CYBERSECURITY OF 5G NETWORKS

Research presentation and panel discussion co-organised by the EU Institute for Security Studies (EUISS) and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

05 July 2022, Residence Palace, Brussels

INTRODUCTION

Convened by the EUISS and CCDCOE, this report presentation and panel debate brought together senior officials and experts on 5G Networks and Cybersecurity to discuss CCDCOE's 2030 scenarios on military movement risks from 5G networks as well as the viewpoints of different sectors on the use of 5G networks. The panel included senior speakers from NATO, the European Union Cyber Security Organisation (ECSO) and the Private Sector. The debate aimed to further mutual understanding of the use of 5G networks in a rapidly changing security environment, and to understand the opportunities and risks associated with 5G in a variety of scenarios and sectors. 5G networks are more secure than earlier generation telecommunications networks but they also entail new security vulnerabilities.

PRESENTATION OF THE CCDCOE REPORT

While the first CCDCOE report focuses on Supply Chain and Network Security for Military 5G Networks, the second report, which was presented during this conference, focusses on Military Movement Risks from 5G Networks.

The report examines a potential NATO military movement scenario in 2030 and its associated interactions with 5G technology in relation to smart seaports and smart road transportation. The report aims to raise awareness among decision-makers about how the quick development of 5G in the commercial setting will impact future military movements and the resultant strategic decisions the Alliance must make to avoid being caught off guard. The report also examines the opportunities and related cyber threats and risks to private 5G networks dedicated to enterprise use.

The main observations from the presentation include the following points:

- The rollout of commercial 5G networks and associated commercial applications is fast approaching: various initiatives in the EU and the US have raised the transatlantic 5G portfolio in the last years.
- Military but more so commercial service providers are key elements of implementing secure 5G networks.
- Cybersecurity risk mitigation of 5G networks is essential. The measures include but are not limited to zero trust, end-to-end security, encryption and data integrity, security by design, risk assessment and mitigation frameworks, public-private and military-private cooperation, transparency, supply chain security framework and controls, etc.
- It is anticipated that in 2030 smart seaports will be operating in many EU member states, and that after 2030 smart roads will be available as pilots in some countries. These developments will impact NATO military movement in cases where there are no alternatives available or their use provides benefits for armed forces.
- Military movement will be affected by 5G networks either by utilising them on own initiative or relying on services provided by commercial provider services.

The recommendations of the research report are grouped into three categories: policies and standards, system security, and specific recommendations related to the use-cases.

- **Setting policies and standards:** The EU toolbox for 5G security and related EU regulations focuses on commercial mobile operators, equipment vendors and third-party service providers. ENISA 5G threat assessments describe multi-access edge computing (MEC) risks but public discussion about 5G networks

security has not focused on MEC security considerations. To address MEC security concerns, collaboration with third party application providers, including military-private sector information exchange, is essential.

- **Improving system security:** A comprehensive 5G cyber-security strategy needs to be developed by institutional and private stakeholders, in line with the security by design principle.
- **Focusing on specific use-cases:** There is a need to prepare for cybersecurity auditing of private 5G networks and their supply chains in smart seaports. Furthermore, the preparation of a regulatory framework for smart road use-cases with an option for disabling some components of services for military use should be considered.

PANEL DISCUSSION ON THE CYBERSECURITY OF 5G NETWORKS

The panel consisting of Manfred Bodreaux-Dehmer, Chief Information Officer, NATO; Roberto G. Cascella Head of Sector, Standardisation, Technology, Supply Chain and Strategic Autonomy, European Cyber Security Organisation (ECSO); and Per Ljungberg Director, Architecture & Portfolio, Ericsson was moderated by Dr Raluca Csernatoni, a visiting scholar on European Security and Defence, Carnegie.

The discussion focused on the use of 5G networks in a broader context, by including NATO, EU and private sector perspectives on the subject. What emerged from the discussion is that the relationship between the public and private sector on 5G networks is crucial. NATO does not make regulations but is specialised in the interoperability of networks and technologies. Thus, more synergies between the EU, NATO and the private sectors should be created. Structures such as the NATO Innovation Fund and DIANA need to be used to further the 5G and cybersecurity agendas. When talking about 5G networks, some difficulties that constitute potential vulnerabilities are that the infrastructure is comprised of a large number of service providers and that the global supply chain is opaque. Diversifying supply chains to avoid a vendor lock-in has been previously acknowledged as a key priority. As there are many dual-use technologies, military-private cooperation should be improved, especially when it comes to exchanging best practices and information. The EU Toolbox for 5G security also needs to be further defined and developed.