CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Tallinn 2021

Research Report Supply Chain and Network Security for Military 5G Networks

Piret Pernik, Taťána Jančárková, Kadri Kaska,
Urmas Ruuto, Costel-Marius Gheorghevici
and Henrik Beckvard

NATO CCDCOE

ABOUT THE AUTHORS

This Research Report is co-authored by Piret Pernik, Taťána Jančárková, Kadri Kaska, Urmas Ruuto, Costel-Marius Gheorghevici, and Henrik Beckvard. Piret Pernik revised and edited the paper and authored three chapters: 'Introduction', 'Supply Chain and Network Security', and 'Recommendations'. Taťána Jančárková and Kadri Kaska co-authored the chapter 'Policy and Regulatory Developments Related to 5G Networks', which includes contributions from Piret Pernik. Urmas Ruuto and Piret Pernik co-authored the chapter 'Radio Spectrum Allocation and Deployment Status of 5G Networks'. Costel-Marius Gheorghevici authored its section on standardisation, which includes contributions by Piret Pernik. Piret Pernik and Henrik Beckvard co-authored the chapter 'Military 5G Network Use Cases'. Urmas Ruuto, Costel-Marius Gheorghevici, and Piret Pernik co-authored the chapter 'Workshop Conclusions'.

ACKNOWLEDGEMENTS

The authors would like to thank Rónán Micheal O'Flaherty and Sungbaek Cho for contributions to the research project. The authors are grateful to Martijn Rasser for offering constructive comments and recommendations. The authors sincerely thank Dan Massey, Jim Dimarogonas, Kennet Nomeland, Dipesh Modi, Amir Stephenson, Warren Low, and John Strand for comments.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the Centre is a diverse group of international experts from military, government, academia and industry.

The CCDCOE (also the Centre) maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational, and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations, and law.

To date NATO CCDCOE is staffed and financed by 29 member nations: Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. Australia, Canada, Ireland, Japan, Luxembourg, the Republic of Korea, Ukraine and others have expressed interest in joining the Centre.

The CCDCOE produces the Tallinn Manual 2.0, the most comprehensive guide for policy advisors and legal experts on how international law applies to cyber operations carried out between and against states and state actors. Since 2010 the Centre has organised Locked Shields, the biggest and most complex technical live-fire challenge in the world. Each year, Locked Shields gives cyber security experts the opportunity to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies, and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision-makers of the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring. The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

DISCLAIMER

Table of Contents

1. Abbreviations

3GPP	3rd Generation Partnership Project
5G NR	5G New Radio
5G PPP	5G Infrastructure Public Private Partnership
5G-VINNI	5G Verticals Innovation Infrastructure
API	Application Programming Interfaces
C2	Command and Control
CCAM	Cooperative, Connected and Automated Mobility
CCRA	Common Criteria Recognition Arrangement
CEF	Connecting Europe Facility
CIS	Communication and Information Systems
CISA	Certified Information Systems Auditor
CMMC	Cybersecurity Maturity Model Certification
CN	Core Network
COTS	Commercial-Off-The-Shelf
CSIS	Centre for Strategic and International Studies
DDoS	Distributed Denial-of-Service
DoD	Department of Defense
DSS	Dynamic Spectrum Sharing
ECC	Electronic Communications Code
EDA	European Defence Agency
EDT	Emerging and Disruptive Technologies
eMBB	Enhanced Mobile Broadband
EDF	Estonian Defence Forces
EU	European Union
EUCC	Common Criteria based European candidate cybersecurity certification scheme
ENISA	European Union Agency for Cybersecurity
FDI	Foreign Direct Investment
gNodeB	5G New Radio base station
GPS	Global Positioning System
GSMA	Global System for Mobile Communications
HPA	Hamburg Port Authority
ICT	Information and Communications Technology
IoT	Internet of Things
IMSI	International Mobile Subscriber Identity
IMT	International Mobile Telecommunications
ISR	Intelligence Surveillance and Reconnaissance
ITS	Intelligent Transport System
ITU-R	International Telecommunications Union Radiocommunications Sector
LTE	Long Term Evolution
MEC	Mobile Edge Computing
MITM	Man in the Middle
MIMO	Multiple-Input/Multiple Output
MNO	Mobile Network Operator
NCI	NATO Communications and Information Agency
NESAS	Network Equipment Security Assurance Scheme
NFV	Network Function Virtualisation
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NPN	Non-Public Networks
NR	New Radio
NSA	Non-Standalone
NTN	Non-Terrestrial Networks
PKI	Public Key Infrastructure
RAN	Radio Access Network
SA	Standalone
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SDN	Software Defined Networking
SMS	Short Message Service
SS7	Signalling System number 7
SUPI	Subscription Permanent Identifier
UAS	Unmanned Aerial Systems
UDG	Unified Distributed Gateway
UDM	Unified Data Management
UE	User Equipment
UHD	Ultra High Definition
UNC	Unified Network Controller
UPCF	Unified Policy Control Function
URLLC	Ultra-Reliable Low-Latency Communication

2. Introduction

Emerging and disruptive technologies (EDT) are a domain of great power competition. Countries that are able to control and master advanced technology can project national power globally, and have a long-term military advantage. Over the past centuries, telecommunications has been used by states for political and military end.[1]

China perceives telecommunication networks as tools through which to project power.[2] This includes the use of 5G networks for spreading disinformation and for kinetic operations.[3] In the military context, the value of control over information and communication technologies (ICT) AIfor the military is underlined, and Chinese scholars and officers advise that the country must 'carefully study and comprehensively demonstrate and formulate our army's 5G technology development strategy for defeating the enemy'.[4] Moreover, the Chinese company Huawei offers affordable 5G technology, which makes it attractive to many countries.[5] The Centre for Security and Emerging Technology (CSET) Policy Brief outlines a wide range of powers and resources used by the Chinese government to ensure that Huawei dominates foreign competition.[6] The brief notes that Huawei is likely larger than the three other major vendors, Ericsson, Nokia and Samsung; it secures about half of the global 4G LTE market, largely in emerging economies. Its prices are typically at least 30% lower than those of its competitors, thanks to government subsidies.[7]

Cybersecurity experts have warned of supply chain and network security risks associated with Chinese 5G technology.[8] For example, high-risk 5G components in edge computing and Radio Access Network (RAN) could expose core network elements to software and hardware vulnerabilities.[9] In the event of a crisis or armed conflict, the presence of Huawei's equipment in telecommunication networks of nations hosting US troops could undermine US capabilities for command and control (C2) and power projection, as well as create new security risks.[10] Due to the security concerns, several EU and NATO countries have banned the use of Chinese equipment in their 5G networks, and others are phasing out equipment of the so-called high risk vendors within a few years.[11]

At the same time, China and Russia aim to reduce their dependence on Western technology. Russia's 2021 National Security Strategy notes that the use of foreign ICT renders the country vulnerable to foreign influence and underscores the aim to strengthen the state's sovereignty in cyberspace. Russia's policy measures in the area of information security include preventing foreign control over the functioning of Russia's telecommunications networks and prioritising the use of Russian ICT.[12] Russia runs cyberspace operations to advance its military, political and strategic objectives. [13] The deployment of 5G for military purposes could augment in the future Russia's artificial intelligence (AI)-enabled information warfare and machine learning (ML)-enabled cyberspace operations.

NATO recently recognised the need to win the technological adoption race vis-a-vis global competitors' such as China.[14] In 2021, NATO leaders recognised for the first time that 'China's growing influence and international policies can present challenges' to the Alliance.[15] They also stated that China's behaviour challenges the rules-based international order and 'areas relevant to Alliance security', and that China's 'frequent lack of transparency'

1 Rush Doshi and Kevin McGuiness, 'Huawei Meets History, Great Powers and Telecommunications Risk, 1840–2021', Brookings Institution, March 2021, https://www.brookings.edu/wp-content/uploads/2021/03/Huawei-meets-history-v4.pdf.

2 'Final Report: National Security Commission on Artificial Intelligence', 22 April 2021.

3 'Final Report: National Security Commission on Artificial Intelligence'.

4 Rush Doshi, Emily De La Bruyere, Nathan Picarsic, and John Ferguson, 'China as a "Cyber Great Power". Beijing's Two Voices in Telecommunication', Brookings Institution, April 2021, https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf.

5 'Final Report: National Security Commission on Artificial Intelligence'.

6 Alex Rubin, Alan Omar Loera Martinez, Jake Dow, and Anna Puglisi, 'The Huawei Moment', CSET Policy Brief, July 2021, https://doi.org/10.51593/20200079.

7 Alex Rubin, Alan Omar Loera Martinez, Jake Dow, and Anna Puglisi, 'The Huawei Moment'.

8 For example, see 'National Security Implications of Fifth Generation (5G) Mobile Technologies', Congressional Research Service, 23 April 2021, https://fas.org/sgp/crs/natsec/IF11251.pdf.

9 'Edge vs. Core: An Increasingly Less Pronounced Distinction in 5G Networks', Cybersecurity and Infrastructure Security Agency, 2020, https://www.cisa.gov/publication/5g-edge-vs-core [accessed 22 July 2021].

10 Elsa B. Kania, 'Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy', 7 November 2019, Center for a New American Security, https://www.cnas.org/publications/reports/securing-our-5g-future.

11 For example, most recently Sweden and Romania. See Johan Ahlander and Supantha Mukherjee, 'Swedish Court Upholds Ban on Huawei Selling 5G Network Gear', Reuters, 22 June 2021, https://www.reuters.com/technology/swedish-court-upholds-ban-huawei-selling-5g-network-gear-2021-06-22/.

12 'Указ Президента Российской Федерации от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации"' [Decree of the President of the Russian Federation of 02 July 2021 No. 400 'On the National Security Strategy of the Russian Federation', Official Internet Portal of Legal Information, 3 July 2021, http://publication.pravo.gov.ru/Document/View/0001202107030001.

13 Samuel Bendett, Mathieu Boulègue, Richard Connolly, Margarita Konaev, Pavel Podvig, Katarzyna Zysk, 'Advanced military technology in Russia. Capabilities and implication', September 2021, Chatham House, https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-23-advanced-military-technology-in-russia-bendett-et-al.pdf.

14 'New Focus on Emerging and Disruptive Technologies Helps Prepare NATO for the Future', NATO, 3 March 2021, https://www.nato.int/cps/en/natohq/news_181901.htm.

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

is concerning.[16] According to NATO deputy secretary general Mircea Geoană, resilient telecommunications networks are essential for NATO's political and military-strategic interests.[17] In order to enhance resilience, the Alliance is implementing baseline requirements for civilian telecommunications, including 5G, and will 'establish, assess, review and monitor resilience objectives to guide nationally developed resilience goals and implementation plans.'[18] At the 2021 Brussels Summit, NATO also agreed to 'foster technological cooperation among Allies in NATO, promote interoperability and encourage the development and adoption of technological solutions to address our military needs'.[19] To support the dual use of EDT for security, NATO announced a civil-military Defence Innovation Accelerator and an Innovation Fund.[20]

NATO armed forces and command structure need to be well informed about the opportunities 5G technologies provide for improving Allied defence and deterrence. At the same time, they need to have a full understanding of the security risks inherent in 5G networks. How do risks related to public (commercial) networks impact NATO's ability to conduct military operations? For example, the confidentiality, integrity, and availability of data and telecommunication infrastructure (and trust therein) is essential for enabling secure and reliable military command and control (C2), communications, and decision-making. If networks are compromised or under the control of adversaries, there may be repercussions to NATO's Military Instrument of Power and to the Euro-Atlantic defence and deterrence. NATO should ensure that these risks are prevented or mitigated and, at the same time, develop means to deploy 5G technology to support its Military Instrument of Power.[21]

2.1. Scope

This Research Report examines supply chain and network security challenges associated with 5G technology, outlining key vulnerabilities, threats, and risks in public and private (including military) 5G networks.[22] The report aims to raise awareness on how operating through public and private 5G networks can impact NATO's deterrence and defence. It aims to provide decision-makers with evidence-based information on vulnerabilities, threats and risks associated with 5G networks, which may impact NATO peacetime missions and military operations. The report is based on non-systematic literature view, and consultations with stakeholders, including discussions at the CCDCOE's workshop, held on 9 June 2021.

First, the paper gives an overview of the recent legislative, regulatory and policy developments in the area of 5G network security and resilience in the EU, focusing on the recommendations of 'Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures'.[23] It reviews changes of national legislation in five EU member states (Estonia, Latvia, Lithuania, Poland, and Germany) and two non-EU NATO nations (the US and Norway). These countries were selected for the use cases because, in the event of a military deployment of NATO forces to the Baltic States from elsewhere in Europe or from North America, one potential geographical trajectory of moving troops and equipment could be through a sea harbour in Germany and road transportation infrastructure in Germany, Poland, and the Baltic States. Norway was included in the study because its advanced public safety and military 5G network use cases (5G-VINNI and FUDGE 5G pilot projects) offer a valuable comparison with the EU initiatives.[24] The United States was also included for similar reasons.

Secondly, the paper describes the current status of 5G network rollout and allocation of radio spectrum in these countries. In addition to Mobile Network Operators (MNOs), deployments of public 5G networks, an overview of 5G trials and military 5G use cases (in Latvia, Norway, and Estonia) are included in the paper. Thirdly, a brief overview of progress in the standardisation of 5G technology and security architecture, and an overview of certification of 5G equipment and services, are provided. Fourthly, the Research Report highlights key supply chain and network security challenges to both public and military 5G networks, reviewing threat and risk assessments in academic papers and industry sources (such as telecommunication manufacturers and cloud providers, white papers, workshop presentations, and social science journal articles). The final section of the Research Report proposes three 5G use cases for NATO and identifies areas for subsequent research.

16 'Brussels Summit Communiqué'.

17 '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.

18 'Brussels Summit Communiqué'.

19 'Brussels Summit Communiqué'.

20 'Brussels Summit Communiqué'.

21 The Military Instrument of Power contributes to the achievement of the Alliance's political objectives in coordination with other instruments of power through a whole-of-government approach, which combines diplomatic, information, economic, and military instruments based on principles such as civilian-military interaction, coherence of actions, and cooperation with external actors. 'NATO Warfighting Capstone Concept', Allied Command Transformation, https://www.act.nato.int/nwcc [accessed 22 July 2021].

22 Of note, the report does not discuss the potential that 5G technology offers to the military, economy and society. The focus is supply chain and network security of public and private 5G networks.

23 'Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures', NIS Cooperation Group, January 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

24 'Norway Main Facility Site', 5G-VINNI, https://www.5g-vinni.eu/norway-main-facility-site/ [accessed 21 June 2021].

2.2. Definition

5G is a fifth-generation mobile network technology, operating on sub-6 GHz and 20–60 GHz millimetre-wave (mmWave) frequencies. Its technological enhancements include a dramatically faster speed, greater connectivity, greater reliability and reduced latency. 5G is expected to enable the use of future digital technologies and expand its use to new industries. Examples of 5G vertical services include 3D video, UHD screens, augmented reality, industry automation, smart homes and cities, smart transportation, self-driving cars, and e-Health. 5G enables more devices, and new kinds of devices, to be connected.

From a technical point of view, this Research Report adopts the definition of 5G technology which is commonly used by NATO nations and the NATO Communications and Information Agency (NCI (Agency). This definition is provided in the 'IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond' (IMT 2020 Vision) released by the International Telecommunications Union in 2015.[25] 5G technology officially started with the Third Generation Partnership Project (3GPP) Release 15, which includes both 4G LTE and 5G New Radio (5G NR). For the purposes of this paper, the concept of 5G technology includes both non-standalone (NSA), including 4G LTE components, and standalone (SA) architectures, in other words 3GPP Releases 15, 16, and beyond. It should be noted that the full potential of 5G which enable the vertical services mentioned above will be available only once the SA architecture is deployed.[26]

According to the aforementioned IMT 2020 Vision, the technology components of 5G are:

- → Software Defined Networking (SDN)
- → Network Function Virtualisation (NFV)
- → cloud-radio access network
- → enhanced mobile broadband (eMBB)
- → massive machine type communications
- → ultra-reliable and low latency communications (URLLC)
- → network energy efficiency
- → mobile terminals
- → privacy and security
- → higher data rates.

Figure 1 shows 5G usage scenarios and technology capabilities, which are the following: peak data rate, user experienced data rate, latency, mobility, connection density, energy efficiency, spectrum efficiency, area traffic capacity, spectrum and bandwidth flexibility, reliability, resilience, security and privacy, and operational lifetime.[27]

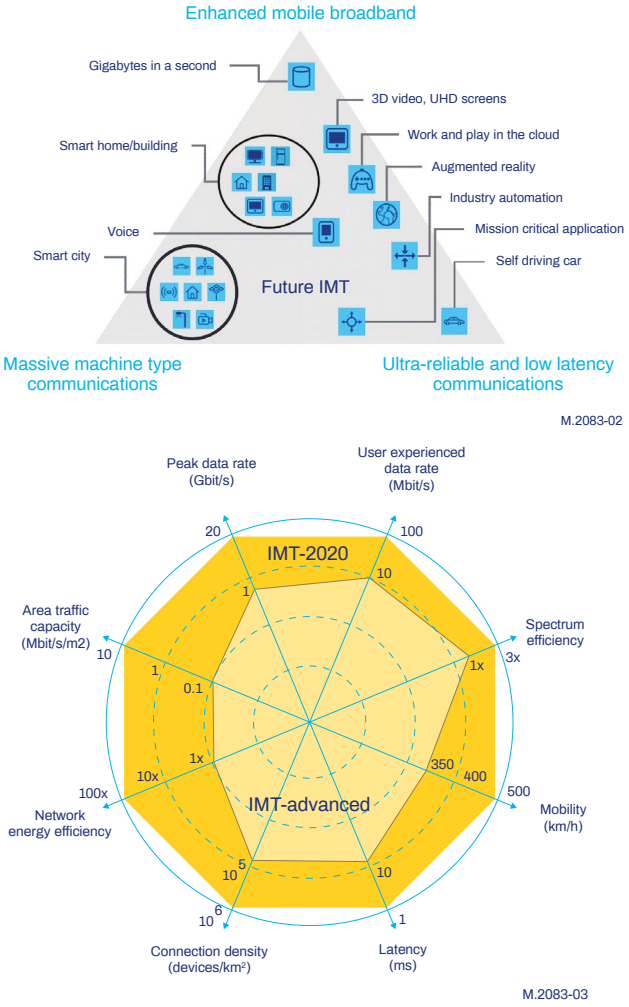

Figure 1. 5G Usage scenarios and capabilities[28]

In addition, the 5G system is composed of the following components: User Equipment (UE); New Radio (NR); and Radio Access Network (RAN), consisting of NR base stations (gNodeB); a core network; and a data network. There are five key foundations of NR:

- → mmWaves, to allow extreme spectrum bandwidth;
- → Small Cell, to allow small footprint and high-density base stations;
- → Massive multiple-input/multiple output (MIMO), to allow multiple simultaneous data streams;
- → Beamforming, to allow steerable data streams, improved radio links and reduced interference;
- → Full Duplex, to allow simultaneous transmission and reception at the same frequency.[29]

25 'IMT Vision: Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond. Recommendation M.2083–0 (09/2015)', International Telecommunication Union, 29 September 2015, https://www.itu.int/rec/R-REC-M.2083-0-201509-I/en. The NCI Agency's working paper uses this definition of 5G technology; see Luis Bastos et al., 'Potential of 5G Technologies for Military Application', 15 September 2020, NCI Agency Working Paper, http://www.mindev.gov.gr/wp-content/uploads/2020/11/Enclosure-2-Working-paper-Potential-of-5G-technologies-for-military-application.pdf.

26 Release 15 defines a new radio interface (5G NR) and improvements to 4G LTE and addresses eMBB usage scenarios. Release 16 comprises the necessary technology enablers for eMBB, URLLC, and mMTC. Luis Bastos et al., 'Potential of 5G Technologies for Military Application'.

27 'IMT Vision: Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond'.

28 'IMT Vision: Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond'.

29 Bastos et al., 'Potential of 5G Technologies for Military Application'.

There are three key foundations of the core network:

→ NFV, to allow a fully virtualised architecture
→ Network Slicing, to allow logical end-to-end networks tailored to usage/customer needs
→ Edge Computing, to allow resources where they are needed (close to the access network).[30]

Finally, for the purposes of this Research Report, 'threat' is defined as a circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.[31]

Risk is a function of impact and the likelihood that a threat will occur. System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems.[32]

3. Policy and Regulatory Developments Related to 5G Networks

3.1. Legal Framework for 5G Radio Spectrum Assignment in the EU

For the countries covered in this Research Report, with the exception of Norway, the overall legal framework for communications networks and MNOs is laid out in the 2018 European Electronic Communications Code (ECC), which EU member states had to transpose into their national legislation by the end of 2020.[33] Harmonised rules outline the conditions for spectrum availability and use across the EU, taking into account both interoperability (including avoidance of harmful radio interference) and effective use for the purposes of the EU single market. This overall framework also applies to the allocation and assignment of radio spectrum designated for 5G.

