CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Tallinn 2021

EXECUTIVE SUMMARY OF

Supply Chain and Network Security for Military 5G Networks

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Executive Summary of Supply Chain and Network Security for Military 5G Networks

NATO needs to keep itself thoroughly informed about the opportunities 5G technologies provide for improving Euro-Atlantic deterrence and defence, as well as about the security risks inherent in 5G networks. How would security risks related to public (commercial) and private (military) networks impact NATO missions and operations? If civilian or military 5G networks ever became compromised or came under the control of potential adversaries, the repercussions for NATO's Military Instrument of Power, and for deterrence and defence, would be severe. NATO must develop ways and means to deploy 5G technology to support the Military Instrument of Power, and security risks related to them must be mitigated.

This Research Report examines supply chain and network security challenges associated with 5G technology. It discusses vulnerabilities, threats, and risks to public and military 5G networks. The report aims to raise awareness among decision-makers on how operating through public and private 5G networks can impact the Alliance's missions and operations. It also aims to provide evidence-based information on security risks associated with 5G technology and networks, risks which may affect NATO missions and operations. The report outlines three use cases for the military use of 5G networks as follows: smart sea ports, road transportation, and public safety networks.

Resilient telecommunication networks are essential for NATO's political and military-strategic interests. Today, NATO implements baseline requirements concerning telecommunications infrastructure and guides NATO nations' resilience goals and implementation plans related to them.[1] The Alliance includes trustworthiness criteria in its security policies and regulations and in the technical procurement of equipment.[2] An improved understanding of supply chain vulnerabilities, risks, and threats is necessary in order to enable evidence-based and risk-informed decision-making by NATO nations regarding the current and future policies related to 5G technologies and infrastructure. Sharing information based on common methodologies and doing so frequently – for example, assessments about vulnerabilities, threats, and risks associated with high-risk 5G vendors – would be a first step toward increasing visibility and building consensus on security risks among the Allies.

Further, since even trusted networks could have untrusted components, which would make them vulnerable, NATO and armed forces must be able to operate over such networks and insecure interfaces. In some cases, sensitive or classified government information should not be transferred or stored in 5G networks if the level of confidentiality, integrity, and availability of those networks cannot be ensured at a sufficient, military-grade level. Security requirements for military communications may be greater than those offered by the commercial 5G service providers. For example, the military needs to avoid being identified, geo-localised, and jammed by an adversary; however, commercial service providers do not normally prioritise those concerns for their other customers' needs. When militaries use specialised communication services requiring high levels of security, reliability, and availability, the military use of 5G technology would require military-grade security controls (on top of the commercial levels

1 'Brussels Summit Communiqué', 14 June 2021, NATO, https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.

2 'Keynote Address by NATO Deputy Secretary General Mircea Geoană at the NCI Agency's NITEC Connect 2021 Conference', NATO, 16 June 2021, https://www.nato.int/cps/en/natohq/opinions_184907.htm.

of supply chain and network security) – for example, robustness against jamming and end-to-end encryption of data. Due to the need to harden public 5G networks and infrastructure for military use, future research and technical testing should address the ways and means of doing so. As a corollary, respective state authorities and armed forces should have a sufficient view of the processes, procedures, and practices used by manufacturers of 5G technology, as well as providers of associated services. This serves to assure the integrity, security, resilience, and privacy, as well as quality, of the acquired products, systems, and services throughout their whole life cycle. NATO should facilitate discussions with 5G equipment manufacturers, service providers, and other stakeholders on how to make possible increased scrutiny of supply chains, with a view to agreeing on a common set of policies and standards for resilient, reliable, available, and secure 5G networks. Armed forces must work closely with commercial service providers to assess supply chain and network security risks, and in some cases, militaries must add suitable security assurances to commercial networks.

This report recommends developing common criteria to assess 5G vendors' trustworthiness, building on risk assessment and management guidelines developed by the EU and national governments. A joint risk management implementation plan related to 5G technology, services, and infrastructure should be developed with a view to addressing military needs and requirements related to them. The first step for NATO is to identify what those needs and requirements are. Furthermore, the requirements could be incorporated by default into the development of standards and technical specifications of 5G technology. To that end, NATO should cooperate with the industry to ensure that military needs and security specifications are taken into account when developing standards. NATO nations' industry representatives' participation in the standard-setting bodies should also be increased.

NATO should also support the adoption of trusted technology globally, which would enable the Alliance to mitigate risks inherent in the technology of authoritarian countries. Nations should refrain from using technology from vendors whose technology has, in the past, been used to undermine universal values and democratic freedoms.

This Research Report contains a set of initial **policy recommendations** in the areas of supply chain and network security, policies and standards, research, education and training, and partnership. It is the first of several reports from the CCDCOE 5G Supply Chain and Network Security research project, which will run until June 2022.