the importance of cybersecurity and secure networks for NATO. Following a wrap-up of the panel discussion and a brief Q&A session, the event ended with closing remarks by Felix Kroll, Deputy Head of the Cyber Policy Coordination Staff at the German Federal Foreign Office, who spoke of the role of cybersecurity in Germany’s upcoming national security strategy

Presentation of the CCDCOE Report

Rapidly advancing technological progress is a driver of innovation and growth, however, it also carries important security implications. As emerging technologies are being deployed in wars and greyzone conflicts, analyzing technologies from a military and security perspective becomes essential to ensure protection against malicious state-sponsored and other threat actors. One example of this, are 5G networks, which lie at the heart of future mobility, the development of the Internet of Things, as well as other innovations reliant on secure, stable and low latency networks. The deployment of 5G has consequences for not only the EU, but also NATO, with new risks and opportunities presenting themselves for states adopting these networks.

Awareness of the potential risks for companies and governments are important for improving network security, but more crucially the military and strategic implications of 5G networks need to be understood and taken into account before making decisions about the choice of vendors. The authors of the CCDCOE report on risks from 5G networks in a military context attempt to fill this gap, by presenting scenarios and explaining the security implications of unsecured networks.

The report examines a potential NATO military movement scenario in 2030 and its associated interactions with 5G technology in relation to two use-case environments: smart seaports and smart road transportation. It addresses technical, strategic, legal, and policy issues of next generation telecommunication infrastructure for NATO allies and close partners. The goal of the report is to raise awareness among decision-makers on the implications of the fast-paced developments of 5G in commercial settings. Future interactions of 5G technology with military deployments will influence strategic decision-making by the Alliance. Hence, opportunities, related cyber threats, and risks to private 5G networks dedicated to enterprise use are examined.

The **main observations** from the presentation include the following points:

- The introduction of commercial 5G networks and associated commercial applications is approaching quickly: Various initiatives in the EU and the USA have expanded their transatlantic

5G portfolio in recent years and some nations are already trialing 5G for military purposes. Additonally, smart seaports are expected to be operational in many EU member states in 2030. Smart roads will be available as pilot projects in some countries after 2030.

- These developments will impact NATO's military mobility in the future. The report shows, that those movements will take place through commercially owned 5G networks. Hence, commercial service providers are key elements in the implementation of secure 5G networks. A close cooperation of the military and the commercial sector is therefore necessary.

- The analysis concludes that 5G improves operational efficiency, reliability, and safety. Operational 5G solutions at ports by 2030 improve the cargo shipment process in movement and decrease operational risks. Smart-road solutions improve traffic safety and smoothness. They also reduce the environmental impact of military mobility.

- On the other side, services offered by private 5G networks will introduce new security risks and require mitigation. There are different measures for mitigating cybersecurity risks: Encryption and integrity protection, validation of used software and hardware, defense-in-depth for virtualized network deployments, security by design principle, and interconnected end-to-end security. Implementing these measures is highly relevant to the security of 5G networks and their safe use for military purposes.

Furthermore, the report develops **recommendations** and presents a framework for mitigating the resulting risks. These encompass three categories: use-cases, system security, as well as policies and standards.

- **Focusing on specific use cases**: The report shows that 5G-enabled use cases carry increased opportunities as well as risks. Hence, risk analysis must be executed to find out if the advantages outweigh the disadvantages. Security auditing of private 5G networks and their supply chains are required. Additionally, the need for temporarily disabling service or its functions due to the wide-ranging technological landscape and operations should be considered for military usage. Moreover, the report suggests to create multinational and cross-organizational pilot programs to address the co-development of 5G systems and associated challenges.

- **Improving system security**: Improving system security to develop a comprehensive 5G cyber security strategy is key. NATO, in close cooperation with the EU, should take a proactive stance here. While doing so it should be engaged in building a secure system and get involved in the development process of commercial 5G systems that are interoperable and accessible by the military. Moreover, a stringent monitoring and security recommendation process needs to be adopted, e.g. by frequent risk analyses to assess the security of the system.

- **Setting policies and standards**: The deployment of 5G networks is in the hands of the member states. Harmonizing their implementation is vital for military mobility. Hence, coordinated policies and standards should be adopted in accordance with closer cooperation between the member states. To achieve this, collaboration and information sharing with network operators, service providers, and vendors as well as the involvement of critical infrastructure operators in regulation processes is key.

Panel Discussion

The panel consisted of 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; and Dr. Daniel Massey, Program Lead – Operate Through 5G to NextG Initiative, U.S. Department of Defense and was moderated by Prof. Dr. Paul Timmers, Research Fellow, Oxford University.

The insightful discussion addressed the relevance but also the risks of 5G in a broader context and concluded with recommendations for its future military use. The debate focused particularly on the following aspects: cooperation, resilience, regulation, and trust.

We live in a time shaped by multiple crises, but also by great technological progress. To solve the problems of our time successfully, these two developments must be brought together. 5G represents the technology of the future – yet it is also associated with novel security risks. To master these and successfully implement 5G, existing infrastructures must be utilized and if necessary expanded. There is already an existing 5G infrastructure among parts of the commercial sector, however, the main barrier to wider adoption – including for military purposes – is a lack of confidence in security. Nevertheless, this barrier can be removed through closer **cooperation** with the private sector. The debate highlights that establishing a multistakeholder ecosystem is essential for the future secure use of 5G for military purposes. This cooperation must be cross-sectoral: international cooperation, e.g. on NATO and EU level, as well as strengthening public-private cooperation are necessary.

Despite this, challenges to bring all relevant stakeholders together and to encourage information and threat sharing persist. **Trust** is vital to establish such an environment. To achieve this, incentives must be created to encourage information sharing accompanied by assurances that shared information will be used in this context only. Cooperative pilot projects between the private sector and the military represent an important contribution to this.

In general, the mindset needs to shift towards making cybersecurity and civil security clear priorities. Beyond that, there is a need for a paradigm shift: While systems should be as secure as possible, i.e. through certification and verification, etc., systems also need to be resilient to emerging threats. Due to the complexity of 5G networks, it is not possible to secure them completely, which is why building **resilience** is crucial.

At the same time, we must actively think one step ahead. During the discussion, it was emphasized that non-binding recommendations are not enough to make networks as secure as possible. Instead, binding **laws and regulations** are required to protect the general security. States should take leading roles in prioritizing security and resilience. However, a balance must be achieved so that there is not too much pressure on the private sector, which will need to be accompanied by increased investment.

Through the panel discussion it became clear that, despite the availability of commercial infrastructure and platform, there will be cases in which existing infrastructure will not be used for military purposes for various reasons. In those cases, the military will have to build its own infrastructure. Such decisions must be based on risk analysis and considerations of risks and opportunities. For this purpose, a more holistic understanding of risks is needed, as well as an overview of existing initiatives, recommendations, and progress in the field of 5G.

In summary, the panel discussion provides a positive outlook for the use of 5G and the possibility of civil-military cooperation.