The EU 2016 5G Action Plan and subsequent EU decisions called for the harmonisation of the 700 MHz (694–790 MHz), 3.6 GHz (3.4–3.8 GHz), and 26 GHz (24.25–27.5 GHz) frequency bands, which are called 'pioneer spectrum bands' for 5G networks, and a list of additional bands below and above 6 GHz.[34]

Radio spectrum allocation and the issuance of authorisations for MNOs in the relevant frequency bands ('rights of use for radio spectrum') are within the competence of national communications regulators. Within the boundaries specified by the ECC and national law, the process of spectrum assignment is, broadly speaking, up to the national governments, and for high-demand frequency bands, competitive tendering is common.[35] All EU countries in the scope of this paper rely on auctions for assigning the 5G spectrum bands and issuing the relevant licences. The deadline to assign the 3.4–3.8 GHz spectrum band licences in the EU was 31 December 2020, although the process has been delayed in some countries due to legal disputes.

To ensure free and fair use, there is a strict limitation on conditions that can be applied to a spectrum licence issued to an operator. Generally, these must be non-discriminatory, proportionate, and transparent, and justified on the grounds of ensuring technical quality, effective use,

30 Bastos et al., 'Potential of 5G Technologies for Military Application'.

31 'CMCC Glossary and Acronyms. Version 1.10', Carnegie Mellon University and Johns Hopkins University Applied Physics Laboratory LL, 30 November 2020.

32 'CMCC Glossary and Acronyms. Version 1.10'.

33 The ECC's principles remain consistent with the preceding 2002 Electronic Communications Framework, which the 2018 Code superseded. The ECC is addressed to EU member states. For Norway and other European Free Trade Area/European Economic Area (EEA) countries, EU law has to undergo EU-EFTA negotiations to become applicable (possibly with adaptations), which can take several years. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJEU L 321/36, 17 December 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1547633333762&uri=CELEX:32018L1972.

34 '5G for Europe: An Action Plan', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2016) 588, European Commission, 14 June 2016, https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2016)588, p. 5; for EU harmonised spectrum decisions, see 'Frequency Bands for Electronic Communication', EurLex, https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32019D0235.

35 'National 5G Plans and Strategies', European 5G Observatory, https://5gobservatory.eu/public-initiatives/national-5g-plans-and-strategies/. Note that it is very questionable whether public procurement rules are relevant in spectrum tenders; also, the extent to which operators buying equipment are subject to public procurement rules is not analysed here. In any case, EU procurement rules set no obligation to award contracts to the highest bidder; the procurer can take into account, among other things, security standards and impose measures to protect public security. Moreover, bidders can be excluded on the basis of risk to essential national security interests. Defence and security procurements, furthermore, are relieved from some competition rules, e.g. they can exclude third country operators. See 'Factsheet: The EU Toolbox for 5G Security', European Commission, 8 March 2021, https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

preventing radio interference, or safeguarding fundamental public interests such as public health and environmental safety. Similar grounds apply for amending or withdrawing an already issued licence.[36]

Outside of such designated frequency ranges, the Estonian Defence Forces (EDF) must apply for a frequency authorisation, which is granted as a priority and where certain conditions (efficient and timely use) are alleviated.[37] ECC requirements are set without prejudice to the actions of member states in the area of defence, including the right of member states to organise and use their radio spectrum for defence and defence networks.[38] Such uses are regulated by national law but must observe international treaty obligations (such as the International Telecommunications Union [ITU] Constitution and Convention and radio spectrum coordination agreements) and comply with electromagnetic compatibility and radio interference rules. With the Estonian radio frequency allocation plan, for example, certain frequencies may be (and are) allocated for exclusive use by the EDF in accordance with specified technical requirements.

3.2. EU 5G Risk Assessment and Toolbox

5G supply chain and network security aspects are covered by a broader EU legislative framework, including the ECC, the Directive on Security of Network and Information Systems (the NIS Directive)[39] and its future revision,[40] the EU Cybersecurity Act, and the FDI framework.[41] While the EU's focus concerning 5G technologies is on the societal and economic opportunities their roll-out will bring, security has been on the mind of EU member states for several years as a prerequisite for a successful deployment, and various related policy and legal instruments have been adopted, starting in 2019. In March 2019, the European Council called for a concerted approach to the security of 5G networks; the Commission subsequently adopted Recommendation 2019/534 on the cybersecurity of 5G networks,[42] followed by a coordinated risk assessment in October 2019[43] and the 'Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures' (the Toolbox), adopted in January 2020.[44] The Toolbox implementation was supported by a related Commission communication.[45] As the main risk mitigation policy instrument, the Toolbox recommends strategic, technical, and supporting actions to address the identified risks related to the following aspects: insufficient security measures, supply chain, modus operandi of main threat actors, interdependencies between 5G networks and critical infrastructure, and end-user devices, including the Internet of Things (IoT).

EU reports published in mid- and late 2020 found that progress had been made towards implementation of the Toolbox measures.[46] In particular, this involved reinforcing the powers of national regulatory authorities regarding a 5G rollout, introducing national supplier risk assessment and restricting the involvement of high-risk suppliers, and reviewing security and resilience requirements for MNOs. However, member states have been found to be lagging on several action lines, such as reducing existing dependencies on high-risk suppliers and developing and carrying out multi-vendor strategies for MNOs individually and at the national level, as well as advancing national screening mechanisms for foreign direct investments (FDI). As of the end of 2020, two-thirds of MNOs in the EU were still using a single vendor for 5G core network equipment, and almost half of RAN equipment was provided by non-EU vendors. The majority of MNOs have indicated that they would need more than five years to replace a high-risk 5G vendor without significant cost and outside the normal

36 European Electronic Communications Code (EECC) Articles 12–13; 18–19; 47; Annex I. For an example of national implementation, see Estonia's Electronic Communications Act, RT I 2004, 87, 593, 8 December 2004, § 11–16, https://www.riigiteataja.ee/en/eli/517122020006/consolide.

37 Electronic Communications Act, § 21.

38 'EECC', recitals 108, 134, Articles 1, 49 and 53.

39 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp. 1–30, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

40 European Commission, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM (2020) 823 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823.

41 Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, as amended, OJ L 79I , 21.3.2019, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0452.

42 European Commission, 'Commission Recommendation of 26 March 2019 on Cybersecurity of 5G Networks', C(2019) 2335 final, OJ L 88, 29.3.2019, pp. 42–47, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019H0534.

43 NIS Cooperation Group, 'EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks', 9 October 2019, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

44 'Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures'. In addition, the European Cybersecurity Agency (ENISA) has published two 5G threat assessment reports. See 'ENISA Threat Landscape for 5G Networks', ENISA, 21 November 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks; and 'ENISA Threat Landscape for 5G Networks Report' (ENISA, 14 December 2020), https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

45 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Secure 5G Deployment in the EU – Implementing the EU Toolbox', COM/2020/50 final, 29 January 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0050.

46 NIS Cooperation Group, 'Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity', July 2020, https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity; European Commission, 'Report on the Impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G Networks', SWD(2020) 357 final, 16 December 2020, https://digital-strategy.ec.europa.eu/en/library/commission-reviews-impacts-eu-process-and-eu-toolbox-and-sets-out-next-steps-ensure-secure-5g.

replacement cycle.[47] However, according to Bloomberg, some MNOs in the EU member states have already begun removing Huawei equipment from their urban wireless networks, and at the time of publication of this Research Report, there is no publicly available information about possible government compensation for replacing these components with trusted vendors' components.[48]

The EU's recently adopted new cybersecurity strategy sets out the implementation of the Toolbox as one of its key strategic initiatives; the full implementation of the Toolbox is called for by the end of the second quarter of 2021.[49] The cybersecurity strategy encourages member states and EU bodies to engage in coordinated risk mitigation, specifically with regard to minimising exposure to high risk suppliers and avoiding dependency on these suppliers at both national and EU level, while also taking into account any new significant developments or risks. Member states are invited to make full use of the Toolbox in further investments into digital capacities and connectivity.[50] However, it is primarily within the remit of the member states to adopt security measures, and the European Commission lacks hard measures to enforce actual implementation, which will depend on the commitment and capacity of member states and their legislative processes, as well as the deemed suitability of particular Toolbox measures under national circumstances.

3.3. EU Legal Requirements for 5G Networks

The 2018 ECC obliges EU member states to ensure that (fixed and mobile) network operators and electronic communications service providers take 'technical and organisational measures to appropriately manage the risks posed to the security of networks and services'. The measures must be appropriate to the risk, have regard to the state of the art, and prevent and minimise the impact of security incidents both on service users and on other networks and services.[51] Similar obligations under EU law have existed since 2002; however, member states have been free to choose the means they consider appropriate to meet this requirement, and accordingly, national approaches vary.

The ECC tasks the European Union Agency for Cybersecurity (ENISA) with coordinating between member states to ensure that divergences in national requirements do not create security risks or impede the EU's internal market. Since December 2020, further implementing acts for risk management may be adopted by the EU Commission (i.e. not subject to formal approval by member states); however, these do not prevent member states from adopting tougher security requirements. Such measures should also, as far as possible, be based on European and international standards.[52] In 2021, the European Commission tasked ENISA with developing a pan-European certification scheme for 5G networks.[53]

Radio spectrum assignment status	Estonia	Germany	Latvia	Lithuania	Norway	Poland
700 MHz	No	Yes	No	No	Yes	No
3.4–3.8 GHz	No	Yes	Yes	No	No	No
24.25–27.5 GHz	No	Yes	No	No	No	No

Table 1. 5G Spectrum Available for Commercial Use

47 BEREC, 'Report of BEREC Recent Activities Concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of Suppliers and Strengthening National Resilience)', BoR (20) 228, 10 December 2020, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/9726-report-of-berec-recent-activities-concerning-the-eu-5g-cybersecurity-toolbox-strategic-measures-5-and-6-diversification-of-suppliers-and-strengthening-national-resilience.

48 Helene Fouquet and Tara Patel, 'France's Huawei Ban Begins to Kick In With Purge in Urban Areas', Bloomberg, 1 March 2021, https://www.bloomberg.com/news/articles/2021-03-01/france-s-huawei-ban-begins-to-kick-in-with-purge-in-urban-areas?srnd=technology-vp.

49 European Commission, High Representative of the Union for Foreign Affairs and Security Policy, 'The EU's Cybersecurity Strategy for the Digital Decade', Joint Communication to the European Parliament and the Council, JOIN(2020) 18 final, 16 December 2020, p. 11, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

50 An appendix to the strategy sets out three main EU-level objectives with regard to 5G cybersecurity, with concrete sort-and mid-term actions and lead actors specified: (1) ensuring further convergence in risk mitigation approaches across the EU, (2) supporting continuous exchange of knowledge and capacity building, and (3) promoting supply chain resilience and other EU strategic security objectives. For these, the Commission, with the support of ENISA, will 'work closely' with member states to fulfil these objectives and actions. Detailed arrangements and milestones for the main actions were slated to be agreed upon in early 2021.

51 EECC, Article 40.

52 EECC, Article 40.

53 ENISA, 'Securing EU's Vision on 5G: Cybersecurity Certification', 3 February 2021, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification/.

3.4. National Status of 5G Service Provision

3.4.1. ESTONIA

Amendments to the Electronic Communications Act adopted in May 2020 authorise the government to impose obligations on operators to provide information on the hardware and software used in the communications network, and prohibit the use of hardware and software for which such information is not provided. Furthermore, for the purposes of national security, operators may be required to gain prior approval from the competent authority for the specific hardware and software used.[54] The notification and approval authorities are to be appointed and the relevant procedures established by a government regulation.[55] A draft regulation was submitted to the government in early March 2021 but failed to gain government approval over concerns of legal clarity.[56] A new spectrum auction for 5G in the 3.6 GHz bands (for up to four licences) has been announced, with an application deadline in November 2021 (tenders for the frequency bands 700 MHz and 26 GHz have not been announced).[57]

3.4.2. GERMANY

On 23 April 2021, the Bundestag passed a law to increase the security of information technology systems (IT Security Act 2.0), which increases the security measures of cellular networks. MNOs have to meet high security requirements, and critical components have to be certified.[58] The law stipulates that a 5G technology vendor can be considered untrustworthy if, among other things, the company has provided false information, does not support security checks or does not immediately report and eliminate IT weaknesses.[59] According to Andreas Könen, director of General Cyber and Information Security at the German Federal Ministry of the Interior, the new law prescribes a procedure that allows the ministry to exclude the use of critical components if they pose a threat to national security and enables evaluating the trustworthiness of the so called high-risk vendors. Vendors must declare that they will comply with a set of criteria for trustworthiness, and the usage of equipment can be prohibited both ex-ante and ex-post if a potential threat to national security is identified or when the declaration is violated.[60]

The German auction of 3.6 GHz band frequencies concluded in June 2019, resulting in the allocation of the assigned spectrum to four operators.[61] The auction of 700 MHz band frequencies concluded in June 2015.[62]

3.4.3. LATVIA

With the 2019 launch of its first two 5G networks and plans for domestic production of 5G routers, Latvia has been among the 5G forerunners in Europe.[63] In February 2020, the Latvian government approved a national roadmap for 5G public mobile communication network deployment. The document provides an overview of spectrum allocation, deployment of commercial networks in large urban centres and coverage obligations planned for the allocation of 700MHz related to railways and roads. In November 2020, the country inaugurated a 5G test site, the first of its kind, at the military base of Ādaži.[64]

3.4.4. LITHUANIA

As of February 2021, the national regulator was preparing for the first 5G spectrum auction in 700 MHz, initially planned for Q1 2021. The work had been hampered by slow progress in negotiation with Russia over the 3.5 GHz band.[65] In November 2020, Telia became the first operator in the country to deploy a trial 5G network on the basis of temporary, non-commercial allocation of 3.5 GHz by the regulator,[66] while also deciding to replace all its Huawei 4G infrastructure and exclude the supplier

54 Electronic Communications Act, § 11 subsection 41, 87 subsection 21 and 22, Riigi Teataja [State Courier], https://www.riigiteataja.ee/en/eli/517122020006/consolide.

55 Electronic Communications Act.

56 Marko Tooming, 'Valitsus lükkas sidevõrkude turvalisuse määruse vastuvõtmise edasi' [The Government Postponed the Adoption of the Regulation on Communications Network Security], ERR, 3 April 2021, https://www.err.ee/1608130453/valitsus-lukkas-sidevorkude-turvalisuse-maaruse-vastuvotmise-edasi.

57 'Avalikud konkursid ja arutelud' [Public Tenders and Discussions], Consumer Protection and Technical Regulatory Authority, https://www.ttja.ee/ariklient/ametist/avalikud-konkursid/avalikud-konkursid-ja-arutelud#avaliku-konkursi-jt [accessed 26 July 2021].

58 'Gesetz zur Erhöhung der IT-Sicherheit mit Koalitionsmehrheit beschlossen' [Law to Increase IT Security Passed by a Coalition Majority], Parliament of Germany, https://www.bundestag.de/dokumente/textarchiv/2021/kw16-de-sicherheit-informationstechnischer-systeme-834878 [accessed 26 July 2021].

59 'Bundestag beschließt Hürden-für-Huawei-Gesetz' [Bundestag Passes Hurdles for Huawei Law], *Spiegel*, 23 April 2021, https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-2-0-bundestag-beschliesst-huerden-fuer-huawei-gesetz-a-2f50a7dc-e5f5-4b35-ba30-1ecbf1db4eed.

60 Andreas Könen, *Cyber Week*, 20 July 2021, Tel Aviv University, https://cw2021.b2b-wizard.com/expo/agenda.

61 Bundesnetzagentur (BNetzA), 'Bundesnetzagentur Assigns 5G Spectrum from Auction', 5 September 2019, https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2019/20190904_5Gspectrum.html.

62 Bundesnetzagentur (BNetzA), Mobiles Breitband, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/MobilesBreitband-node.html [accessed 20 June 2021].

63 Andris Tauriņš, Gunvaldis Leitens, and Lūcija Strauta, 'The Technology, Media and Telecommunications Review: Latvia', *Law Reviews*, 3 February 2021, https://thelawreviews.co.uk/title/the-technology-media-and-telecommunications-review/latvia.

64 Olevs Nikers, '5G Technologies in Latvia Advance Military Capabilities and National Economy', *Eurasia Daily Monitor* 17, no. 178, 15 December 2020, https://jamestown.org/program/5g-technologies-in-latvia-advance-military-capabilities-and-national-economy/.

65 BNS/TBT Staff, 'Lithuania Holds No Direct Talks with Russia on Border Frequencies: Regulator', *Baltic Times*, 22 February 2021, https://www.baltictimes.com/lithuania_holds_no_direct_talks_with_russia_on_border_frequencies___regulator/.

66 Communications Regulatory Authority of the Republic of Lithuania (RRT), 'RRT Shares the 5G Development Plans in Lithuania', 20 November 2020, https://www.rrt.lt/en/rrt-shares-the-5g-development-plans-in-lithuania/.

from participating in the building of the 5G network.[67] This trend has been confirmed by the Lithuanian parliament's passing of amendments to the Communications Act and to the Law on Protection of Objects of Importance to Ensuring National Security in May 2021. Taking effect on 1 July 2021, these amendments provide for a compliance check of suppliers and the possibility to exclude from the electronic communications market manufacturers and suppliers deemed unreliable.[68] As of the beginning of 2021, there were no specific plans for the 26 GHz band in Lithuania.[69]

3.4.5. NORWAY

The Norwegian government has not announced any plans to specifically ban particular suppliers, but it has prioritised a risk assessment of suppliers and network security. As of September 2020, Huawei can participate in the development of 5G RAN, but only in up to 50% of the network. Norway's armed forces are implementing the 5G-VINNI and FUDGE 5G pilot projects.[70]

3.4.6. POLAND

In September 2020, the government presented draft amendments to cyber security legislation that introduced a system of risk assessment for suppliers of connectivity, software, and network infrastructure. The outcome of such risk assessment would influence not only suppliers' access to new infrastructure but also their retention in the existing infrastructure. [71] The draft law is still in the process of consultations and has been criticised as contributing to further delays in 5G rollout in Poland.[72]

3.4.7. BALTIC COOPERATION

In September 2020, the Baltic States and Poland signed a memorandum of intent on supporting the development of Via Baltica 5G/Cross-border corridors for Connected and Automated Mobility, connecting Tallinn, Riga, Kaunas, and the Lithuanian-Polish border.73 The focus of cooperation is road safety, sustainable mobility and innovation in transportation systems, as well as the testing of autonomous vehicles.74 Under the Three Seas Initiative, Lithuania has proposed Via-Baltica/Rail-Baltica 5G cross-border transport corridors for connected and automated mobility.

3.5. Developments in the US

In the US in 2020, the White House released the National Strategy for 5G security, the Department of Defense (DoD) released a 5G strategy, and the CISA released its own 5G strategy. In addition, the DoD released a 5G implementation plan detailing current activities. Section 224 of the FY2021 National Defense Authorisation Act directs DoD to create a 5G governance structure, and Section 225 directs DoD to demonstrate the maturity of 5G component technologies.[75] In 2020 the US DoD announced $600 million would be made available for developing 5G test beds at 12 military sites where 5G experimentation and testing together with the industry will be conducted. The use cases include smart warehousing, distributed command and control, and augmented and virtual reality training. The 5G test bed at Joint Base San Antonio includes the DoD 5G Core Security Experimentation Network.[76]

August 2020 saw the launch of the Clean Network program, an attempt at a comprehensive approach to the security of 5G communications used by the US government. Building upon an earlier Clean Path initiative, the Clean Network involved six lines of effort aimed primarily at containing China's influence in communication networks located in the US and used by the US. In that vein, the US government called upon other states and the private sector to join the initiative. As of March 2021, about 60 states have signed a memorandum of understanding with the US or have in some other way aligned themselves with the initiative, and about 180 private sector entities have declared their support. The initiative requires that network traffic entering and exiting US diplomatic facilities abroad does not use transmission, control, computing, or storage equipment from untrusted IT vendors in 5G networks.

---

67 Reuters, 'Telia to Remove All Huawei Equipment in Lithuania', Reuters, 30 November 2020, https://www.reuters.com/article/huawei-lithuania-idUSL8N2IG2RY.

68 BNS, 'Lithuania Bans "Unreliable" Technologies from Its 5G Network', LRT English, 25 May 2021, https://www.lrt.lt/en/news-in-english/19/1417429/lithuania-bans-unreliable-technologies-from-its-5g-network#:~:text=The%20Lithuanian%20parliament%20has%20voted,deploying%205G%20mobile%20network%20technology. Official texts available at https://www.e-tar.lt/portal/en/legalAct/399b0b90c2df11eba2bad9a0748ee64d and https://www.e-tar.lt/portal/en/legalAct/774554a0c2df11eba2bad9a0748ee64d (in Lithuanian).

69 BNS, 'Lithuania Bans "Unreliable" Technologies'.

70 Ericsson provides a 5G core network which runs on a Nokia cloud platform. Huawei and Ericsson equipment are used for RAN. 'Norway Main Facility Site', 5G-VINNI, https://www.5g-vinni.eu/norway-main-facility-site/ [accessed 20 June 2021].

71 'Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy Prawo telekomunikacyjne', Komitet Rady Ministrów do spraw Cyfryzacji, January 2021, https://www.gov.pl/web/krmc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-telekomunikacyjne.

72 Msnet, 'Pracodawcy RP: Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa to dalsze opóźnienia we wdrażaniu sieci 5G', Telepolis, 9 February 2021, https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/pracodawcy-rp-ustawa-o-krajowym-cyberbezpieczenstwie-opoznienia-5g.

73 '5G Connected and Automated Mobility (CAM)', *European 5G Observatory*, https://5gobservatory.eu/5g-trial/5g-connected-and-automated-mobility-cam/ [accessed 20 June 2021].

74 Ministry of Digital Affairs, '5G – współpraca państw bałtyckich', 21 September 2020, https://www.gov.pl/web/cyfryzacja/5g--wspolpraca-panstw-baltyckich.

75 The US Congress passed the Secure 5G and Beyond Act requiring the president to develop a 5G protection strategy. Section 254 of the FY2020 (NDAA) required the secretary of defense to develop a DOD 5G strategy. See 'National Security Implications of Fifth Generation (5G) Mobile Technologies', Congressional Research Service, 4 June 2021, https://fas.org/sgp/crs/natsec/IF11251.pdf.

76 'DoD Names Seven Installations as Sites for Second Round of 5G Technology Testing, Experimentation', US Department of Defense, 3 June 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2206761/dod-names-seven-installations-as-sites-for-second-round-of-5g-technology-testin/.

Although the Clean Network program will help to reduce the impact of 5G supply chain related concerns globally, it cannot by itself mitigate the security risks associated with global 5G deployment. As a result, in 2020, the Office of the Under Secretary of Defense for Research and Engineering announced their Operate Through program, a key part of the DoD 5G Initiative. This program is focused on ensuring that the DoD and its partners can leverage any and all 5G infrastructure, in spite of adversary market manipulations and potential supply-chain-related concerns. Although this program is focused on mitigating supply chain risks, its goals appear to be broader than just the supply chain; they also focus on harnessing security across the 5G architecture and ensuring that the US and its allies can leverage 5G when needed in support of global operations. While it remains to be seen how the Biden administration assesses its predecessor's policies concerning 5G, no major overhauls are expected in the overall approach to 5G.

Of the countries covered in this study, all but Norway and Germany have signed joint declarations or memoranda of understanding with the US, aligning themselves with the US approach in some way. The first of these was Poland in October 2019, followed by Estonia in November 2019, Latvia in February 2020 and Lithuania in September 2020.

In the US, commercial 5G networks have been launched by Verizon (in October 2018 for fixed wireless access and in April 2019 for mobile services), AT&T (in December 2018 for network and in June 2019 for mobile services), Sprint (in May 2019) and T-Mobile (in July 2019).[77] In the third quarter of 2021, a cloud-native 5G network provided by the Dish Network is expected to go live in Las Vegas.[78]

4. Radio Spectrum Allocation and Deployment Status of 5G Networks

In addition to the EU 5G pioneer frequency bands, all other bands used for mobile communication can be considered as potential 5G radio spectrum. This can be achieved with dynamic spectrum sharing, where 4G and 5G can use the same radio channel simultaneously through time division.[79] The US and the EU use different radio frequency bands for mobile communication. In order to be interoperable, user equipment manufacturers need to use chipsets covering all these frequency bands. The EU-harmonised frequency bands used for mobile communication are as follows:

→ Low-band: 700 MHz, 800 MHz, 900 MHz
→ Mid-band: 1.8 GHz, 2.1 GHz, 2.6 GHz, 3.6 GHz
→ Millimetre wave: 27 GHz

Frequency bands used for mobile communication in US are as follows:

→ Low-band: 600 MHz, 700 MHz, 850 MHz
→ Mid-band: 1.7/2.1 GHz, 1.8 GHz, 1.9 GHz, 2.3 GHz, 2.5 GHz
→ Millimetre wave: 39 GHz, 28 GHz

Globally, as of July 2021, there are 177 commercial 5G networks deployed (with 185 commercial networks forecast by the end of 2021) that adhere to 3GPP standards. By 2023, according to projections, there will be 47 commercial 5G networks in Eastern Europe and 80 in Western Europe.[80] Currently, in Europe there are 173 LTE and 84 live commercial 5G network deployments.[81]

Globally, 5G network connection numbers have surged, with 401 million 5G subscriptions at the end of 2020.[82] The number of 5G connections is expected to reach 619 million globally by the end of 2021 and 3.4 billion by the end of 2025.[83] Some EU member states have introduced 5G services via Dynamic Spectrum Sharing (DSS), which is using the same radio channel for 4G and 5G users (time division).[84] This is a good start, but without the introduction of 5G pioneer bands, no additional capacity or functionality will be added to the network.

77 Frédéric Pujol, Carole Manero, Basile Carle, and Santiago Remis, '5G Observatory Quarterly Report 11 Up to March 2021', European Commission, April 2021, http://5gobservatory.eu/wp-content/uploads/2021/04/90013-5G-Observatory-Quarterly-report-11-2.pdf.

78 Nic Fildes, 'Dish Hopes to Serve up New Kind of 5G Network', *Financial Times*, 27 June 2021, https://www.ft.com/content/5e8a7d9c-784f-44b2-be9d-fddeddea209d.

79 'DSS: Dynamic Spectrum Sharing', October 2020, https://www.3gpp.org/dss.

80 '3GPP Releases 16, 17 and Beyond', 5G Americas, January 2021, https://www.5gamericas.org/3gpp-releases-16-17-beyond/.

81 '5G and LTE Deployments', 5G Americas, https://www.5gamericas.org/resources/deployments/ [accessed 23 July 2021].

82 'Worldwide 5G Connections to Reach 619 Million by the End of 2021', Help Net Security, 1 April 2021, https://www.helpnetsecurity.com/2021/04/01/5g-connections-2021/.

83 'Worldwide 5G Connections to Reach 619 Million by the End of 2021'.

84 Dynamic spectrum sharing enables quick NR deployment on existing LTE bands, with efficient pooling of the resources between LTE and NR. DSS provides a path for NR and LTE to coexist while also enabling a granular spectrum re-farming. See '3GPP Releases 16, 17 and Beyond', 5G Americas, January 2021, https://www.5gamericas.org/3gpp-releases-16-17-beyond/; https://www.3gpp.org/dss.

Mobile operators have started 5G buildout from bigger cities and are gradually moving to smaller ones. They prioritise densely populated areas in order to cover as many subscribers as possible. 5G users are conducting connection speed tests. The overview of the speed test gives information about the existing performance and coverage of 5G.[85]

4.1. 5G Radio Spectrum Coverage in the Baltic States, Poland, Germany, and Norway

At the end of March 2021, 24 EU countries have deployed 5G services (including Estonia, Latvia, Poland, and Germany), and several countries have more than one 5G service provider. Among the countries covered in this study, only Lithuania has not launched 5G services.[86] Figure 2 presents EU countries that have launched commercial 5G service.

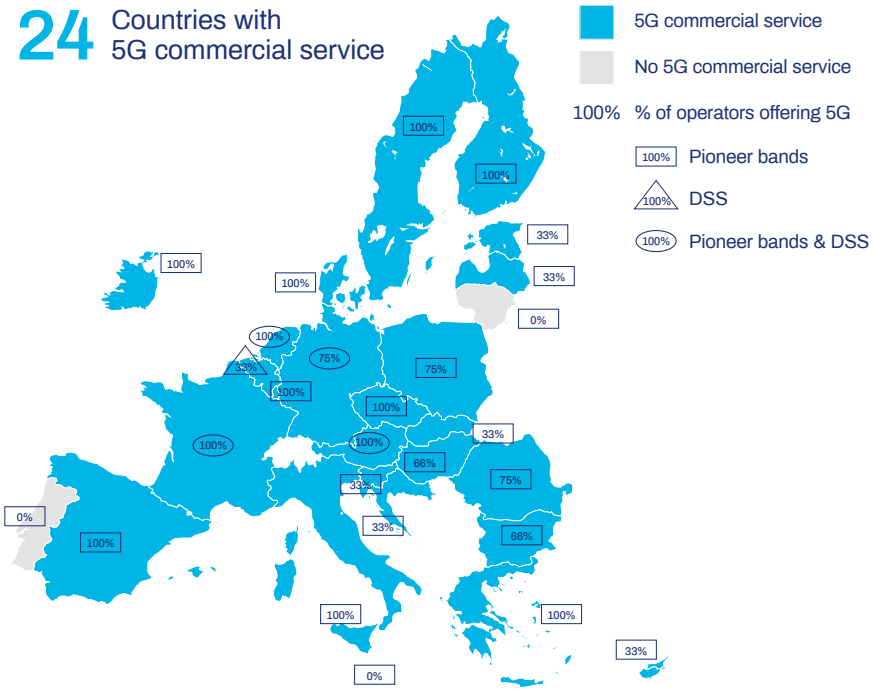

Figure 2. Countries With 5G Commercial Service

As of the end of March 2021, the most tested frequency band in Europe by far has been the 3.6 GHz band (69% of the tests), whose spectrum assignment percentage is almost 55%, whereas 46% of the spectrum in the 700 MHz band has been assigned in the EU. The 26 GHz band is still gaining traction very slowly. Among the countries included in this study, as of March 2021, the 700 MHz frequency band has been assigned only in Norway and Germany, and the 3.4–3.8 GHz frequency band only in Germany and Latvia.[87] Furthermore, it should be noted that the development of 5G networks in some parts of the assigned spectrum, such as 3.4–3.8 GHz and 700 MHz in the Baltic States, can be disturbed by the fact that Russia uses the same frequencies, partially for military purposes and partially for TV broadcasting. Attempts at reaching agreement between Russia and Estonia have so far been unsuccessful.[88]

In Estonia, Telia's commercial 5G network was launched in November 2020 in Tallinn, Tartu and Pärnu. The network uses Ericsson Spectrum Sharing technology, enabling Telia to utilise its existing frequencies, since the government has not yet auctioned off 3.5 GHz licences for 5G.[89]

In Germany, Deutsche Telekom announced that its 5G network covered 40 million Germans, representing half of the population. Services were available in over 3,000 towns and municipalities. The company announced that it planned to cover 80% of the population by the end of 2021. Telekom uses spectrum in the 2.1 GHz band to provide customers with 5G coverage in less densely populated areas, while the 3.6 GHz band is being used in large cities. Dynamic Spectrum Sharing is also being deployed. As of February 2021, Vodafone offers 7,000 5G antennas at almost 2,500 locations, providing coverage to more than 20 million Germans, with this figure set to rise to 30 million by the end of 2021. Vodafone is using the 1800 MHz band to provide 5G in densely populated cities, while the 700 MHz range is being deployed in rural areas, and the 3500 MHz band is being rolled out in high-traffic areas such as stadiums and train stations. In October 2020, Telefonica became Germany's third MNO to introduce 5G services in the 3.6 GHz band, with plans to cover more than 30% of the population by the end of 2021. The operator expects to reach around 50% by the end of 2022 and the whole country by 2025. In rural areas, the company will use Dynamic Spectrum Sharing.[90]

In Latvia, Latvian Mobile Telephone (LMT) extended commercial 5G services to the cities of Jelgava and

85 'Ookla 5G Map', https://www.speedtest.net/ookla-5g-map [accessed 23 July 2021].
86 Pujol et al., '5G Observatory Quarterly Report 11 Up to March 2021'.
87 Pujol et al., '5G Observatory Quarterly Report 11 Up to March 2021'.
88 'Russia to Play a Big Role in Estonia's 5G Future', ERR, 10 June 2021, https://news.err.ee/1100189/russia-to-play-a-big-role-in-estonia-s-5g-future.
89 Pujol et al., '5G Observatory Quarterly Report 11 Up to March 2021'.
90 Pujol et al., '5G Observatory Quarterly Report 11 Up to March 2021'.

Daugavpils in January 2020. Tele2 launched also commercial 5G services in Daugavpils and Jelgava in January 2020. By September 2020, the network was available in Riga, Jurmala and Valmiera. In January 2021, the operator announced plans to expand its 5G network with the deployment of base stations in 13 more cities over the course of 2021.[91]

In Poland, Polkomtel (Plus) provides 5G services to about 900,000 people in seven cities: Warsaw, Gdansk, Katowice, Lodz, Poznan, Szczecin, and Wroclaw. The company is planning to have coverage for 11 million Poles in 150 cities and towns with 1,700 base stations by the end of 2021. Orange Poland launched 5G services covering up to six million people in July 2020. By the end of June 2020, T-Mobile aimed to cover Warsaw, Lodz, Krakow, Poznan, Wroclaw, Plock, Opole, Czestochowa, Rzeszow, Bielsko-Biala, and Kielce. Play announced the launch of commercial 5G services in June 2020 over 50 base stations in 16 cities. Polish operators use the 2.1 GHz band.[92]

In Norway, Telenor Norge offers a 5G network in nine locations throughout the country: Kongsberg, Elverum, Bodo, Askvoll, Fornebu, Kvitfjell, Spikersuppa, Oslo, and Trondheim. In November 2020, Telenor launched a FWA 5G service. In May 2020, Telia launched 5G for customers in Lillestrøm and parts of Groruddalen in Oslo, with plans to expand to other areas in 2020. In November 2020, Telia launched a FWA 5G service.[93]

Table 2 shows MNOs in the six countries covered in this study that have deployed RAN and a core network, as well as key sites of their 5G radio (or existing 4G) spectrum coverage.

Country	MNO	RAN Provider	Core Network Provider
Estonia	Telia	Ericsson	Nokia
Estonia	Elisa	Huawei (4G)	Ericsson
Estonia	Tele2	Nokia (4G)	Nokia
Latvia	LMT	Nokia	Nokia
Latvia	Bite	Huawei	Huawei
Latvia	Tele2	Nokia	Nokia
Lithuania	Omnitel (Telia)	Ericsson	Nokia
Lithuania	Bite	Ericsson	Ericsson
Lithuania	Tele2	Nokia	Nokia
Poland	Plus (Polkomtel)	Nokia/Ericsson	Ericsson
Poland	T-Mobile	No data	No data
Poland	Orange	Ericsson	No data
Poland	Play	No data	No data
Poland	Deutsche Telekom	Huawei/Ericsson	No data
Poland	Vodafone	Ericsson/Huawei	Ericsson
Poland	O2 (Telefonica)	Nokia/Huawei/NEC	Ericsson
Norway	Telenor	Ericsson/Huawei	Nokia/Ericsson
Norway	Telia	Ericsson	Nokia
Norway	Ice	Nokia	No data

Table 2. RAN and CORE Network Providers of MNOs

91 Pujol et al., '5G Observatory Quarterly Report 11 Up to March 2021'.
92 Pujol et al., '5G Observatory Quarterly Report 11 Up to March 2021'.
93 Pujol et al., '5G Observatory Quarterly Report 11 Up to March 2021'.

4.2. 5G Trials in the EU

As part of the Horizon 2020 framework, 5G trials are funded by the European Commission under the 5G Infrastructure Public Private Partnership (5G PPP) programme.[94] As of March 2021, more than 200 5G trials have been launched in the member states,[95] including 12 'digital cross-border corridors', which have conducted live tests for Cooperative, Connected and Automated Mobility (CCAM). In addition, other trials provide applications in areas such as rail, inland waterways, ferries, and ports. Germany and Estonia are among the top 10 member states where trials are conducted. [96] Seven 5G projects were launched in June 2019, and eight projects started in November 2019. In September 2020, an additional 11 projects were launched with the objective of validating 5G ecosystems for CCAM along three new European cross-border corridors. In the Baltic States and Poland, 5G-Routes is a Horizon 2020 project that will test and validate over 150 km of the Via Baltica corridor with a ferry extension to Helsinki, including ports and maritime routes.[97]

The European Commission has launched the Connecting Europe Facility (CEF2) Digital programme, which funds a buildout of infrastructure needed for additional sites on motorways for Intelligent Transportation Systems (ITS). The programme supports the creation of trans-European 5G transport corridors.[98] Another 5G use case is a smart sea port. In Germany, the Hamburg Port Authority (HPA), in collaboration with Deutsche Telekom and Nokia, has performed tests using 5G technology to create such a port.[99] The tests included sensors on ships enabling real-time monitoring and analysis of motion and environmental data from the port area; remotely controlling the traffic flows in the port via traffic lights connected to the mobile network; and augmented and virtual reality (AV/RV) applications for the port's engineering team to help the day-to-day maintenance of the port.

The 5G-VINNI facility and experimentation sites in Norway, Germany, the UK and other EU member states are also relevant for the use cases included in this Research Report. For example, a moving experimentation facility site is enabled by the satellite connected rapid response vehicle, which provides satellite backhaul capabilities.[100]

4.2.1. 5G SECURITY TEST BED OF ESTONIA'S CYBER RANGE CR14

Estonia's Cyber Range CR14 is set to deploy private 5G SA test bed infrastructure based on Nokia hardware and software solutions in Tallinn, Estonia, in the third quarter of 2021. The project is entitled 'Cyber Defence Simulation of Internet of Things and Mobile Networks in the Cyber Range', and it is being carried out in cooperation with universities, MNOs, and other partners.[101] The aim of the test bed is to provide a research capability for network security in 5G military use cases. Initially, the 5G SA test bed will include a 3GPP Release 15-compatible private 5G core network and three gNodeBs (indoor and outdoor) operating on 3GPP band N5 (869–894 MHz), with a future 3GPP Release 16 upgrade option by the provider. The 5G private network will be connected to the CR14 Cyber Range, which can be deployed at remote sites. The 5G private network can provide data network services to locally managed subscribers.

94 The 5G Infrastructure Public Private Partnership (5G PPP) is a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications operators, service providers, SMEs, and researcher Institutions). https://5g-ppp.eu/ [accessed 23 July 2021].

95 'This Page Lists 5G Trials That Have Been Publicly Announced in EU27, UK, Norway, Russia, Switzerland and Turkey', European 5G Observatory, https://5gobservatory.eu/5g-trial/major-european-5g-trials-and-pilots/ [accessed 20 June 2021].

96 Pujol et al., '5G Observatory Quarterly Report 11 Up to March 2021'.

97 Pujol et al., '5G Observatory Quarterly Report 11 Up to March 2021'.

98 'Connecting Europe Facility (CEF2) Digital', European Comission, 21 March 2021, https://ec.europa.eu/digital-single-market/en/connecting-europe-facility-cef2-digital.

99 'Smart Sea Port Use Case', https://5g-monarch.eu/smart-sea-port-use-case/ [accessed 23 July 2021].

100 'Moving Experimentation Facility Site (Satellite Connected Vehicle)', 5G-Vinni, https://www.5g-vinni.eu/moving-experimentation-facility-site/ [accessed 21 June 2021].

101 'Cyber Defence Simulation of Internet of Things and Mobile Networks in the Cyber Range' is an ongoing research project led by a consortium of institutions and companies including NATO CCDCOE, University of Tartu, Thinnect OÜ, Elisa Eesti AS, CybExer Technologies OÜ. See more at https://cybersecurity.cs.ut.ee/Research/CIISIM.

5. Supply Chain and Network Security

The North Atlantic Council (NAC) recently expressed that 'cyber threats to the security of the Alliance are complex, destructive, coercive, and becoming ever more frequent.'[102] The council affirmed determination 'to employ the full range of capabilities, as applicable, at all times to actively deter, defend against, and counter the full spectrum of cyber threats, in accordance with international law.'[103] Telecommunications, including 5G networks, are also susceptible to cyber threats. This section outlines the supply chain and network security risks related to 5G technology and systems.

The armed forces of NATO nations and NATO command structure need to take into account vulnerabilities, threats and risks related to both public and private 5G networks. Three 5G network deployment models for military use identified in this report come with their own security challenges, which should be understood and assessed.[104] While the Research Report focuses on military use cases, it cannot disregard the vulnerabilities, threats and risks associated with commercial 5G networks, because in practice, the military will largely use networks and equipment available commercially. Almost all telecommunication technologies are for dual (i.e. military and civilian) use, and inevitably, there will be interdependencies (and hence, vulnerabilities) across the whole life cycle involving many stakeholders (including third-party suppliers and service providers, such as private companies that own and operate mobile cell towers). Therefore, visibility into the supply chain ecosystem is essential for the military.

The security of 5G networks is a very broad and complex topic, and research on it continues to evolve. Many white papers, research reports, overviews and other studies have been published in this area in the last decade. Several distinct threat taxonomies and categorisations of non-technical and technical 5G security risks have been developed by international and governmental organisations, equipment vendors and technical security researchers. A choice of a specific methodology to assess risks depends on a particular target audience – for example, reports addressed to telecommunication sector experts offer a very detailed description of technical security risks associated to infrastructure, components and interfaces of 5G architecture. In addition, the academic and think-tank literature includes a large body of writings offering overviews for policy-makers and regulators who lack technical knowledge of telecommunications.

In addition to supply chain challenges (including the trustworthiness criteria of vendors) and network security challenges, physical security and electromagnetic inference threats to military use cases must be considered, along with traditional insider threats.[105] In case of the deployment of the military 5G network on an expeditionary operation in an armed conflict, electromagnetic interference attacks are likely to impede network connectivity and system capacity. However, those attacks have also been launched in peacetime. 5G networks used for expeditionary operations in high-intensity kinetic conflict must meet the most stringent military security requirements in the areas of resistance to jamming, network resilience, and security.

The armed forces must assume that 5G network infrastructure is vulnerable to cyberattacks from both encryption and resiliency standpoints. The military must be able to operate over untrusted networks or networks, including some untrusted components or insecure interfaces.[106] This could mean that the military cannot transfer and store classified data in some 5G networks, even though pilot projects for classified information exist. Needless to say, the fact that a given equipment manufacturer, MNO, or third-party service provider is geographically located in the jurisdiction of an EU or NATO nation does not guarantee that infrastructure, equipment, or services provided by these stakeholders are secure. Even trusted networks with recognised security maturity can be accessed physically, by malicious insiders (such as MNO employees), and through electromagnetic and cyberattack means. In such cases, the NATO nations' armed forces need to consider what types of information and military functions can be transmitted and stored in public and hybrid 5G networks.

102 'Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise', 19 July 2021, NATO, https://www.nato.int/cps/en/natohq/news_185863.htm.

103 'Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise'.

104 The three models are the private 5G network deployment model (not connected to public or other private networks and the Internet); the hybrid 5G network deployment model, where the private 5G network components (such as antennas, sensors, and base stations) are connected to some components of a public 5G network (such as RAN or core network); and the public 5G network deployment model, where military uses public 5G networks which have a dedicated (i.e. isolated) slice.

105 Due to its limited scope, this Research Report does not address insider threats, physical security, or electromagnetic spectrum threats.

106 Milo Medin and Gilman Louie, 'The 5G Ecosystem: Risks and Opportunities for DoD', Defense Innovation Board, 3 April 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

5.1. Supply Chain Security and Risk Management

As discussed in the introduction, the supply chain has become a common attack vector for nation states' cyber espionage and the theft of government and defence sector data.[107] Recent large-scale, high-impact supply chain cyberattacks, for example, NotPetya in 2017 and SolarWinds (also known as Solarigate/Sunburst backdoor malware attacks) in 2020, have disrupted public services in many countries, causing huge economic losses. Moreover, cyberattacks have damaged and disabled critical infrastructure and ICT systems. Supply chain attacks can be difficult to trace and manage. Yet they can cause serious second-order effects such as the sabotage or physical destruction of critical infrastructure, or the theft or manipulation of sensitive or classified information.[108] This trend will continue in the current decade, and the repercussions for NATO nations' economic and national security are likely to be severe.

The use of open source software, poor coding practices, insufficient patching, and cyber hygiene; the reliance on commercial-off-the-shelf (COTS) products, systems, and services; and the complexity of global supply chain bring new threats to the military use of 5G technology. The global and distributed nature of product and service supply chains make it difficult to determine how the acquired technology has been developed and deployed. In addition, supply chain risks can also include so-called insider threats.[109]

Broadly speaking, supply chain security risks concern the reliability, availability, safety, and redundancy of networks, as well as the market diversity of 5G equipment and associated services. Supply chain risks to market diversity constitute a situation where MNOs have limited choice of equipment vendors. This can happen when a single vendor, whose proprietary hardware and software is not interoperable with other vendors' products, dominates a global market. In this example, a lack of vendor choice can lock a MNO into using equipment from an untrusted vendor, which creates new security risks related to the supply chain. Further examples of cyber supply chain risks include: insertion of counterfeits; unauthorised production; malicious insiders; tampering; theft; insertion of malicious software and hardware (GPS tracking devices, computer chips, etc.); and poor manufacturing and development practices in the cyber supply chain. These risks are realised when threats in the cyber supply chain exploit existing vulnerabilities.[110]

Supply chain attack vectors can be utilised at any point during the ICT life cycle, from design to maintenance and retirement. Implants (or other vulnerabilities inserted prior to the installation of equipment) can be used to infiltrate government and defence sector data or manipulate hardware and software, computer operating systems, or end user devices and associated services for economic, political, and military purposes.[111] For example, the Solarigate/Sunburst supply chain attack, which has been attributed to the Russian government, targeted the software development process; this popular attack vector has frequently been used by Russia, China and other authoritarian countries.[112] Software supply chain attacks can also target telecommunications technology, including 5G networks – for example, VNF and software defined networking (SDN) introduce vulnerabilities to the core network, which may be exploited by malicious actors.

The US DoD 5G Strategy prescribes addressing strategic risks and adopting mitigation measures to minimise risks to the supply chain. The strategy prescribes avoidance of the use of 5G technology vendors who are considered untrusted or who have unreliable products.[113] Likewise, the Prague Proposals on 5G security (2019) and the Centre for Strategic and International Studies (CSIS) 'Criteria for Security and Trust in Telecommunications Networks and Services' (2020) provide further non-technical criteria for national decision-makers to assess risks to determine the trustworthiness of a potential supplier and manufacturers.[114] For example, the CSIS criteria include the following aspects: political and governance, business practice assessment, and cybersecurity risk mitigation

107 The term 'supply chain' refers to the linked set of resources and processes between and among multiple levels of enterprises, each of which is an acquirer that begins with the sourcing of products and services and extends through their life cycle. 'Cyber Supply Chain Risk Management Practices for Systems and Organizations. Draft NIST Special Publication 800–161, 2 Revision 1', NIST, https://doi.org/10.6028/NIST.SP.800-161r1-draft [accessed 22 July 2021], p. 1.

108 'Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy', NIST Special Publication 800–37, revision 2, December 2018, https://csrc.nist.gov/Projects/risk-management/publications.

109 'Insider threats' refer to the vulnerability of the supplier to attack from trusted staff and partners that are embedded internal to the supplier operations, for example, intentional tampering or interference. See 'Appendix I: Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force (TF) Threat Evaluation Working Group: Threat Scenarios', CISA, February 2020, https://www.ntia.gov/files/ntia/publications/5g_ip_appendices_1-5.pdf.

110 'Cyber Supply Chain Risk Management Practices for Systems and Organizations. Draft NIST Special Publication 800–161, 2 Revision 1', p. 7.

111 A supply chain is a system of organizations, people, activities, information, and resources that provides products or services to consumers. 'CMCC Glossary and Acronyms'.

112 See a comprehensive overview of nation-state supply chain attacks in Trey Herr, William Loomis, Stewart Scott and June Lee, 'Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain', Atlantic Council, 26 July 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/#attacks.

113 'Department of Defense 5G Strategy', Department of Defense, 2 May 2020.

114 The Prague Proposals are enshrined in bilateral MOUs and joint declarations on 5G security between the US and NATO nations. See 'The Prague Proposals: The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World', Prague 5G Security Conference, 3 May 2019, https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf. 'Criteria for Security and Trust in Telecommunications Networks and Services', CSIS Working Group on Trust and Security in 5G Networks, 13 May 2020, https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services.

criteria, and government actions to increase confidence in choosing a supplier.[115] The EU assessment and Prague Proposals address many of the same concerns.

In regard to the supply chain risk, the main concerns of the US Cybersecurity and Infrastructure Security Agency (CISA) are counterfeit components (which are more susceptible to cyber-attacks and more likely to fail because of their poor quality) and compromised components. A component may be compromised through interference with the source code repository, the theft of signing keys, or the penetration of distribution sites and channels. The CISA notes that third-party suppliers, vendors, and service providers may have weaker security controls and audits than MNOs, which makes compromised components in their supply chain more likely. For example, a MNO may buy the core network system's management software from a trusted provider; however, it may happen that, unbeknownst to this trusted provider, one of the components it uses in the product is compromised and contains malicious code.[116] In an earlier advisory from 2019, the CISA divides 5G security risks into four categories: supply chain, competition and choice, network security, and deployment. According to this simplified approach, supply chain risks include malicious hardware and software and vulnerabilities in the manufacturing of products and their maintenance. The advisory proposes mitigation measures such as adequate standardisation and certification schemes, auditing, and vetting and procurement policies.[117]

According to a recent survey, large MNOs in the European Union have moved parts of their operations outside the EU countries because of more favourable legislative or business environments. This exacerbates the difficulty of ensuring the reliability, integrity, safety, and security of the supply chain and introduces new vulnerabilities on the top of the existing ones mentioned in this sub-chapter, which can be leveraged by non-EU and non-NATO countries for malicious use.[118] In sum, supply chain risk management is a very complex and multifaceted undertaking, requiring building trust relationships and communicating with both internal and external stakeholders.[119]

It is essential that NATO nations' governments and militaries have sufficient transparency into the processes, procedures, and practices used by manufacturers of 5G technology and providers of associated services in order to assure the integrity, security, resilience, and privacy, as well as quality, of the acquired products, systems, and services throughout their whole life cycle.[120] Hence, militaries must work closely with commercial 5G network providers to jointly assess supply chain and network security risks and add suitable security assurances for military-grade 5G networks. At the time of publication of this Research Report, the Alliance has not begun broad discussions with vendors, MNOs, or other stakeholders on how to achieve comprehensive visibility into the supply chain of 5G networks.

5.2. Taxonomies of Network Security Risks Related to 5G Networks

At a very broad level, network security challenges to 5G networks can be split into technical and non-technical (largely strategic and regulative) risks. However, as mentioned previously, some types of threats and risks are related to both supply chain and network security. Examples of non-technical risks include political and strategic questions of trustworthiness of 5G technology hardware and software manufacturers and vendors, MNOs, and associated service providers (such as cloud providers). The EU coordinated risk assessment report addresses risks in three categories (strategic, technical, and supportive), and the Toolbox includes mitigation measures in all three areas.[121] However, progress in implementing risk management measures is uneven across the EU – as of July 2020, only 14 member states have included (or plan to include) non-technical criteria into national regulations to assess high-risk vendors.[122]

Figure 3 presents key threats to 5G technology. For the military, the priority threats are those targeting the availability and reliability of the networks, including electromagnetic interference attacks.

115 'Criteria for Security and Trust in Telecommunications Networks and Services'.

116 'Potential Threat Vectors to 5G Infrastructure', CISA, May 2020, https://www.cisa.gov/publication/5g-potential-threat-vectors.

117 'Overview of Risks Introduced by 5G Adoption in the United States', CISA, 31 July 2019, https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.

118 'Assessment of EU Telecom Security Legislation', ENISA, 13 July 2021, https://www.enisa.europa.eu/publications/assessment-of-eu-telecom-security-legislation.

119 NIST Special Publication 800–37, revision 2.

120 NIST Special Publication 800–37, revision 2. System development life cycle includes research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, disposal, and overall management of an organization's products and services. 'Cyber Supply Chain Risk Management Practices for Systems and Organizations: Draft NIST Special Publication 800–161, 2 Revision 1', NIST, https://doi.org/10.6028/NIST.SP.800–161r1-draft [accessed 22 July 2021], p. 4.

121 'The EU Toolbox for 5G Security', European Commission, 8 March 2021, https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

122 NIS Cooperation Group, 'Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity', European Commission, July 2020, https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

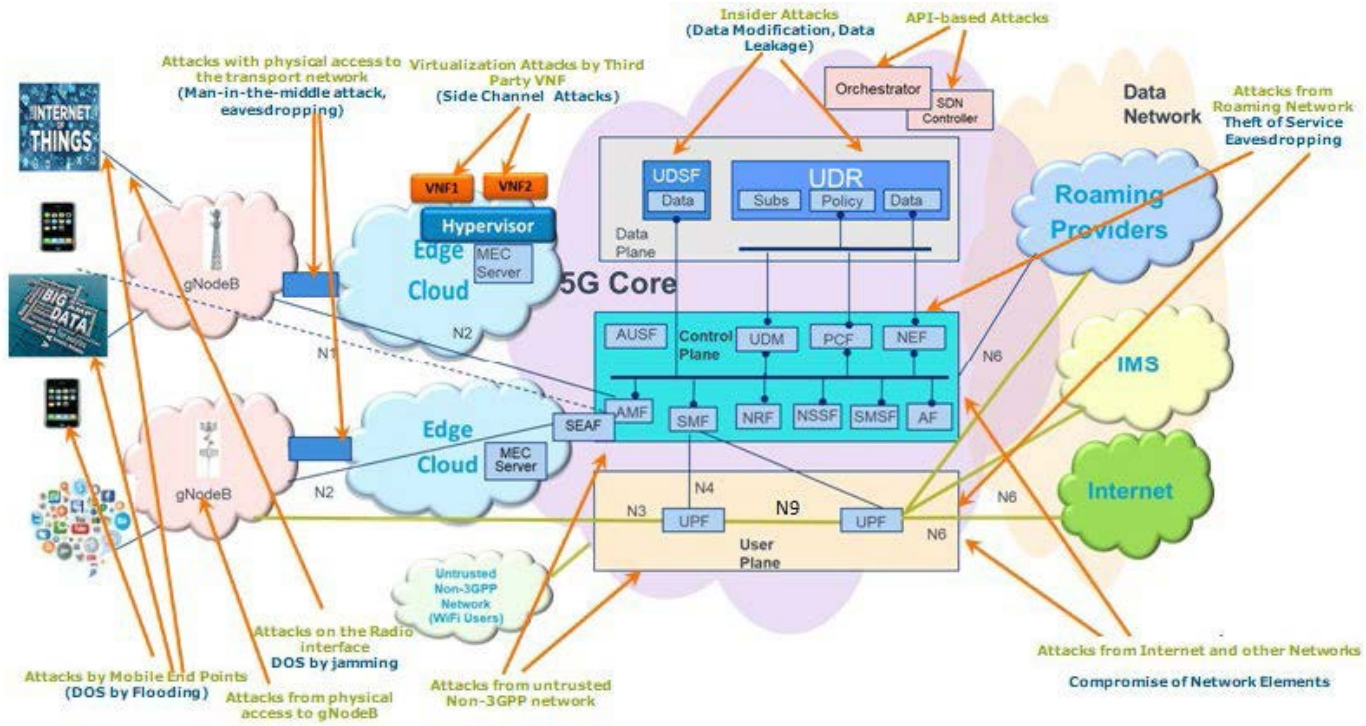

Figure 3. 5G Threat model[123]

5.2.1. ENISA'S THREAT TAXONOMY

The ENISA Threat Landscape for 5G Networks categorises 5G threats into nine categories of both a non-technical nature (such as legal actions, physical attacks, and natural and environmental disasters) and a technical nature (such as service outages, technical failures and malfunctions, intentional and unintentional damages, eavesdropping, interception and hijacking, and nefarious activities).[124] This comprehensive and detailed threat taxonomy also includes supply chain threats of an intentional and technical nature (these are included in a category of 'nefarious activities' which may emerge from a third-party personnel accessing MNO facilities, and intentional exploitation of hardware and software vulnerabilities). Other supply chain security challenges in ENISA's assessment are of a non-intentional nature – for example, counterfeit or poor-quality products, which can compromise the confidentiality, integrity, and availability of network assets.[125]

5.2.2. CISA'S THREAT TAXONOMY

An in-depth cybersecurity supply chain threat taxonomy is presented in the CISA Supply Chain Risk Management Task Force publication 'Threat Scenarios' (2020), which includes the following 10 threat categories: counterfeit parts, cybersecurity, internal security operations and controls, system development life cycle processes and tools, insider threats, economic risks, threats in an extended supplier chain, legal risks, national disasters, and geopolitical issues.[126]

In May 2021 CISA released a report, 'Potential Threat Vectors to 5G Infrastructure', which identifies three main threat vectors to 5G infrastructure: policy and standards, supply chain, and 5G systems architecture.[127] 5G standards development can be leveraged by adversary countries as a threat vector. The report notes that adversarial countries can influence the standardisation, which may reduce market competition and limit the use of trusted vendors' equipment or push them out of the market, as discussed in the introduction of this Research Report. Moreover, untrusted technologies may be interoperable with trusted vendors' equipment, which also limits the use of the latter in cases when the former have market dominance (as is the case for Huawei at the moment). Another threat vector related to 5G standards is the voluntary nature of security by design – in some cases, security protocols prescribed by 5G standards are optional, and hence MNOs may not implement them, which also increases network security risks.[128]

5.2.3. VENDORS' THREAT TAXONOMY

On the industry side, Ericsson enlists the following 5G attack vectors: devices, air interfaces, RAN and base stations, the

123 'International Network Generations Roadmap. 2021 Edition. Security and Privacy', IEEE (Institute of Electrical and Electronics Engineers, Incorporated) [accessed 20 June 2021].

124 'ENISA Threat Landscape for 5G Networks Report', European Union Agency for Cybersecurity, 14 December 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/.

125 'ENISA Threat Landscape for 5G Networks Report'.

126 'Appendix I. Information And Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force (TF) Threat Evaluation Working Group: Threat Scenarios'.

127 'Potential Threat Vectors to 5G Infrastructure', CISA.

128 'Potential Threat Vectors to 5G Infrastructure', CISA.

core network, and the cloud. Ericsson provides four broad categories of key security challenges of 5G technology: operations process, deployment, development process of a vendor's products, and the standardisation process.[129] Cisco provides the following list of network security risks against components of the 5G ecosystem:

1) end-user devices (malware, bots DDoS, device tampering, etc.);
2) air interface (MITM attack and jamming);
3) RAN;
4) MEC and backhaul;
5) 5G packet core and operations, administration, and maintenance;
6) SGi/N6 and external roaming threats.[130]

In addition, possible 5G threat scenarios, according to Cisco, are loss of availability, loss of confidentiality, loss of integrity, loss of control, malicious insiders, and theft of service.[131]

5.2.4. US DEPARTMENT OF DEFENSE'S THREAT TAXONOMY

The US DoD categorises network security threats as follows:

→ risks related to signalling (SS7, Diameter, and HTTP), which are largely associated with the confidentiality of SMS and GPS coordinates, roaming fraud, and interception of voice[132]
→ vulnerabilities to the core network related to network virtualisation and slicing
→ a larger attack surface due to poorly protected IoT and large quantity of potentially exposed small cells
→ edge computing-related risks
→ supply chain risks
→ risks related to Application Programming Interfaces (API)
→ vulnerabilities related to local network configuration.[133]

5.3. Risk Management Frameworks, Policies, Guidelines

Fortunately, NATO nations are developing regulations, guidelines, frameworks, and tools to improve software security and supply chain security. Supply chain risk management is a systematic process that identifies susceptibilities, vulnerabilities, and threats throughout the supply chain and develops mitigation strategies to combat those threats, whether presented by the supplier, the supplied product, and its subcomponents or the supply chain.[134] However, in many cases it may not be possible to distinguish the supply chain from network security threats, as threats can fall simultaneously into both categories. Typically, the government's network security risk assessment and management guidelines would include supply chain security as a sub-category. The implementation of supply chain risk management concepts is expected to mitigate the following risks: untrustworthy suppliers, insertion of counterfeits, tampering, unauthorised production, theft, insertion of malicious code, and poor manufacturing and development practices. These risks can be mitigated by a number of measures, such as procurement policies, conducting risk assessments and collecting supply chain threat intelligence, identifying and implementing risk-based mitigations, and performing monitoring functions.[135]

In addition to focusing on supply chain security, NATO nations have already incorporated strategic-political criteria of trustworthiness into national legislation. For example, the president's Executive Order 13873 prohibits the US DoD from acquiring, importing, transferring, installing, dealing in, or using 5G technologies produced by foreign adversaries, including Chinese companies.[136]

In addition to developing specific criteria for selecting trusted vendors and suppliers, many NATO countries use supply chain risk management frameworks and guidelines for the acquisition and procurement of state- and government-owned and -operated ICT technology and services. Cyber supply chain risk management is a new concept that covers the entire life cycle of ICT. It is defined as 'the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of ICT product and service supply chains'.[137]

In the US, the National Institute of Standards and Technology (NIST) established a forum and a dedicated website for Cyber Supply Chain Risk Management for

129 'A Guide to 5G Network Security: Conceptualizing Security in Mobile Communication Networks – How Does 5G Fit In?' Ericsson, https://www.ericsson.com/en/security/a-guide-to-5g-network-security [accessed 20 June 2021].
130 Pramod Nair, 'Why 5G Is Changing Our Approach to Security', 10 June 2020, Cisco blog, https://blogs.cisco.com/sp/5g_secure.
131 Nair, 'Why 5G Is Changing Our Approach to Security'.
132 Signaling System Number 7 (SS7) is a telecommunications signalling architecture traditionally used for the setup and tear-down of telephone calls. Diameter is an authentication, authorisation, and accounting protocol used by computer networks. Hypertext transfer protocol (HTTP) is a fundamental protocol used on the Internet in order to control data transfer to and from a hosting server, in communication with a web browser. See 'Technology Dictionary', Techopedia, https://www.techopedia.com/dictionary [accessed 20 June 2021].
133 'Department of Defense 5G Strategy Implementation Plan', Department of Defense, 15 December 2020, p. 10, https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf [accessed 20 June 2021].
134 The supply chain consists of production, packaging, handling, storage, transport, mission operation, and disposal. See 'CMCC Glossary and Acronyms'.
135 NIST Special Publication 800–37, revision 2.
136 Executive Order 13873, 'Securing the Information and Communications Technology and Services Supply Chain', 15 May 2019, *Federal Register*, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.
137 'National Strategy to Secure 5G Implementation Plan Appendices', NTIA, https://www.ntia.gov/files/ntia/publications/5g_ip_appendices_1-5.pdf.

federal agencies, as well as publishing several guidelines.[138] Pursuant to Executive Order 140208, the NIST published guidance outlining security measures for critical software and guidance recommending minimum standards for vendors' testing of their software source code. In 2022 the NIST will publish further guidance identifying practices that enhance software supply chain security, including standards, procedures, and criteria.[139]

Concerning the national defence sector, an important activity of the US DoD 5G strategy is the identification and assessment of vulnerabilities, threats and risks to 5G technology and infrastructure.[140] The DoD is in charge of developing 5G supply chain risk management strategies, guidelines and procedures, including developing an industry standard for 5G supply chain assurance.[141] Another example of a cybersecurity risk management scheme that includes managing supply chain risks is the DoD's Cybersecurity Maturity Model Certification (CMMC) for the defence industrial base. In addition to these efforts, in February 2021 US president Joe Biden ordered a review of supply chain risks for the defence industrial base and for critical sectors and subsectors of the ICT industrial base, including for the development of ICT software, data, and associated services.[142]

As this Research Report demonstrates, NATO nations must build visibility into supply chain vulnerabilities, risks, and threats. This would enable improved evidence-based risk-informed decision-making by national governments regarding 5G technologies and infrastructure. NATO nations must improve sharing information and threat assessments about vulnerabilities, threats and risks associated with high risk or untrusted 5G vendors, technology and infrastructure. At the time of this Research Report's publication, there are no regular processes or methodologies for 5G threat sharing.

5.4. Network Security

For the purposes of this Research Report, 'network security' can be understood as the confidentiality, integrity, and availability of data, systems, and networks. All components of 5G security architecture must be evaluated from a network security point of view, and security by design must be considered from the beginning of the product and services life cycle. Despite a larger attack surface and the increased complexity of the 5G architecture, 5G is generally considered more secure than the previous generations of telecommunications (2G, 3G, 4G LTE). However, advances throughout 5G network architecture simultaneously expand the threat surface, and threats from legacy technology remain.[143] The currently still-evolving 5G architecture entails a variety of security challenges and 3GPP standards do not address all of them. For example, new risks are associated with the following characteristics of 5G networks: distributed core network, edge computing, network slicing, virtualisation and IoT. In addition to these, cyberattacks can be launched through encrypted channels.[144]

Those in the field and in international organisations have published a large body of literature detailing the wide range of 5G vulnerabilities, threats, and risks. According to the CISA, in the area of 5G systems' architecture (broadly corresponding to network security), there are multiple threat vectors related to software configuration, network security, network slicing, legacy infrastructure, MEC, spectrum sharing, and SDN.[145]

Another example of network security threat assessment mentioned earlier is the 'ENISA Threat Landscape for 5G Networks'.[146] According to ENISA, network security threats target the following dimensions of 5G architecture: wireless communication, IoT and end user devices, and 5G infrastructure components (servers, base stations, cells, etc.). Threats to wireless communication fall into four categories: eavesdropping and traffic analysis, jamming, DoS/DDoS and the man in the middle attack (MITM). The major threats against 5G infrastructure (e.g. servers and cloud-based servers) are virtualisation, network slice security, improper access control, data replication, roaming partner vulnerabilities, and DoS/DDoS attacks.[147]

As mentioned, virtualisation and network slicing concepts introduce new opportunities for network security risk detection and mitigation but also new risks that the current 5G standards do not address. Three major attack vectors

138 Examples of NIST guidance include 'Supply Chain Risk Management Practices for Federal Information Systems and Organizations, SP 800–161', and a draft 'Cyber Supply Chain Risk Management Practices for Systems and Organizations, SP 800–161 Rev. 1'. See: 'Cyber Supply Chain Risk Management C-SCRM, Publications', NIST, https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications [accessed 15 July 2021].

139 'Executive Order 14028, Improving the Nation's Cybersecurity', Fact Sheet, NIST, https://www.nist.gov/system/files/documents/2021/07/13/EO%20Fact%20Sheet%20July%202021.pdf [accessed 25 July 2021].

140 'Appendix I: Information And Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force (TF) Threat Evaluation Working Group; Threat Scenarios'. https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf.

141 'Department of Defense 5G Strategy Implementation Plan', p. 8.

142 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

143 Nair, 'Why 5G Is Changing Our Approach to Security'.

144 Nair, 'Why 5G Is Changing Our Approach to Security'.

145 'Potential Threat Vectors to 5G Infrastructure', CISA.

146 'ENISA Threat Landscape for 5G Networks Report,' European Union Agency for Cybersecurity, 14 December 2020, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

147 Anshu Bhardwaj, '5G for Military Communications', Third International Conference on Computing and Network Communications (CoCoNet'19), *Procedia Computer Science* 171, 2020, pp. 2665–2674, Elsevier B.V., https://doi.org/10.1016/j.procs.2020.04.289 [accessed 20 June 2021].

that have not been addressed are user data extraction (i.e. location tracking); DoS against another network function; and access to a network function and related information of another vertical.[148] When new security risks related to evolving 5G standards are discovered, standards will be improved and enhanced security measures will be suggested to reduce the discovered new threats. For example, a hacker compromising an edge network function connected to the MNOs' service-based architecture could exploit a flaw in the design of network slicing standards to have access to both the operator's core network and the network slices for other enterprises. This could allow user location tracking, the loss of charging related information, and even the potential interruption of the operation of the slices and network functions themselves.[149] This flaw in 5G standards creates an opportunity to access data across multiple slices if the attacker has access to the 5G service-based architecture, including to a mobile phone location or IMSI. The measures to protect against these threats include network traffic filtering and validation of users.[150] Threats against end-user devices – such as targeting user data and privacy such as IMSI catching- and signalling-based attacks – should also be considered. Attacks against end user equipment include application threats associated with the use of malware to either disrupt or extract sensitive user information such as MITM, DDoS, device tampering, and sensor susceptibility.[151]

Zero Trust Security is the principle that software and equipment are not to be trusted and that some parts of a network might be compromised, allowing the exfiltration of data, failure to transmit data, or the jamming of parts of the radio spectrum, among other threat vectors.[152] Zero Trust Security is also an approach that is expected to foster the confidentiality, integrity, and availability of data and systems for NATO forces who will operate through untrusted 5G networks at expeditionary operations. Alongside network security risks, electronic jamming and physical risks to 5G network infrastructure must be included in comprehensive risk analysis and mitigation. Methods to protect against electronic jamming (i.e. availability) might include, for example, anti-jamming techniques and dynamic spectrum utilisation. The confidentiality of data and systems can be improved by end-to-end encryption and obfuscation techniques.

Cloud providers, cyber security companies, and other 5G equipment and service providers offer a large variety of products and services to secure cloud native virtualised 5G core network deployments. These tools include: secure access based on Zero Trust principles, secure API and non-API communications, end-to-end monitoring for multi-vendor 5G networks, and end-to-end threats mitigation. Furthermore, specific solutions exist on the market for virtualised open RAN, which allow for vendor diversity and modularity. Open RAN offers the benefits of vendor diversity and better interoperability between equipment from different vendors. By using open RAN, a lack of transparency and the security risks associated with depending on a single vendor could, to a large extent, be avoided, thereby decreasing the overall security risks.[153]

5G Americas has published several white papers describing, at the technical level, 5G threats across nine areas of 5G wireless technology: 4G threats, IoT, massive IoT, user equipment, RAN (including rogue base station), subscriber privacy, core network, NFV and SDN, and interworking and roaming.[154] There are two main approaches to secure 5G architecture. These are network slicing and threat mitigation for IoT and DDoS.[155] 5G Americas points out that the implementation of 5G technology elements requires additional encryption, extra defence in edge networks, and sophisticated new protocols to handle the demands of network slicing, MEC, and a disaggregated RAN. The 5G Americas' reports also delve into various techniques that would mitigate threats, including Zero Trust principles.[156]

Due to the need to harden 5G networks and infrastructure for military use, future research (including technical testing) should address the ways and means to do so. Because militaries use specialised communication services requiring high levels of security, reliability, and availability, the military use of 5G technology requires military-grade

148 Network slicing allows MNOs to divide the core and the radio network into multiple distinct virtual blocks that provide different amounts of resources and prioritisation to different types of traffic; vertical customers can be isolated. A recent report identifies within the slicing model how information might potentially be exposed, how services could be misused, and how DoS attacks could be executed against network elements. See 'A Slice in Time: Slicing Security in 5G Networks', White Paper, Adaptive Mobile Security, 24 March 2021, https://www.adaptivemobile.com/newsroom/press-release/adaptivemobile-security-details-major-security-flaw-in-5g-core-network-slicing-design.

149 'AdaptiveMobile Security Details Major Security Flaw in 5G Core Network Slicing Design', 24 March 2021, https://www.adaptivemobile.com/newsroom/press-release/adaptivemobile-security-details-major-security-flaw-in-5g-core-network-slicing-design.

150 Máirín OSullivan, '5G Network Slicing Vulnerability: Location Tracking Attacks', 27 April 2021, https://www.adaptivemobile.com/blog/5g-network-slicing-vulnerability-location-tracking-attacks.

151 OSullivan, '5G Network Slicing Vulnerability: Location Tracking Attacks'.

152 'Department of Defense 5G Strategy Implementation Plan', p. 10. Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy. It includes security monitoring, controls, and system security automation, focusing on protecting critical assets in real-time within a dynamic threat environment. 'Special Publication 800–207: Zero Trust Architecture', National Institute of Standards and Technology, https://csrc.nist.gov/publications/detail/sp/800-207/final.

153 Open RAN should be distinguished from open source software. Open RAN is a wireless network architecture that uses open, defined, standards-based, interoperable elements that can be decomposed into modular 'swappable' components from multiple vendors, which can include proprietary or open source technologies. Eric Wenger, 'Are Openness and Security Both Possible in a 5G World?' https://blogs.cisco.com/gov/are-openness-and-security-both-possible-in-a-5g-world.

154 'The Evolution of Security in 5G', 5G Americas, July 2019, https://www.5gamericas.org/the-evolution-of-security-in-5g-2/.

155 'The Evolution of Security in 5G'.

156 'Security Considerations for the 5G Era', 5G Americas, July 2020, https://www.5gamericas.org/security-considerations-for-the-5g-era/.

security controls (on top of the commercial levels of supply chain and network security), such as robustness against jamming and end-to-end encryption of data.

As mentioned, several NATO nations have general cyber supply chain security risk management frameworks in place, but these omit (voluntary) standards and best practices for manufacturers and operators of telecommunications equipment. Furthermore, because countries apply different criteria concerning identifying and limiting high-risk or untrusted vendors NATO should attempt to harmonise diverse and uneven national 5G security policies across Allies.

The Alliance already includes telecommunications' trustworthiness criteria in technical procurement, security policies and regulations.[157] NATO should set criteria to assess a trustworthiness level of a specific 5G vendor. An implementation plan to manage risks related to 5G technology, services, and infrastructure should also be developed jointly by NATO nations. As a rule, critical military communications (including classified information-sharing networks) should be connected only to trusted 5G technology and service providers. The Zero Trust Security approach should be applied to 5G networks, keeping in mind that trusted technology can also become compromised.

5.5. Threats Specific to Military 5G Networks

In 2019, NATO's NCI Agency began an analysis to identify opportunities for the military to employ 5G technology. As part of this work, several reference scenarios have been developed: deployed CIS for expeditionary operations, tactical operations, maritime operations, and static communications. These scenarios use either public or private 5G networks. The agency also identified security challenges pertaining to developing the use cases. In addition, NATO launched a multinational 5G programme, MN5G, in order to develop scenarios and identify both opportunities and challenges associated with the use of 5G technology for the military.[158] In the future, this work will include an analysis of the security of public 5G networks and infrastructure.[159] However, there is currently no comprehensive overview of 5G technology security challenges for NATO nations' militaries.

The European Defence Agency (EDA) conducted an analysis of security aspects of 5G technology for the defence sector and published the '5G Defence White Paper', which advises militaries to restrict the use of commercial 5G equipment to only those use cases which do not require higher levels of security. It recommends that the armed forces harden commercial 5G networks and customise COTS 5G equipment in order to improve their security for military use. The EDA White Paper recommends configuring 5G technology in order to increase security by approaches such as hidden network slicing. The EDA advisory notes that in addition to end-to-end encryption of data and information in transit and that stored through commercial 5G networks, network slicing provides isolation of services for a military slice without influence from other slices and infrastructure providers such as MNOs. It points out that public 5G technologies can be adopted to build a proprietary military 5G network, but the latter requires add-ons and adaptations, including resilience to power outages and measures to avoiding single points of failure.[160] The paper, however, gives only a high-level overview of possible security challenges and mitigation measures for the military.

In addition to the supply chain and network security challenges discussed earlier, the availability of 5G networks is critical for the military. This depends on complex interdependencies from critical infrastructure that affect 5G networks. For example, the ICT sector, as well as various vertical business cases enabled by 5G networks, depends on the supply of power (i.e. electricity), while power grids themselves depend on the resilience and continuous functioning of ICT services and on operational technology (i.e. industrial control systems such as SCADA of energy grids).[161] The difficulty of mitigating these interdependent threats emerges from poor understanding of those complex interconnectivities and dependencies.

Another security challenge which the military must analyse stems from linking public and private 5G networks. The concept of network slicing offers a degree of resource isolation and allows the deployment of dedicated and customised services. It can be a solution for business and office traffic, but it is not resilient enough to network disruptions and may not fulfil the security and isolation requirements of military deployments and operations.[162] For example, the FUDGE 5G pilot project provides the separation of a military network slice from public network slices. In the concept of network slicing, network security can be provided by the following methods: removal of attack vectors, shielding of metadata, disabling legacy

157 'Keynote Address by NATO Deputy Secretary General Mircea Geoană at the NCI Agency's NITEC Connect 2021 Conference',.

158 Luis Bastos, '5G Technologies for Military Applications', *NITECH: NATO Innovation and Technology*, no. 5, June 2021, https://issuu.com/globalmediapartners/docs/nitech_issue_05_jun_2021.

159 'Multinational Collaboration of 5G', NCI Agency, http://www.mindev.gov.gr/wp-content/uploads/2020/11/Enclosure-3-Leaflet-Multinational-Collaboration-on-5G.pdf [accessed 8 July 2021].

160 '5G Technologies for Defence', White Paper, European Defence Agency, January 2021.

161 For discussion on threats to critical infrastructure connected to the '5G ecosystem', see 'International Network Generations Roadmap: 2021 Edition. Security and Privacy'.

162 '5G Technologies for Defence'.

technology, autonomy, and coverage 'on demand'.[163] To ensure the security of critical government and military information, classified information (and information relevant to national security) should, by default, be isolated from the internet without external SS7 links and international roaming partnerships.[164]

It should be noted that open source software also has well-known vulnerabilities. There are specific vulnerabilities inherent to Open RAN architecture that might require additional security features that have not yet been addressed.[165] Open architectures enable greater functionality and enhance security by bringing interoperable components from a wide variety of suppliers, but this also increases complexity and decreases control over network components.[166] The introduction of additional interfaces and nodes and the decoupling of hardware and software furthermore expands the threat and attack surface. Hence, on the one hand, Open RAN architecture increases security by adding auditable security through modularity and open interfaces, but on the other hand, open interfaces increase security risks.[167] Moreover, O-RAN Alliance, which develops standardised architecture and technical specifications, includes almost 50 Chinese companies, including ZTE and Chinese telecom companies.[168] Thus, given that China's publicly declared policy goal is to influence the development of 5G standards and technical specifications through international standardisation organisations and other forums, liberal democracies should ensure that the forthcoming open RAN standards are coherent with democratic values and freedoms, such as privacy and human rights. In addition, Chinese firms are very active throughout 3GPP and other international standardisation organisations.[169]

5.6. Standardisation

Vulnerabilities, threats, and risks across the whole life cycle of 5G technology must be identified and mitigated. The life cycle of 5G technology encompasses standards and soft- and hardware testing, implementation, and operation. 5G technology standards are considered key for network security, which will be built into technology by design. International technical standards for telecommunications are developed by the International Telecommunication Union (ITU) Radiocommunication Sector. In 2015, the ITU published technical requirements for 5G technology in the 'IMT 2020 Vision'.[170] The technical specifications of 5G technology are developed by the 3GPP and issued through iterative releases that are then standardised by the ITU. Figure 2 illustrates the current 3GPP roadmap of Releases 15–18. Release 15 is the first official description of 5G, and Release 16 addresses eMBB and URLLC enhancements, as well as industrial IoT, among other improvements.

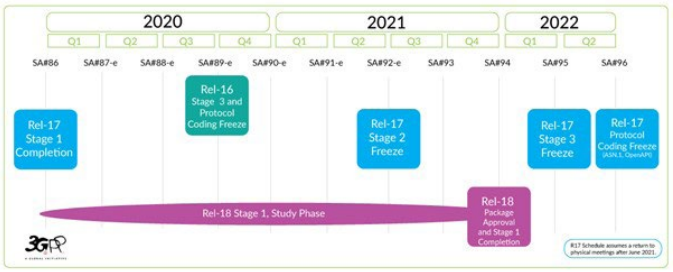

Figure 4. 3GPP roadmap

3GPP Technical Specification Group Service and System Aspects Working Group 3 develops security and privacy requirements for 5G technology.[171] With **Release 15,** 3GPP standards include, for the first time, Non-Terrestrial Networks (NTN) which are relevant for military 5G use cases. Different deployment scenarios of NTN are

163 Pål Grønsund, Andres Gonzalez, Kashif Mahmood, Kennet Nomeland, Jan Pitter, Antonios Dimitriadis, Tom-Kristian Berg, and Stephen Gelardi, '5G Service and Slice Implementation for a Military Use Case', 2020 IEEE International Conference on Communications Workshops (ICC Workshops), 21 July 2020, https://ieeexplore.ieee.org/document/9145236.

164 Pål Grønsund, Andres Gonzalez, Kashif Mahmood, Kennet Nomeland, Jan Pitter, Antonios Dimitriadis, Tom-Kristian Berg, and Stephen Gelardi, '5G Service and Slice Implementation for a Military Use Case', 2020 IEEE International Conference on Communications Workshops (ICC Workshops), doi: 10.1109/ICCWorkshops49005.2020.9145236.

165 'Open RAN' is industry's generic term for an open radio access network (RAN) architecture. An Open RAN has open interoperable interfaces, RAN virtualization, and support for big data and AI-enabled RAN. O-RAN refers to Open RAN as standardised by the O-RAN Alliance. See 'Security Considerations of Open RAN', Ericsson, August 2020, https://www.ericsson.com/en/security/security-considerations-of-open-ran. See more about security risks in open source software and Open RAN in Jason Boswell, 'Security Considerations of Open RAN', presentation, NATO CCDCOE 5G military security workshop, Tallinn, 3–4 February 2021.

166 For Open vRAN to improve security, see Eric Hanselman, 'Security Benefits of Open Virtualized RAN', 451 Research, May 2020, https://www.cisco.com/c/en/us/solutions/service-provider/5g-network-architecture.html#~products https://www.cisco.com/c/dam/en/us/solutions/service-provider/pdfs/5g-network-architecture/white-paper-sp-open-vran-security-benefits.pdf.

167 Eric Wenger, 'Are Openness and Security Both Possible in a 5G World?' 28 January 2021, Cisco blog, https://blogs.cisco.com/gov/are-openness-and-security-both-possible-in-a-5g-world.

168 For further discussion about possible risks associated with the influence of Chinese companies in the O-RAN Alliance, see 'Does Huawei Not Believe in Open RAN? Or Is Just Playing Poker with the O-RAN Alliance and Policymakers?' StandConsult, 23 March 2021, https://strandconsult.dk/does-huawei-not-believe-in-open-ran-or-is-just-playing-poker-with-the-o-ran-alliance-and-policymakers/.

169 For example, the 3GPP Technical Specification Group Service and System Aspects Working Group is chaired by a Huawei executive, and its sub-group, entitled Working Group 3, which develops security and privacy requirements for 5G technology, is chaired by a Nokia executive, and a vice chair is a Huawei executive. '3GPP Officials per TSG/WG: 3GPP Officials for Group; 3GPP SA 3 ("S3")', 3GPP, https://www.3gpp.org/DynaReport/TSG-WG--SP--officials.htm, https://www.3gpp.org/DynaReport/TSG-WG--S3--officials.htm [accessed 18 August 2021].

170 'IMT Vision: Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond'. Recommendation M.2083–0 (09/2015), https://www.itu.int/rec/R-REC-M.2083-0-201509-I/en. NCI Agency's working paper uses this definition of 5G technology; see Luis Bastos et al., 'Potential of 5G Technologies for Military Application', 15 September 2020, NCI Agency Working Paper, http://www.mindev.gov.gr/wp-content/uploads/2020/11/Enclosure-2-Working-paper-Potential-of-5G-technologies-for-military-application.pdf.

171 The main objectives of Working Group 3 include defining the requirements and specifying the architectures and protocols for security and privacy in 3GPP systems. 'SA3: Security and Privacy', 3GPP, https://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security [accessed 18 August 2021].

described in a 3GPP technical report.[172] Two possible NTN use cases for military use are:

→ Satellite or aerial vehicle with gNodeB on board and connected to 5G core network
→ Dual connectivity for a handheld or IoT device, connection with satellite or aerial vehicle and terrestrial gNodeB served by the same or independent core networks.

Release 16 not only introduces capacity and operational enhancements but also expands 5G's reach into new verticals that could facilitate the military use cases. Release 16 specifications cover a variety of applications that are relevant for the military:

1) Vehicle to Everything (V2X): platooning, extended sensors, automated driving, and remote driving
2) Non-Terrestrial Radio Access: satellites and airborne base stations
3) Maritime Communications: intra-ship, ship-to-shore, and ship-to-ship.

Release 16 work item on NR V2X introduced the possibility for side link (i.e. direct device-to-device communication). Although it is focused on the V2X scenario, the side link can be used in other scenarios as well, such as for public safety.[173]

Release 17 is expected to be finalised in July 2022.[174] It will specify general enhancements for Release 16 features, including NR side link, DSS, Network Slicing, Non-Public Networks (NPN), and NR over Non-Terrestrial Networks. According to the 3GPP work plan, Release 17 will include several studies on supporting Unmanned Aerial Systems (UAS) that can be relevant for developing military 5G use cases.[175] The Release 17 work plan includes multiple studies on security aspects, including a technical report on 5G security enhancements against False Base Station attacks, also known as International Mobile Subscriber Identity (IMSI) catchers.[176] The report offers risk-mitigation solutions against types of attacks that were commonly launched against the radio interface of the previous generation of mobile technologies (4G LTE, 3G and 2G).

From a network security point of view, 3GPP Technical Specification 33.501 specifies 5G general system security architecture and procedures. The standardised security specifications probably meet the needs of commercial 5G deployments but would be insufficient to cover the security needs of a whole spectrum of military applications. Some security mechanisms specified in 3GPP Technical Specification 33.501 that could be used to improve the overall network security are mentioned as optional (for example, secondary authentication) or are simply omitted from the scope of the 3GPP standards. For example, public key infrastructure (PKI) management for the keys used to protect the Subscription Permanent Identifier (SUPI) are not included in these standards.[177] Further studies are needed regarding the implementation of the existing security features prescribed by the standards, and regarding what additional security requirements (not included in the standards) should be implemented.

Security requirements for military communications are 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 may not prioritise those concerns for their own needs. Thus the defence sector's security requirements should be incorporated by default into the development of standards and technical specifications. The number of NATO nations' industry representatives at standard-setting bodies should be increased, and NATO military representatives should cooperate closely with the industry to ensure that military specifications are considered. For example, the Chinese government supports Chinese MNOs' participation in the standardisation bodies to promote national standards and orders those firms to support Chinese national interests, which allegedly has swayed 5G standardisation decisions in Huawei's favour. As an illustration of Huawei's influence on standards, 3GPP has approved about one-fourth of all the 4G proposals from Huawei. [178]

5.7. Certification

Cybersecurity certification requires the formal evaluation of products, services, and processes by an independent and accredited body against a defined set of criteria, standards, and the issuing of a certificate indicating conformance.[179]

Globally, there are two international arrangements relevant to assuring 5G product security. The Network Equipment Security Assurance Scheme (NESAS), developed jointly by GSMA and 3GPP, covers security assessments of 5G vendor development and product life cycle processes and security evaluations of network products. The

172 '3GPP TR 38.811: Study on New Radio (NR) to Support Non-Terrestrial Networks', 3GPP, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3234 [accessed 18 August 2021].

173 '5G Americas White Paper, 3GPP Releases 16 and 17 and Beyond', January 2021, https://www.5gamericas.org/wp-content/uploads/2021/01/InDesign-3GPP-Rel-16-17-2021.pdf.

174 Release 15 was finalised in June 2018 and informally referred to as 5G Phase I. Release 16 was finalized in June 2020 and informally referred to as 5G Phase II.

175 '3GPP Work Plan', https://www.3gpp.org/specifications/work-plan [accessed 18 June 2021].

176 '3GPP TR 33.809: Study on 5G Security Enhancements against False Base Stations (FBS) Version 0.15.0', 3GPP, https://www.3gpp.org/ftp/Specs/archive/33_series/33.809/33809-0f0.zip [accessed 20 June 2021].

177 The secondary authentication allows the operator to delegate the authorisation to a third party. It is meant for authentication between user equipment and external data networks residing outside the operator's domain. Similar service was also possible in 4G, but it is now integrated into 5G architecture.

178 Rubin et al., 'The Huawei Moment'.

179 'EU Cybersecurity Certification Framework', ENISA, https://www.enisa.europa.eu/topics/standards/certification [accessed 13 July 2021].

overall objective of NESAS is to provide an industry-wide security assurance framework and security baseline to facilitate improvements in security levels across the whole mobile industry. However, NESAS does not accredit or certify equipment vendors or their products. Moreover, participation of mobile network equipment vendors in NESAS is voluntary, and at the time of publication of this Research Report, major equipment vendors have had their development and product life cycle management processes assessed.[180] After a vendor's development and product life cycle processes have been audited, network products can be evaluated by an accredited NESAS Security Test Laboratory. The vendors who have accredited their equipment as of July 2021 are Nokia, Ericsson, Huawei and ZTE.[181] In August 2020, Huawei announced that its 5G RAN gNodeB, 5G Core UDG, UDM, UNC, UPCF, and LTE eNodeB passed NESAS. According to Huawei, NESAS assessment is a valuable reference for MNOs, 5G equipment vendors, government regulators, and application service providers, and Huawei urges the industry to widely adopt it.[182] However, the value of NESAS accreditation is questionable, because in recent years, Huawei's software development practices have continued to pose significant risks to MNOs operating in the UK, as assessed by the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. [183]

Secondly, 5G products can also be certified under the Common Criteria Recognition Arrangement (CCRA), which is currently composed of 31 member countries. Under the arrangement, certification bodies and licenced laboratories for testing IT products are designated in the member countries, which are listed on the CCRA webpage. After assessing and approving IT products and protection profiles, a certification body issues a Common Criteria certificate complying with consistent standards, which can be used in all member countries for procuring IT products without the need for further evaluation. The telecommunication industry can have their products evaluated once and thereafter sell them to all member countries.[184] For example, among network and network-related devices and systems, ZTE obtained a CCRA certificate for 5G RAN in 2021, and Huawei obtained one for 5G gNodeB software in 2020.[185]

In the EU, the Cybersecurity Act, which entered into force in June 2019, created a framework for European cybersecurity certification schemes for products, processes, and services.[186] The certification framework provides EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards, and procedures.[187] In May 2021 ENISA published a Common Criteria-based European candidate cybersecurity certification (EUCC) scheme, which does not address 5G networks but does address ICT products, services, and processes more broadly.[188]

In a 2019 document entitled 'Cybersecurity of 5G Networks', the European Commission recommends that the new cybersecurity certification framework also be applied to 5G equipment and software in order to promote consistent security levels.[189] The document notes that the development of cybersecurity certification schemes for ICT products, services, or processes used for 5G networks should be an immediate priority for the member states. It further suggests that 5G networks should be protected across their entire life cycle, including design, development, procurement, and deployment, as well as the operation and maintenance phases of 5G equipment and networks.[190] Similarly, the Toolbox requires the EU certification to be used for 5G network components, customer equipment, and equipment suppliers' processes, as well as for devices and cloud services, which are connected to 5G networks.[191] The European Commission asked ENISA to develop a candidate European cybersecurity certification scheme for 5G networks. In February 2021, ENISA announced that it would proceed with the preparation of the cybersecurity certification scheme, taking into account the existing cybersecurity certification schemes.[192] In July 2021, ENISA launched an ad hoc working group on 5G cybersecurity certification.[193]

---

180 'NESAS FAQs', GSMA, https://www.gsma.com/security/nesas-faqs/ [accessed 15 July 2021].

181 'NESAS Evaluated Network Equipment Products', https://www.gsma.com/security/nesas-evaluated-network-equipment-products/ [accessed 15 July 2021].

182 'Huawei 5G: Passes GSMA's Network Equipment Security Assurance Scheme', Huawei, 20 August 2021.

183 According to the latest report of HCSEC, Huawei's approach to software development brings significantly increased risk to UK operators. See 'Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2020', Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, September 2020, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2020.

184 'The Common Criteria', https://www.commoncriteriaportal.org/ [accessed 15 July 2021].

185 'Certification Report', 4 June 2020, https://www.commoncriteriaportal.org/files/epfiles/2018-60-INF-3128.pdf; 'Certified Products', Common Criteria, https://www.commoncriteriaportal.org/products/ [accessed 15 July 2021].

186 'Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures'.

187 'The EU Cybersecurity Certification Framework', European Commission, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework [accessed 13 July 2021].

188 'Cybersecurity Certification: Candidate EUCC Scheme V1.1.1', ENISA, May 2021, https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1.

189 'Commission Recommendation of 26 March 2019 on Cybersecurity of 5G Networks'.

190 'Commission Recommendation of 26 March 2019 on Cybersecurity of 5G Networks'.

191 'Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures'.

192 'Securing EU's Vision on 5G: Cybersecurity Certification', ENISA, 3 February 2021, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification.

193 'Ad-Hoc Working Group on 5G Cybersecurity Certification', ENISA, https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification [accessed 13 July 2021].

In the US, there is no cybersecurity certification scheme for 5G networks and devices. Although the 2020 'CISA 5G Strategy' does not address the certification of 5G systems, it announces plans to evaluate key existing 5G components and identify security vulnerabilities in cooperation with academia and industry.[194] The CISA has established the ICT Supply Chain Risk Management (SCRM) Task Force with the aim of identifying and developing consensus strategies to enhance the overall ICT supply chain security (not specific to 5G).[195] The Federal Communications Commission's advisory committee 'Communications Security, Reliability, and Interoperability Council VII' has established several working groups on 5G security and published several reports on 5G security. For example, the March 2021 report recommends ways to mitigate the risks introduced by 3GPP Releases 15 and 16. It also identifies optional features in 3GPP standards that can diminish the effectiveness of 5G security and recommends ways to address these gaps.[196] In addition, in keeping with the 'National Strategy to Secure 5G' released by the White House in March 2020, the CISA has established working groups assessing risks and vulnerabilities to 5G infrastructure, and has released reports on 5G security. [197] As mentioned, in May 2021 the CISA released a report entitled 'Potential Threat Vectors to 5G Infrastructure'.[198]

The 5G Supply Chain Working Group of the Alliance for Telecommunication Industry Solutions, which was established in 2019, aims to identify and develop standards for 5G systems and evaluate audit and certification options for ICT solution providers and infrastructure and endpoint device equipment manufacturers.[199] In November 2020, the Federal Mobility Group published a framework to conduct 5G security testing.[200] As a follow-up to the 'National Strategy to Secure 5G', the implementation plan released by the National Telecommunications and Information Administration in January 2021 also addresses efforts to expand the national and international capacity related to testing and evaluation of 5G technology.[201]

6. Military 5G Network Use Cases

The key advances of 5G NR were mentioned in the introduction of this Research Report (e.g. bandwidth, speed, low latency, reliability, security, and connectivity).[202] Broadly speaking, 5G technologies provide higher throughput (improved data rates), lower latency (time delay), and a higher density and mobility range. Military 5G networks can enable voice, video, chat, and push-to-talk services. According to Ericsson, 5G can be used by the military for users' communication and security, logistics and asset protection, and agile and remote deployment.[203]

Potential military applications of 5G technologies include autonomous vehicles, Command and Control (C2), logistics, maintenance, augmented and virtual reality, and Intelligence Surveillance and Reconnaissance (ISR) systems. Autonomous military vehicles could potentially circumvent on-board data processing limitations by storing large databases (e.g. maps) in the cloud. Safe vehicle operations would require 5G's high data rates and low latency to download off-board information and synthesise it with on-board sensor data. Likewise, 5G could be used to transfer sensor data between operators and unoccupied vehicles and to network vehicles, potentially enabling new military concepts of operations, such as swarming (i.e. cooperative behaviour in which vehicles autonomously coordinate to achieve a task).[204]

5G technologies could be incorporated into ISR systems, which increasingly demand high bandwidths to process, exploit, and disseminate information from a growing

194 'CISA 5G Strategy', CISA, August 2020, https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf.

195 'Framework to Conduct 5G Testing', Federal Mobility Group, November 2020, https://www.cio.gov/assets/files/Framework-to-Conduct-5G-Testing-508.pdf, p. 9.

196 'Communications Security, Reliability, and Interoperability Council VII', Federal Communications Commission, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii [accessed 15 July 2021].

197 'National Strategy to Secure 5G', White House, March 2020, https://www.hsdl.org/?view&did=835776.

198 'Potential Threat Vectors to 5G Infrastructure', CISA, May 2020, https://www.cisa.gov/publication/5g-potential-threat-vectors.

199 'New ATIS Working Group Addresses 5G Supply Chain Standards and Development of Assured Commercial 5G Networks', ATIS, 6 November 2019, https://www.atis.org/press-releases/new-atis-working-group-addresses-5g-supply-chain-standards-and-development-of-assured-commercial-5g-networks/.

200 'Framework to Conduct 5G Testing'.

201 'National Strategy to Secure 5G Implementation Plan', National Telecommunications and Information Administration, 19 January 2021, https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf.

202 The five key technologies that bring opportunities for militaries are spectrum, 5G NR, 5G core network, proximity services, and non-terrestrial networks. See Bastos et al., 'Potential of 5G Technologies for Military Application'. In addition, NATO STO IST-187, '5G Technologies Application to NATO Operations', examines the applicability of 5G functionality in military scenarios in operations. See '5G Technologies Application to NATO Operations', NATO STO, https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16937 [accessed 21 June 2021].

203 Kelly Krick, presentation at the NATO CCDCOE, 5G Supply Chain and Network Security Workshop, 9 June 2021.

204 'National Security Implications of Fifth Generation (5G) Mobile Technologies', Congressional Research Service, 4 June 2021, https://fas.org/sgp/crs/natsec/IF11251.pdf.

number of battlespace sensors. This could provide commanders with timely access to actionable intelligence data, thus improving operational decision-making. Similarly, 5G will reduce latency in other data-intensive activities, such as logistics and maintenance, and could also enable augmented or virtual reality environments that could enhance training. Similarly, C2 could benefit from the high-speed, low-latency capability of 5G by improving the decision-making cycle. For example, satellite communications are currently used for long-distance communications, but satellites increase latency due to the large distance a signal needs to travel, causing delays in the execution of military operations.[205]

This section addresses three use cases that NATO Allies could employ in deploying their armed forces and equipment from North America to Europe during peacetime and in an operational environment. In order to deploy troops and military equipment through different physical jurisdictions across the Alliance, the military largely uses the host nation's civilian and commercial infrastructure, such as seaports, railroads, and highways. In doing so, it relies largely on those commercial providers for its communications and energy supply (e.g. fuel, electricity). When the military utilises civilian infrastructure, the latter will be protected by the country (host nation) in which this infrastructure resides. As the majority of infrastructure is owned or operated by public institutions or commercial enterprises, close cooperation is needed between the stakeholders. The key stakeholders are 5G network operators, MNOs, and vertical business case users, such as maritime port authorities, operators of ITS, and smart warehouse operators.

When armed forces are deploying troops and equipment abroad for humanitarian missions or for peacetime deployments such as military exercises, they rely on civilian infrastructure. In areas where there are 5G networks, militaries can connect their private 5G networks to public and commercial 5G networks and the broader 5G 'ecosystem' of verticals, such as smart ports, smart warehouses, and ITS. In the context of the military use of public 5G networks, the armed forces need to ensure that public 5G networks are secure, reliable, and available. This could be done, for example, through network slicing which provides isolation for the military, implementing additional Zero Trust models, and mitigating security risks by limiting the type of military use cases that are implemented on the public 5G networks. If public 5G networks are based on open source software, additional security measures are necessary due to the greater security risks in open source software.

The three deployment models for military (which can coexist) are envisioned in the peacetime operational environment as follows:

→ Private 5G network deployment model

The military uses a private 5G network, which is not connected to public 5G networks or to the Internet. This military network has private RAN and a core network and can be deployed to a mission area where it operates autonomously from local MNOs.[206]

→ Hybrid 5G network deployment model

The military uses components (such as antennas and base stations) of a private 5G network, which are connected to components of a public 5G network (for example, to public RAN or a core network).

→ Public 5G network deployment model

The military uses a public 5G network, which has a dedicated (i.e. isolated) network slice for military use.

The use of a 5G network for expeditionary operations also depends on the availability of radio spectrum in a host nation. It must be taken into account that in the Baltic States, some radio frequency bands may not be available. For example, Russia has reserved 3.6 GHz for its military satellites and law enforcement and uses 700 MHz, which may mean that fewer radio frequency bands are available for MNOs in the Baltic States. In addition, if a host nation uses other bands than a NATO nation that deploys its military 5G network to that country, the two may not be interoperable, due to different radio frequency bands, because end-user devices may be designed for specific bands only. Thus the availability of radio spectrum should be considered when planning deployment scenarios for 5G military networks.

The next sections describe the three military 5G use cases which are likely to use hybrid or public network deployment models.

6.1. Smart Sea Port

Shipping carries around 90% of the world's freight, thereby providing a backbone for global trade and the global economy; it is also crucial for military mobility. With the use of IoT and 5G networks, sea port facilities may become much more efficient with real-time monitoring, real-time ship-to-shore communication for port-to-vessel traffic management, and just-in-time operations. A Smart Port can include sensors, edge computing, handsets, augmented reality devices, and autonomous vehicles and vessels. One example is the 5G test bed built by the Hamburg Port Authority (HPA), Deutsche Telekom,

205 'National Security Implications of Fifth Generation (5G) Mobile Technologies'.

206 The military 5G network is isolated from the Internet by default, but it should be possible to allow access to and from some trusted domains. Communication between military users and with military applications should use end-to-end encryption. See Grønsund et al., '5G Service and Slice Implementation for a Military Use Case'.

and Nokia, which demonstrates three 5G use cases that require URLLC, eMBB, MTC, and network slicing. Each use case is based on service level agreements between partners. One network slice is created for each use case, with all slices using the same 5G radio infrastructure.[207]

In this scenario, a shore-based public 5G network radio cell provides ship-to-shore connectivity in addition to satellite communications for the military through network slicing, where the military slice is isolated. The second possibility is to implement shipborne 5G military radio cell in the 700 MHz band on an amphibious assault ship connected to shore through military 5G gNodeB located in the port area. A public 5G network is used for transporting weapons platforms and military vehicles to smart warehouses. After military equipment is stored in the warehouses at the port area, a low radio spectrum band 5G military network is used for vehicle platooning, which will be discussed in the second use case.

In case of North American troop deployment in European harbours, the EU 5G pioneer frequency bands (700 MHz, 3.6 GHz, 26 GHz) need to be used as a first priority or, alternatively, other EU frequency bands which are allocated for mobile communication and use 4G/5G spectrum sharing.

6.2. Intelligent Transportation System

With its low latency, high capacity, and reliability, 5G technology has the potential to provide increased visibility and control over transportation systems with end-to-end connectivity and the possibility of an ITS with autonomous vehicles.[208]

The roll-out of 5G technology architecture will support many types of communications for transportation for both companies and private citizens. Some of the most important communications include:

- → Vehicle-to-Vehicle (V2V), where vehicles relay signals directly to each other
- → Vehicle-to-Infrastructure (V2I), where vehicles communicate with sensors on infrastructure such as bridges, roads, and traffic lights
- → Vehicle-to-Person (V2P), where vehicles detect persons posing a risk
- → Vehicle-to-Everything (V2X), where vehicles may react to anything posing a risk

The platooning of vehicles is a method for moving a group of vehicles together. This method allows trucks to accelerate or brake simultaneously, thereby reducing the distance between vehicles and increasing vehicle capacity on existing roads. This method also reduces fuel consumption through the control of speed, braking and acceleration, and reduction of drag. Finally, road safety may also be improved by reducing road collisions and driver fatigue.

Static platooning involves the movement of a number of pre-planned group vehicles from one location to another in a cooperative manner. Dynamic platooning involves vehicles with operators cooperating to link platoons in transit, with vehicles joining and leaving the platoon as needed.[209] To enable these types of platooning, vehicles are required to have a high level of autonomy. Furthermore, platooning requires support from appropriate roadside and network infrastructure to enable the vehicles to operate in a cooperative manner.

The EU is helping to build 5G coverage on all major transport routes, including the trans-European transport networks.[210] This will create an opportunity for military mobility to benefit from 5G connectivity and related services, such as Cooperative, Connected and Automated Mobility (CCAM), which belongs to ITS.[211] Military transporting trucks will be connected to other vehicles, transport infrastructure, and other users in order to coordinate their actions. A local network is created for the platooning between the trucks and is protected from unauthorised users.

6.3. Public Safety

In the context of crisis management and disaster response, the military will invariably be working alongside civilian actors with whom it will have to coordinate.[212] A public

207 Adlane Fellah, '5G Smart Sea Port: Hamburg Port Authority', Nokia, 2019, https://onestore.nokia.com/asset/206571 [accessed 21 June 2021].

208 The levels of autonomy of vehicles are described in the Society of Automotive Engineers International document 'Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_201806', Society of Automotive Engineers International, 15 June 2018, https://www.sae.org/standards/content/j3016_201806/.

209 Platooning enables the vehicles to dynamically form a group travelling together. All the vehicles in the platoon receive periodic data from the leading vehicle in order to carry on platoon operations. This information allows the distance between vehicles to become extremely small, i.e. the gap in terms of time can be miniscule (sub second). Platooning applications may allow the vehicles following to be autonomously driven. '5G Trials for Cooperative, Connected and Automated Mobility along European 5G Cross-Border Corridors. Challenges and Opportunities', White Paper, 5G PPP H2020 ICT–18–2018 Projects, Version 1.0, October 2020, https://5g-ppp.eu/wp-content/uploads/2020/10/5G-for-CCAM-in-Cross-Border-Corridors_5G-PPP-White-Paper-Final2.pdf, p. 16.

210 'Connecting Europe Facility (CEF2) Digital: Shaping Europe's Digital Future', European Commission, 12 March 2021, https://ec.europa.eu/digital-single-market/en/connecting-europe-facility-cef2-digital.

211 'Cooperative, Connected and Automated Mobility', Mobility and Transport, European Commission, https://ec.europa.eu/transport/themes/its/c-its_en [accessed 21 June 2021].

212 Crisis management is an iterative process of organised and coordinated actions by and among all responsible stakeholders at the local, national, regional, and international levels. A multiplicity of actors are involved in any given emergency situation – local, regional, international, state, and non-state (i.e. NGOs); nevertheless, first responders are usually state and local authorities who possess the instruments and tools for immediate response (fire, police, and emergency medical services agencies). 'Crisis and Crisis Management', CMDRCOE, https://www.cmdrcoe.org/menu.php?m_id=112 [accessed 21 June 2021].

safety 5G network provides mission-critical services, which enable first responders (law enforcement, rescue service officers, fire brigades, emergency medical personnel) to set up voice calls, including broadcast and group calls; to stream high-definition videos; and to send data (maps, locations, and messages) and other relevant information to create situational awareness.[213] The military may have an isolated slice of the public safety 5G network. The military IoT (such as sensors on drones or vehicles) can provide invaluable input to crisis management and disaster response – for example, aerial reconnaissance of a flooded area can capture precise and up-to-date images of the evolving situation on the ground. 5G networks will give the military the opportunity to share data with first responders on a 5G network and hence assist in disaster response.

Public safety 5G networks dedicate a 'fast lane' that provides highly secure communications such as priority access, more network capacity, and a resilient, hardened connection.[214] Due to its better reliability, security and availability, the use of a public safety network is preferable to the use of a public (commercial) 5G network. In emergency situations, heavy use can overload public 5G networks, which would limit the communication of first responders due to congestion and capacity issues. In cases when a public 5G network or public safety 5G network is unavailable, the military could provide a private 5G network for ensuring communication and situational awareness for public safety actors. However, the use of military 5G networks by first responders will inevitably increase supply chain and network security risks to military networks, and those risks should be carefully examined and mitigated as much as possible. In some cases (for example, in supporting the military's own mission critical services), merging military 5G networks with public safety or public 5G networks must be avoided.

If a public safety 5G network is functional and operational, but the military does not have a local base station in that geographic area, it can use an isolated slice of a public safety network for its own communication purposes, contributing to a shared situational awareness.

Examples from today's pilot projects include the Norwegian armed forces' pilot project 5G-VINNI, which deploys a fixed 5G network (gNodeB and Enterprise Edge). It provides multiple use cases, including public safety and disaster recovery with drone control for remote examination. 5G-VINNI also uses AI and ML.[215] Another Norwegian armed-forces project, Fudge-5G, includes the mobile cellular service Cell of Wheels.[216] Likewise, the US has developed 5G test beds for first-responder scenarios (such as the Cosmos test bed in New York City and the Powder test bed in Salt Lake City).[217]

7. Workshop Conclusions

On 9 June 2021, the CCDCOE organised an informal workshop, 'Military 5G Networks' Supply Chain and Network Security'. Subject matter experts from academia, the telecommunications industry, NATO, and NATO nations gave presentations and discussed the topic with a view to offering suggestions for future research directions. A summary of those discussions is captured in the conclusion. Participants of the workshop expressed interest in receiving continuous updates and an overview of CCDCOE research in this area in the future.

7.1. 5G Deployment Models

The Research Report describes three military 5G network use cases and three deployment models: private, hybrid, and public. Participants of the workshop tended to agree that a private 5G network is the preferred deployment scenario for the military, but due to technical and/or legislative requirements (e.g. no available radio frequencies), it will not always be available. Characteristics of the use case are also important; for instance, a smart warehouse could use a public 5G network but a deployed military headquarters could not due to the higher degree of security required for military command and control. Generally speaking, vulnerabilities, risks, and threats do not differ significantly across the three deployment models (private, hybrid, and public), but there may be some differences, e.g. private 5G networks may not have active roaming interfaces.

Workshop participants proposed that NATO establish its

213 'Deployable 5G Network for Public Protection and Disaster', Fudge-5G, https://fudge-5g.eu/en/use-cases/ppdr [accessed 21 June 2021].

214 'FirstNet Was Created to Be a Force-Multiplier for First Responders – To Give Public Safety Lifesaving, 21st Century Communication Tools', First Net Authority, https://firstnet.gov/network [accessed 21 June 2021].

215 'Norway Main Facility Site', 5G-Vinni, https://www.5g-vinni.eu/norway-main-facility-site/ [accessed 21 June 2021].

216 Other mobile deployment possibilities in use are a cell on light trucks, a cellular repeater on wheels, and a generator on a trailer.

217 Ashutosh Dutta, 'Keysight Mil-Grade 5G Panel Discussion', Johns Hopkins Applied Physics Laboratory, https://on24static.akamaized.net/event/30/73/06/3/rt/1/documents/resourceList1617988089681/ashutoshduttausecaseslides1617988088286.pdf [accessed 21 June 2021].

own NATO-accredited virtual MNO (MVNO) and distribute e-SIMs to nations in order to facilitate the deployment of 5G military networks. NATO nations should certify a defence/NATO network slice in national commercial networks that conforms to common standards (security, quality of service, etc.). This would enable the Alliance to ensure a common baseline security level across networks.

7.2. 5G Network Security

Workshop participants opined that network security needs to be integrated as early as possible into the design, building, and initial deployment of the 5G network. NATO and NATO nations can influence MNOs regarding the security level of network architecture and services they provide. When the military operates through public 5G networks in NATO nations, they need to understand who is responsible in a particular country for incident response in commercial networks (i.e. does the main responsibility lie with the MNO or with a national authority responsible for cyber security?). The military must be aware of vulnerabilities, risks and threats in those networks and must be able to prevent, mitigate, and respond to the threats that affect defence segments (e.g. defence network slice). NATO nations' armed forces must cooperate with national vendors and MNOs to gain insight into commercial 5G networks' security posture. NATO should determine appropriate network security levels for the specific use case and deployment model. Security controls must be balanced with competing needs, as higher security requirements may impact on the quality of service (e.g. increased latency). NATO should collectively determine what security levels are appropriate for NATO missions and operations. NATO nations should therefore jointly develop minimum security requirements for reference deployment models which nations could apply to national military use cases.

Military usage of a public 5G network should assume by default that the network has been compromised. Therefore, Zero Trust Security is an inevitable component of ensuring network security. The main network security concerns for the military are data protection and geo-location, as well as the confidentiality of metadata. Threats on availability are more important for the military than for commercial 5G networks, because availability is critical for conducting military operations.

Zero Trust Security focuses on assuring confidentiality and integrity but does not provide greater availability. Threats to the availability of the 5G core network could be mitigated via dynamic networking provided by the Software Defined Network architecture. Threats to RAN (e.g. jamming) should be assessed as well.

Participants opined that NATO, as a political-military organisation, should, through appropriate industry representation, participate in the 3GPP standardisation bodies' work, and the interests of the defence sector should be taken into account by design (and not merely as an afterthought) when developing standards and technical specifications. During the workshops, questions arose regarding this aspect: will militaries need to modify 3GPP specifications for military use after they have been adopted for the commercial service providers, or should military stakeholders drive the 5G technology standardisation process in order to incorporate functionality and military-grade network security requirements for military applications?

It was highlighted that in the case of hybrid and public 5G models, the military must have a comprehensive understanding of vulnerabilities, threats, and risks in commercial networks and constantly assess whether the MNO's network and supply chain security posture is sufficient for military use. For example, regular accreditation of products and services of commercial networks may be insufficient, and more dynamic risk assessments may be required. Network security threats can emerge from personal devices used in 5G networks. Some 5G user equipment has limited security functions implemented and thus should be avoided or upgraded to the military-grade level of security.

It was expressed that at present, the military lacks insight into the network and supply chain security posture of MNOs, and it would be useful for the military to develop ways and means to gain better monitoring, testing, assessment, and other such capabilities regarding public 5G networks. Risk assessment and auditing should be a continuous process (i.e. not simply conducted once prior to the deployment of the use case). Due to the evolving threats and landscape, dynamic risk assessments are required.

7.3. 5G Test Bed

Cooperation between test beds is needed, because many 5G test beds conduct testing and experimentation for the same use cases. Currently, the 5G-VINNI and FUDGE 5G trials in Norway would be considered the most advanced ongoing 5G trial projects in Europe. US Department of Defense Tranche 2 has also established test beds focused on 5G security (for example, a Joint Base in San Antonio, Texas), and these military test beds will be integrated with public 5G networks.

The question of whether the CR14 5G SA test bed can be used to test the security features of the three use cases is unclear and must be elaborated in the future work during 2021–2022. In general, private 5G networks can be considered a more secure deployment model than hybrid or public ones, due to the better isolation capability of the former. For this reason, in the short term, research should focus on testing the security of the private 5G networks, and hybrid and public deployment models can be tested later on.

8. Recommendations

8.1. Supply Chain Security

NATO should set trustworthiness criteria for high-risk 5G equipment manufacturers and associated service providers with a view to mitigating malicious intent (such as the insertion of vulnerabilities, interception, or disruptions of supply). In cooperation with the EU, risk assessment and management procedures and the baseline criteria for supply chain and network security should be developed and implemented in cooperation with MNOs (taking into account that untrusted elements also exist in trusted networks). Mitigating supply chain risks requires a close public-private partnership of NATO, national governments, and industry.

MNOs should share information with governments and armed forces regarding security controls of critical network functions (notably, pertaining to soft- and hardware, systems, and products and services) and provide information on the security vetting of personnel who have access to them.

8.2. Network Security

NATO nations should jointly determine appropriate network security levels and add-ons to commercial security controls for military-grade networks and associated services. NATO should determine common criteria for the certification of products and services.

Further research should be encouraged with regard to technical network security challenges, including on how to apply Zero Trust Security principles and respective industry tools, end-to-end encryption for military communications over 5G networks, autonomy and automation for monitoring and detection, and AI-enabled analytics and security.

8.3. Policies and Standards

NATO nations should harmonise national strategies and policies to secure commercial and military 5G networks. NATO should consider developing a strategy and/or roadmap for the development of military 5G use cases, addressing, among other things, interoperability of equipment, services, and the radio frequency spectrum. The roadmap should identify the type of military use cases deployed over commercial networks and deployment scenarios for private (military/defence/NATO) 5G networks.

NATO's standards development organisation should consider how the current 3GPP standards address the security requirements of the military. NATO nations should certify products, processes, and services associated with 5G technology according to jointly agreed criteria, taking into account the existing certification schemes and assessing their value and sufficiency. Nations should actively participate in standardisation work.

NATO nations should ensure the interoperability of national commercial and military 5G networks.

NATO should consider developing Alliance-wide standards for resilient, reliable, available and secure civilian and military 5G networks and consider military-grade standards for military networks.

8.4. Research, Education, and Training

Further research should explore the opportunities 5G technologies can provide for improving Allied defence and deterrence and the security risks inherent in these networks. Awareness raising concerning risks associated with both public (commercial) and military 5G networks should continue targeting specific training audiences (such as the general public, parliaments, decision-makers in government and industry, and military officers). NATO nations should also commission studies to determine what competence and skills are needed in the armed forces and NATO to enable the deployment of military 5G networks and ensure their security.

Further research is needed into what use cases are feasible and less risky from a security point of view. For example, integrating mission-critical C2 with commercial 5G networks in an armed conflict/combat scenario may be too risky, but the use of commercial 5G networks for uses cases such as predictive maintenance, vehicle platooning, or AR/VR training might be feasible.

NATO nations should invest into network security testing laboratories (such as Estonia's Cyber Range CR14 5G SA test bed) and encourage cooperation between test beds.

NATO should commission research on practical ways and means to enhance nations' participation in global standardisation work.

O-RAN should be studied in terms of opportunities to increase security, the interoperability of products, and market diversity, as well as to assess risks emerging from open source technology. O-RAN standards should follow the industry best practices. This research should recommend ways and means to mitigate O-RAN risks.

Further research is also needed on how to establish a

NATO-owned and -accredited virtual MNO and e-SIM that NATO nations could use.

8.5. Partnerships

NATO nations should enhance timely information and best-practices-sharing, including risk assessments, concerning commercial and military 5G networks. To this end, nations should establish points of contact and create subject-matter-expert networks in relevant government and armed forces organisations. Similar networks of experts should be created with the participation of universities, research institutions, and industry.

Governments and armed forces should have sufficient visibility of supply chain and network security processes, procedures, and practices used by manufacturers of 5G technology and providers of associated services (such as MNOs and cloud service providers). Armed forces should establish partnerships with commercial service providers and equipment manufacturers that enable them to assess risks and assure the integrity, security, resilience, privacy, and quality of the acquired products, systems, and services throughout their life cycle. 5G network service providers should be encouraged to cooperate with armed forces to access the security controls of RAN, MEC, core network, and other critical functions. MNOs should share confidential information with armed forces on issues such as their 5G risk assessments, security policies and controls, and certification of their network components.

NATO and the EU should set up a regular informal consultation body to jointly assess risks and develop mitigation measures across strategic, technical, and supportive dimensions, building on the EU's experience with risk assessments and the Toolbox.

Technology can be neutral and value-agnostic in principle, but it rarely is in practice. NATO should counterbalance China's ambitions to attain global dominance in key EDT by developing like-minded technologies that are trusted, secure, reliable, available and resilient. NATO should support the adoption of this trusted technology globally, while refraining from using authoritarian opponents' technology that is commonly used undermine democratic values and freedoms.

9. References

→ 3GPP. '3GPP TR 33.809: Study on 5G Security Enhancements against False Base Stations (FBS) Version 0.15.0', https://www.3gpp.org/ftp/Specs/archive/33_series/33.809/33809-0f0.zip [accessed 20 June 2021].

→ 3GPP. '3GPP TR 38.811: Study on New Radio (NR) to Support Non-Terrestrial Networks', https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3234.

→ 3GPP. '3GPP Officials per TSG/WG: 3GPP Officials for Group; 3GPP SA ("SP")'. https://www.3gpp.org/DynaReport/TSG-WG--SP--officials.htm [accessed 18 August 2021].

→ 3GPP. '3GPP Officials per TSG/WG: 3GPP Officials for Group; 3GPP SA 3 ("S3")'. https://www.3gpp.org/DynaReport/TSG-WG--S3--officials.htm [accessed 18 August 2021].

→ 3GPP. '3GPP Work Plan', https://www.3gpp.org/specifications/work-plan [accessed 18 June 2021].

→ 3GPP. 'DSS: Dynamic Spectrum Sharing', 14 October 2020, https://www.3gpp.org/dss.

→ 3GPP. 'SA3: Security and Privacy'. https://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security [accessed 18 August 2021].

→ 5G Americas. '3GPP Releases 16, 17 and Beyond', January 2021, https://www.5gamericas.org/3gpp-releases-16-17-beyond.

→ 5G Americas. '5G and LTE Deployments', https://www.5gamericas.org/resources/deployments/ [accessed 23 July 2021].

→ 5G Americas. 'The Evolution of Security in 5G', July 2019, https://www.5gamericas.org/the-evolution-of-security-in-5g-2/.

→ 5G Americas. 'Security Considerations for the 5G Era', July 2020, https://www.5gamericas.org/security-considerations-for-the-5g-era/.

→ 5G-MoNArch. 'Smart Sea Port Use Case', https://5g-monarch.eu/smart-sea-port-use-case/ [accessed 23 July 2021].

→ 5G-PPP. '5G Infrastructure Public Private Partnership', https://5g-ppp.eu/ [accessed 23 July 2021].

→ 5G-PPP. '5G Trials for Cooperative, Connected and Automated Mobility along European 5G Cross-Border Corridors: Challenges and Opportunities', White Paper, 5G PPP H2020 ICT-18-2018 Projects, Version 1.0, October 2020, https://5g-ppp.eu/wp-content/uploads/2020/10/5G-for-CCAM-in-Cross-Border-Corridors_5G-PPP-White-Paper-Final2.pdf.

→ 5G-VINNI. 'Norway Main Facility Site', https://www.5g-vinni.eu/norway-main-facility-site [accessed 21 June 2021].

→ 5G-VINNI. 'Moving Experimentation Facility Site (Satellite Connected Vehicle)', 5G-Vinni, https://www.5g-vinni.eu/moving-experimentation-facility-site/ [accessed 21 June 2021].

→ Adaptive Mobile Security. 'A Slice in Time: Slicing Security in 5G Networks – White Paper', 24 March 2021, https://www.adaptivemobile.com/newsroom/press-release/adaptivemobile-security-details-major-security-flaw-in-5g-core-network-slicing-design.

→ Ahlander, Johan, and Supantha Mukherjee. 'Swedish Court Upholds Ban on Huawei Selling 5G Network Gear', Reuters, 22 June 2021, https://www.reuters.com/technology/swedish-court-upholds-ban-huawei-selling-5g-network-gear-2021-06-22/.

→ ATIS. 'New ATIS Working Group Addresses 5G Supply Chain Standards and Development of Assured Commercial 5G Networks', 6 November 2019, https://www.atis.org/press-releases/new-atis-working-group-addresses-5g-supply-chain-standards-and-development-of-assured-commercial-5g-networks/.

→ Bastos, Luis. '5G Technologies for Military Applications', *NITECH: NATO Innovation and Technology*, no. 5, June 2021, https://issuu.com/globalmediapartners/docs/nitech_issue_05_jun_2021?fr=sYzc0ZTM3OTA3MDU.

→ Bastos, Luis, Germano Capela, and Alper Koprulu. 'Potential of 5G Technologies for Military Application', 15 September 2020, NCI Agency Working Paper, http://www.mindev.gov.gr/wp-content/uploads/2020/11/Enclosure-2-Working-paper-Potential-of-5G-technologies-for-military-application.pdf.

→ Bendett, Samuel, Mathieu Boulègue, Richard Connolly, Margarita Konaev, Pavel Podvig, Katarzyna Zysk. 'Advanced military technology in Russia. Capabilities and implication'. September 2021. Chatham House, https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-23-advanced-military-technology-in-russia-bendett-et-al.pdf.

→ BEREC. 'Report of BEREC Recent Activities Concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of Suppliers and Strengthening National Resilience)', BoR (20) 228, 10 December 2020, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/9726-report-of-berec-recent-activities-concerning-the-eu-5g-cybersecurity-toolbox-strategic-measures-5-and-6-diversification-of-

suppliers-and-strengthening-national-resilience.

→ Bhardwaj, Anshu. '5G for Military Communications', Third International Conference on Computing and Network Communications (CoCoNet'19), *Procedia Computer Science* 171, 2020, pp. 2665–2674, Elsevier B.V., https://doi.org/10.1016/j.procs.2020.04.289.

→ BNS/TBT Staff. 'Lithuania Holds No Direct Talks with Russia on Border Frequencies: Regulator', *Baltic Times*, 22 February 2021, https://www.baltictimes.com/lithuania_holds_no_direct_talks_with_russia_on_border_frequencies___regulator/.

→ Boswell, Jason. 'Security Considerations of Open RAN', presentation, NATO CCDCOE 5G military security workshop, Tallinn, 3–4 February 2021.

→ Boswell, Jason, and Scott Poretsky. 'Security Considerations of Open RAN', Ericsson, August 2020, https://www.ericsson.com/en/security/security-considerations-of-open-ran.

→ Bundesnetzagentur (BNetzA). 'Bundesnetzagentur Assigns 5G Spectrum from Auction', 5 September 2019, https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2019/20190904_5Gspectrum.html.

→ Bundesnetzagentur (BNetzA). 'Mobiles Breitband', https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/MobilesBreitband-node.html [accessed 20 June 2021].

→ Carnegie Mellon University and Johns Hopkins University Applied Physics Laboratory LL. 'CMCC Glossary and Acronyms: Version 1.10', 30 November 2020.

→ CISA. 'CISA 5G Strategy'. August 2020, https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf.

→ CISA. 'Overview of Risks Introduced by 5G Adoption in the United States', 31 July 2019, https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.

→ CISA. 'Potential Threat Vectors to 5G Infrastructure', May 2020, https://www.cisa.gov/publication/5g-potential-threat-vectors.

→ CISA. 'Edge vs. Core: An Increasingly Less Pronounced Distinction in 5G Networks', 2020, https://www.cisa.gov/publication/5g-edge-vs-core [accessed 22 July 2021].

→ Cisco. 'Why 5G Is Changing Our Approach to Security?' 10 June 2020, https://blogs.cisco.com/sp/5g_secure.

→ CMDRCOE. 'Crisis and Crisis Management', https://www.cmdrcoe.org/menu.php?m_id=112 [accessed 21 June 2021].

→ Common Criteria. 'Certification Report', 4 June 2020, https://www.commoncriteriaportal.org/files/epfiles/2018-60-INF-3128.pdf.

→ Common Criteria. 'Certified Products', https://www.commoncriteriaportal.org/products [accessed 15 July 2021].

→ Common Criteria. 'The Common Criteria', https://www.commoncriteriaportal.org [accessed 15 July 2021].

→ Communications Regulatory Authority of the Republic of Lithuania (RRT). 'RRT Shares the 5G Development Plans in Lithuania', 20 November 2020, https://www.rrt.lt/en/rrt-shares-the-5g-development-plans-in-lithuania/.

→ Congressional Research Service. 'National Security Implications of Fifth Generation (5G) Mobile Technologies', 4 June 2021, https://fas.org/sgp/crs/natsec/IF11251.pdf.

→ Consumer Protection and Technical Regulatory Authority. 'Avalikud konkursid ja arutelud' [Public Tenders and Discussions], https://www.ttja.ee/ariklient/ametist/avalikud-konkursid/avalikud-konkursid-ja-arutelud#avaliku-konkursi-jt [accessed 26 July 2021].

→ CSIS Working Group on Trust and Security in 5G Networks. 'Criteria for Security and Trust in Telecommunications Networks and Services', 13 May 2020, https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services.

→ Cyber Security Hub. 'Cyber Defence Simulation of Internet of Things and Mobile Networks in the Cyber Range', https://cybersecurity.cs.ut.ee/Research/CIISIM [accessed 23 June 2021].

→ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp. 1–30, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

→ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJEU L 321/36, 17 December 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1547633333762&uri=CELEX:32018L1972.

→ Doshi, Rush, Emily De La Bruyere, Nathan Picarsic, and John Ferguson. 'China as a "Cyber Great Power". Beijing's Two Voices in Telecommunication', Brookings Institution, April 2021, https://www.brookings.edu/wp-content/uploads/2021/04/FP_20210405_china_cyber_power.pdf.

→ Doshi, Rush, and Kevin McGuiness. 'Huawei Meets History, Great Powers and Telecommunications Risk, 1840–2021', Brookings Institution, March 2021, https://www.brookings.edu/wp-content/uploads/2021/03/

Huawei-meets-history-v4.pdf.

→ Dutta, Ashutosh. 'Keysight Mil-Grade 5G Panel Discussion', Johns Hopkins Applied Physics Laboratory, https://on24static.akamaized.net/event/30/73/06/3/rt/1/documents/resourceList1617988089681/ashutoshduttausecaseslides1617988088286.pdf [accessed 21 June 2021].

→ ENISA. 'Ad-Hoc Working Group on 5G Cybersecurity Certification', https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification [accessed 13 July 2021].

→ ENISA. 'Assessment of EU Telecom Security Legislation', 13 July 2021, https://www.enisa.europa.eu/publications/assessment-of-eu-telecom-security-legislation.

→ ENISA. 'Cybersecurity Certification: Candidate EUCC Scheme V1.1.1', May 2021, https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1.

→ ENISA. 'ENISA Threat Landscape for 5G Networks Report', 14 December 2020, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

→ ENISA. 'EU Cybersecurity Certification Framework', https://www.enisa.europa.eu/topics/standards/certification [accessed 13 July 2021].

→ ENISA. 'Threat Landscape for 5G Networks', 21 November 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

→ ENISA. 'Securing EU's Vision on 5G: Cybersecurity Certification', 3 February 2021, https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification/.

→ Ericsson. 'A Guide to 5G Network Security: Conceptualizing Security in Mobile Communication Networks – How Does 5G Fit In?', https://www.ericsson.com/en/security/a-guide-to-5g-network-security [accessed 20 June 2021].

→ ERR. 'Russia to Play a Big Role in Estonia's 5G Future', 10 June 2021, https://news.err.ee/1100189/russia-to-play-a-big-role-in-estonia-s-5g-future.

→ EUR-Lex. 'Frequency Bands for Electronic Communication', https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32019D0235 [accessed 21 June 2021].

→ European 5G Observatory. '5G Connected and Automated Mobility (CAM)', https://5gobservatory.eu/5g-trial/5g-connected-and-automated-mobility-cam/ [accessed 20 June 2021].

→ European 5G Observatory. 'Major European 5G Trials and Pilots: 5G Observatory', https://5gobservatory.eu/5g-trial/major-european-5g-trials-and-pilots/ [accessed 20 June 2021].

→ European 5G Observatory. 'National 5G Plans and Strategies', https://5gobservatory.eu/public-initiatives/national-5g-plans-and-strategies/ [accessed 23 June 2021].

→ European Commission. 'Connecting Europe Facility (CEF2) Digital', 21 March 2021, https://ec.europa.eu/digital-single-market/en/connecting-europe-facility-cef2-digital.

→ European Commission. '5G for Europe: An Action Plan', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2016) 588, 14 June 2016, https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2016)588.

→ European Commission. 'Commission Recommendation of 26 March 2019 on Cybersecurity of 5G Networks', C(2019) 2335 final, OJ L 88, 29 March 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019H0534.

→ European Commission. 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Secure 5G Deployment in the EU – Implementing the EU Toolbox', COM/2020/50 final, 29 January 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0050.

→ European Commission. 'Connecting Europe Facility (CEF2) Digital: Shaping Europe's Digital Future', 12 March 2021, https://ec.europa.eu/digital-single-market/en/connecting-europe-facility-cef2-digital.

→ European Commission. 'Cooperative, Connected and Automated Mobility', Mobility and Transport, https://ec.europa.eu/transport/themes/its/c-its_en [accessed 21 June 2021].

→ European Commission. 'Factsheet: The EU Toolbox for 5G Security', 8 March 2021, https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

→ European Commission. 'Report on the Impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G Networks', SWD(2020) 357 final, 16 December 2020, https://digital-strategy.ec.europa.eu/en/library/commission-reviews-impacts-eu-process-and-eu-toolbox-and-sets-out-next-steps-ensure-secure-5g.

→ European Commission. 'The EU Cybersecurity Certification Framework', https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework [accessed 13 July 2021].

→ European Commission. Proposal for a Directive of the European Parliament and of the Council on

measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823.

→ European Commission, High Representative of the Union for Foreign Affairs and Security Policy. 'The EU's Cybersecurity Strategy for the Digital Decade', Joint Communication to the European Parliament and the Council, JOIN(2020) 18 final, 16 December 2020, p. 11, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

→ European Defence Agency. '5G Technologies for Defence', White Paper, January 2021.

→ Federal Communications Commission. 'Communications Security, Reliability, and Interoperability Council VII', https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii [accessed 15 July 2021].

→ Federal Mobility Group. 'Framework to Conduct 5G Testing', November 2020, https://www.cio.gov/assets/files/Framework-to-Conduct-5G-Testing-508.pdf.

→ Federal Register. 'Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain', 15 May 2019, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

→ Fellah, Adlane. '5G Smart Sea Port: Hamburg Port Authority', Nokia, 2019, https://onestore.nokia.com/asset/206571.

→ Fildes, Nic. 'Dish Hopes to Serve up New Kind of 5G Network'. *Financial Times*, 27 June 2021. https://www.ft.com/content/5e8a7d9c-784f-44b2-be9d-fddeddea209d.

→ First Net Authority. 'The Network', https://firstnet.gov/network [accessed 21 June 2021].

→ Fouquet, Helene, and Tara Patel. 'France's Huawei Ban Begins to Kick In With Purge in Urban Areas'. Bloomberg. 1 March 2021. https://www.bloomberg.com/news/articles/2021-03-01/france-s-huawei-ban-begins-to-kick-in-with-purge-in-urban-areas?srnd=technology-vp.

→ FUDGE-5G. 'Deployable 5G Network for Public Protection and Disaster', https://fudge-5g.eu/en/use-cases/ppdr [accessed 21 June 2021].

→ Grønsund, Pål, Andres Gonzalez, Kashif Mahmood, Kennet Nomeland, Jan Pitter, Antonios Dimitriadis, Tom-Kristian Berg, and Stephen Gelardi. '5G Service and Slice Implementation for a Military Use Case'. 2020 IEEE International Conference on Communications Workshops (ICC Workshops), doi: 10.1109/ICCWorkshops49005.2020.9145236.

→ GSMA. 'NESAS Evaluated Network Equipment Products', https://www.gsma.com/security/nesas-evaluated-network-equipment-products [accessed 15 July 2021].

→ GSMA. 'NESAs FAQs', https://www.gsma.com/security/nesas-faqs/ [accessed 15 July 2021].

→ Hanselman, Eric. 'Security Benefits of Open Virtualized RAN', 451 Research, May 2020, https://www.cisco.com/c/dam/en/us/solutions/service-provider/pdfs/5g-network-architecture/white-paper-sp-open-vran-security-benefits.pdf.

→ Help Net Security. 'Worldwide 5G Connections to Reach 619 Million by the End of 2021', 1 April 2021, https://www.helpnetsecurity.com/2021/04/01/5g-connections-2021/.

→ Herr, Trey, William Loomis, Stewart Scott, and June Lee, 'Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain', Atlantic Council, 26 July 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/#attacks.

→ Homeland Security. 'National Strategy to Secure 5G', March 2020, https://www.hsdl.org/?view&did=835776.

→ Huawei. 'Huawei 5G: Passes GSMA's Network Equipment Security Assurance Scheme', 20 August 2021, https://www.huawei.com/en/news/2020/8/huawei-5g-passes-gsma-nesas.

→ Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. 'Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2020'. September 2020, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2020.

→ IEEE. 'International Network Generations Roadmap: 2021 Edition; Security and Privacy', https://futurenetworks.ieee.org/images/files/pdf/INGR_2021_Edition/IEEE_INGR_Security_2021Ed_Promo.pdf [accessed 20 June 2021].

→ ITU. 'IMT Vision: Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond; Recommendation M.2083-0 (09/2015)', 29 September 2015, https://www.itu.int/rec/R-REC-M.2083-0-201509-I/en.

→ Kania, Elsa B. 'Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy', 7 November 2019, Center for a New American Security, https://www.cnas.org/publications/reports/securing-our-5g-future.

→ Komitet Rady Ministrów do spraw Cyfryzacji. 'Projekt ustawy o zmianie ustawy o krajowym

systemie cyberbezpieczeństwa oraz ustawy Prawo telekomunikacyjne', January 2021, https://www.gov.pl/web/krmc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-telekomunikacyjne.

→ Könen, Andreas. 'Cyber Week', 20 July 2021, Tel Aviv University, https://cw2021.b2b-wizard.com/expo/agenda.

→ Krick, Kelly. Presentation at the NATO CCDCOE, 5G Supply Chain and Network Security Workshop, 9 June 2021.

→ LRT. 'Lithuania Bans "Unreliable" Technologies from Its 5G Network', LRT English, 25 May 2021, https://www.lrt.lt/en/news-in-english/19/1417429/lithuania-bans-unreliable-technologies-from-its-5g-network.

→ Medin, Milo, and Gilman Loui. 'The 5G Ecosystem: Risks and Opportunities for DoD', Defense Innovation Board, 3 April 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

→ Ministry of Digital Affairs. '5G – współpraca państw bałtyckich', 21 September 2020, https://www.gov.pl/web/cyfryzacja/5g--wspolpraca-panstw-baltyckich.

→ Msnet. 'Pracodawcy RP: Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa to dalsze opóźnienia we wdrażaniu sieci 5G', Telepolis, 9 February 2021, https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/pracodawcy-rp-ustawa-o-krajowym-cyberbezpieczenstwie-opoznienia-5g.

→ Nair, Pramod. Presentation at the NATO CCCDCOE meeting, May 2021.

→ National Security Commission on Artificial Intelligence. 'Final Report', 22 April 2021, https://www.nscai.gov/2021-final-report/.

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

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

→ NATO. 'New Focus on Emerging and Disruptive Technologies Helps Prepare NATO for the Future', 3 March 2021, https://www.nato.int/cps/en/natohq/news_181901.htm.

→ NATO. 'Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise', 19 July 2021, https://www.nato.int/cps/en/natohq/news_185863.htm.

→ NATO ACT. 'NATO Warfighting Capstone Concept', https://www.act.nato.int/nwcc [accessed 22 July 2021].

→ NATO STO. '5G Technologies Application to NATO Operations', https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16937 [accessed 22 June 2021].

→ NCIA. 'Multinational Collaboration of 5G', http://www.mindev.gov.gr/wp-content/uploads/2020/11/Enclosure-3-Leaflet-Multinational-Collaboration-on-5G.pdf [accessed 8 July 2021].

→ Nikers, Olevs. '5G Technologies in Latvia Advance Military Capabilities and National Economy', *Eurasia Daily Monitor* 17, no. 178, 15 December 2020, https://jamestown.org/program/5g-technologies-in-latvia-advance-military-capabilities-and-national-economy/.

→ NIS Cooperation Group. 'Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures', January 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

→ NIS Cooperation Group. 'EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks', 9 October 2019, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

→ NIS Cooperation Group. 'Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity', July 2020, https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

→ NIST. 'Cyber Supply Chain Risk Management Practices for Systems and Organizations: Draft NIST Special Publication 800-161, Revision 1', https://doi.org/10.6028/NIST.SP.800-161r1-draft [accessed 22 July 2021].

→ NIST. 'Executive Order 14028: Improving the Nation's Cybersecurity Fact Sheet', https://www.nist.gov/system/files/documents/2021/07/13/EO%20Fact%20Sheet%20July%202021.pdf [accessed 25 July 2021].

→ NIST. 'Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy', NIST Special Publication 800–37, revision 2, December 2018, https://csrc.nist.gov/Projects/risk-management/publications.

→ NIST. 'Special Publication 800–207: Zero Trust Architecture', August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

→ NTIA. 'Appendix I: Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force (TF) Threat Evaluation Working Group; Threat Scenarios', February 2020, https://www.ntia.gov/files/ntia/publications/5g_ip_appendices_1-5.pdf.

→ NTIA. 'National Strategy to Secure 5G Implementation Plan', 19 January 2021, https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf.

→ Official Internet Portal of Legal Information. 'Указ Президента Российской Федерации от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации"' [Decree of the President of the Russian Federation of 02 July 2021 No. 400 'On the National Security Strategy of the Russian Federation'], Russia, 3 July 2021, http://publication.pravo.gov.ru/Document/View/0001202107030001.

→ OSullivan, Máirín. '5G Network Slicing Vulnerability: Location Tracking Attacks', 27 April 2021, https://www.adaptivemobile.com/blog/5g-network-slicing-vulnerability-location-tracking-attacks.

→ Parliament of Germany. 'Gesetz zur Erhöhung der IT-Sicherheit mit Koalitionsmehrheit beschlossen' [Law to Increase IT Security Passed by a Coalition Majority], https://www.bundestag.de/dokumente/textarchiv/2021/kw16-de-sicherheit-informationstechnischer-systeme-834878 [accessed 26 July 2021].

→ Prague 5G Security Conference. 'The Prague Proposals: The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World', 3 May 2019, https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.

→ Pujol, Frédéric, Carole Manero, Basile Carle, and Santiago Remis. '5G Observatory Quarterly Report 11 Up to March 2021', European Commission, April 2021, http://5gobservatory.eu/wp-content/uploads/2021/04/90013-5G-Observatory-Quarterly-report-11-2.pdf.

→ Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, as amended, OJ L 79I , 21.3.2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0452.

→ Reuters. 'Telia to Remove All Huawei Equipment in Lithuania', Reuters, 30 November 2020, https://www.reuters.com/article/huawei-lithuania-idUSL8N2IG2RY.

→ Riigi Teataja [State Courier]. Electronic Communications Act, § 11 subsection 41, 87 subsection 21 and 22, https://www.riigiteataja.ee/en/eli/517122020006/consolide.

→ Riigikogu. Estonia's Electronic Communications Act, RT I 2004, 87, 593, 8 December 2004, §§ 11–16, https://www.riigiteataja.ee/en/eli/517122020006/consolide.

→ Rubin, Alex, Alan Omar Loera Martinez, Jake Dow, and Anna Puglisi. 'The Huawei Moment', CSET Policy Brief, July 2021, https://doi.org/10.51593/20200079.

→ Society of Automotive Engineers International. 'Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_201806', 15 June 2018, https://www.sae.org/standards/content/j3016_201806/.

→ Speedtest. 'Ookla 5G Map', https://www.speedtest.net/ookla-5g-map [accessed 23 July 2021].

→ Spiegel. 'Bundestag beschließt Hürden-für-Huawei-Gesetz' [Bundestag Passes Hurdles for Huawei Law], 23 April 2021, https://www.spiegel.de/netzwelt/netzpolitik/it-sicherheitsgesetz-2-0-bundestag-beschliesst-huerden-fuer-huawei-gesetz-a-2f50a7dc-e5f5-4b35-ba30-1ecbf1db4eed.

→ StandConsult. 'Does Huawei Not Believe in Open RAN? Or Is Just Playing Poker with the O-RAN Alliance and Policymakers?' 23 March 2021, https://strandconsult.dk/does-huawei-not-believe-in-open-ran-or-is-just-playing-poker-with-the-o-ran-alliance-and-policymakers/.

→ Tauriņš, Andris, Gunvaldis Leitens, and Lūcija Strauta. 'The Technology, Media and Telecommunications Review: Latvia', *Law Reviews*, 3 February 2021, https://thelawreviews.co.uk/title/the-technology-media-and-telecommunications-review/latvia.

→ Three Seas. 'Projects: 5G Cross Border Transport Corridors for Connected and Automated Mobility (CAM) in Baltics (Via-Baltica/Rail-Baltica)'. https://projects.3seas.eu/projects/5g-cross-border-transport-corridors-for-connected-and-automated-mobility-(cam)-in-baltics-(via-balticarail-baltica)-submitted-by-lithuania [accessed 20 June 2021].

→ Tooming, Marko. 'Valitsus lükkas sidevõrkude turvalisuse määruse vastuvõtmise edasi' [The Government Postponed the Adoption of the Regulation on Communications Network Security], ERR, 3 April 2021, https://www.err.ee/1608130453/valitsus-lukkas-sidevorkude-turvalisuse-maaruse-vastuvotmise-edasi.

→ US Department of Defense. 'Department of Defense 5G Strategy Implementation Plan', 15 December 2020, https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf.

→ US Department of Defense. 'Department of Defense 5G Strategy', 2 May 2020, https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf.

→ US Department of Defense. 'DoD Names Seven Installations as Sites for Second Round of 5G Technology Testing, Experimentation'. 3 June 2020. https://www.defense.gov/Newsroom/Releases/Release/Article/2206761/dod-names-seven-installations-as-sites-for-second-round-of-5g-technology-testin/.

→ Wenger, Eric. ‘Are Openness and Security Both Possible in a 5G World?’ 28 January 2021, https://blogs.cisco.com/gov/are-openness-and-security-both-possible-in-a-5g-world.

→ White House. ‘Executive Order on America’s Supply Chains’, 24 February 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains.