CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Tallinn 2022

RESEARCH REPORT

Military Movement: Risks from 5G Networks

CCDCOE

About the authors

This document is based on four unpublished individual reports (see Introduction) which have been compiled into one holistic document by a dedicated task force. The task force was led by Civitta Estonia. The Civitta Estonia team was composed of Veeli Oeselg, Rokas Šalaševičius, Hendrik Ploom and Andreas Palm, and assisted by external experts Alar Kuusik, Tony Lawrence and Kadri Peeters.

Acknowledgements

The authors would like to thank the creators of the four base documents from Ericsson, TalTech, Nokia, and the International Centre for Defence and Security Estonia

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 CCDCOE is a diverse group of international experts from military, government, academia, and industry, currently representing 35 sponsoring and contributing nations.

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.

The Centre is staffed and financed by Austria, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Montenegro, North Macedonia, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States.

The CCDCOE produces the *Tallinn Manual*, the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields gives cybersecurity 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 from 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

This publication is a product of the CCDCOE. It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purposes, provided that copies bear a full citation.

Table of Contents

Abbreviations

MILITARY-RELATED

21st TSC	21st Theater Sustainment Command
BCT	Brigade Combat Team
CIS	Communications and information system
COM JTF	Commander of Joint Task Force
ESS	Enablement Support Services
GCSS-Army	Global Combat Systems Support-Army
HETs	Heavy Equipment Transporters
RO/RO	Roll on/Roll off vehicle transportation ferry
RSOMI	Reception, Staging, Onward Movement, and Integration
SACEUR	Supreme Allied Commander Europe
SDDC	Military Surface Deployment and Distribution Command
VITAL	Visibility in Transit Asset Logging
VJTF	Very High Readiness Joint Task Force

5G-RELATED

3GPP	3rd Generation Partnership Project
5G NR	5G New Radio
AES	Advanced Encryption Standard
AGVs	Automatic Guided Vehicles
APN	Access Point Name
AV	Autonomous Vehicle
CN	Core Network
CNF	Cloud-Native Functions
C-V2X	Cellular Vehicle to Everything
D2D	Device-to-Device communication
DoS	Denial-of-Service
DSRC	Dedicated Short-Range Communication
EAP	Extensible Authentication Protocol
eMBB	Enhanced Mobile Broadband
eNBs	LTE base stations
FDD	Frequency Division Duplexing
gNBs	5G New Radio base stations
GNSS	Global Navigation Satellite System
GSMA	Global System for Mobile Communications
HV	Head Vehicle
IAB	Integrated Access Backhaul
IETF	Internet Engineering Task Force
IMT	International Mobile Telecommunications
IMSI	International Mobile Subscriber Identifier
IoT	Internet of Things
IPSec	Internet Protocol Security
ITS	Intelligent Transport System
LPWA	Low-Power Wide-Area Networks
LTE	Long Term Evolution
M2M	Machine-to-Machine communication
MCC	Mobile Cloud Computing
MEC	Multi-access Edge Computing
MIMO	Multiple Input and Multiple Output
mMTC	Massive Machine-Type Communications

mmWave	Millimetre Wave – band of spectrum between 30 GHz and 300 GHz
MNO	Mobile Network Operator
MOC	Multi-Operator Core
MVNO	Mobile Virtual Network Operator
NESAS	Network Equipment Security Assurance Scheme framework
NIST	National Institute of Standards and Technology
NPN	Non-Public Network
OFDM	Orthogonal Frequency Division Multiplexing
ORAN	Open Radio Access Network
PC5	Cellular sidelink based device-to-device communication
PMR	Professional Mobile Radio
ProSe	Proximity Services
QoS	Quality of Service
RAN	Radio Access Network
RSU	Roadside Unit
SNPN	Standalone Non-Public Network
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege
TDD	Time Division Duplexing
TOS	Terminal Operations System
TLS	Transport Layer Security
UE	User Equipment
UHF	Ultra-High Frequency
URLLC	Ultra-reliable low-latency communication
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VHF	Very High Frequency
VNF	Virtualised Network Functions
VRU	Vulnerable Road User
WSN	Wireless Sensor Networks

1. Introduction

In 2020, the United States and Estonia assigned the The NATO Cooperative Cyber Defence Centre of Excellence to conduct a two-year project on 5G supply chain and network security related to the new generation telecommunication infrastructure to address the strategic, legal, and policy issues for NATO Allies and close partners. The aim of the project is to study different aspects of telecommunications networks' supply chain security, support relevant research and outline recommendations for the Alliance. CCDCOE, subsequently, published a Research Report on Supply Chain and Network Security for Military 5G Networks in 2021. This second report focuses on practical aspects of 5G Networks in the context of military movement and is a follow-up to the first study, using two case studies of Smart Seaport and C-V2X Supported Road Transportation.

For this second report, CCDCOE received four unpublished reports by:

- TalTech – Supply chain and cybersecurity challenges to C-V2X technology. Authors: Toomas Ruuben, Alar Kuusik, Alejandro Guerra Manzanares, Ivo Müürsepp, Urmas Ruuto;
- Ericsson – Cybersecurity in 5G enabled Smart Sea Ports. Authors: Per Ljungberg, Dr Thouraya Toukabri, Dag Åberg, Bodil Josefsson, Dr Harri Pietilä;
- Nokia – Smart Port Security. Author: Ian Oliver;
- International Centre for Defence and Security (ICDS)– From the North Sea to the Baltic: A Military Movement Scenario. Authors: Tony Lawrence, Martin Hurt.

Emergence of new technologies creates significant benefits and potential use cases for many industries, while also being a tool in the domain of great power competition. To this end, telecommunications and communication technologies have been used by states large and small for political and military advantage – sometimes bringing a measure of parity and balance among competitors of differing size and relative power. The 5G cellular communication roll-out is happening on gradual and continuing basis requiring military, intelligence services, and the private sector to continually adjust to avoid any potential disadvantage. 5G technology, however, also brings numerous new solutions and applications to the military sector. With the continuous technological development, even without developing 5G solutions for the military itself, new risks and threats arise. Due to the rapid development of civil technologies and the military's dependency on civil solutions, e.g., for military movement, 5G will inevitably reach the military and affect day-to-day operations. Therefore, all relevant parties involved need to be ready to address both the opportunities and risks that will arise with 5G. With the new rising risks and threats, network security aspects need to be considered and addressed today to eliminate potential threats in the future, especially for the militaries of NATO Allies and close partners. Thus, both network opportunities and risks need to be evaluated from a technical point of view to understand the impact for the military while moving equipment and supplies across NATO countries. To achieve functional NATO awareness, use cases will serve as a foundation for recommendations to policy makers in this arena.

The report examines network security challenges associated with 5G connectivity technology in a military movement scenario in 2030 using smart ports and smart roads as the case studies. The report aims to raise awareness on how operating through public and private 5G networks can impact NATO's collective defence during peacetime and thereby provide decision makers evidence-based information on possible challenges associated with 5G networks.

The report introduces a future looking storyline on military movements in the Baltic region in 2030. It then provides a description of two 5G use cases, i.e.

smart seaports and smart roads, that could be used in 2030 to move military equipment and supplies for NATO’s collective defence purposes. Based on a 5G implementation related risk and threat analysis, the report highlights key cybersecurity risks and challenges that the military may face using private and public networks. Finally, the report formulates a set of recommendations for allied and/or NATO policymakers to consider when developing 5G infrastructure and making network-related policies and decisions.

2. Military Movement 2030

2.1 Establishing the Scenario

The underlying scenario under consideration takes place in **2030**. Europe's security considerations continue to be dominated by the fallout from Russia's large-scale invasion of Ukraine, which began eight years earlier. Russia's armed forces were badly bloodied in the war, but it has used the intervening period to rebuild much of its military strength. Relations between the West and an isolated Russia are tense and Russia bitterly nurses grudges against the West and remains gripped by a conviction that Europe's security order must be recast in its favour. In addition, and despite Western efforts from the beginning of the 2020s, China has acquired enough critical technologies to challenge Western economic and national security interests and aims to strengthen its influence over Russia as a continuation of its block building policy. **Russia and its client state, Belarus**, **begin to assemble large numbers of military units at multiple locations close to their borders with Lithuania, Latvia, and Estonia**. The Russian president demands that the West take Russia's demands seriously or face unprecedented consequences.

Recognising a **growing threat to NATO territory** and determined not to be taken off guard, ambassadors to the North Atlantic Council, NATO's most senior decision-making body, agree to **military reinforcement of the Baltic region**. As an immediate step, they task the Supreme Allied Commander Europe (SACEUR) to deploy the Very High Readiness Joint Task Force (VJTF) to Latvia and to activate the rest of the NATO Response Force.[1] The US, meanwhile, orders the 82nd Airborne Division's global response force, a light airborne brigade, to the region and begins to deploy forward other units based in Poland, Germany, and Italy. To backfill the Armored Brigade Combat Team (BCT) based in Żagań, Poland, which is now moving to Lithuania, the US also orders the 1st Armored (BCT) of the 1st Infantry Division, based in Fort Riley, Kansas, to Poland. At the same time French, German and UK brigade-sized forces are ordered to the region, as are smaller units from most NATO states. The UK brigade will reinforce the UK's permanent presence in Estonia.

2.1.1 Requirements and Features of Military Movement

While the above describes **peacetime moves**, the international circumstances require the deploying armed forces to adopt practices more typically associated with crisis-time movement. To ensure effective deterrence and, if necessary, defence of NATO territory, these military movements **must be conducted at speed**.[2] Security considerations are also more prominent than they would be for regular peacetime movement such as the rotation of a contingent of NATO's multinational presence in the Baltic region. The moving units will need to **consider extra physical and cybersecurity precautions**. At the same time, however, Europe still being in peacetime, has not put in place the necessary emergency measures to prioritise military movement in case of a crisis. The deploying armed forces must **compete both with each other, and with civilian users of transport infrastructure and services**. Consequently, five relevant features of military movement can be underlined.

[1] The 40,000-strong NATO Response Force is the Alliance's main rapid reaction capability. The VJTF is the spearhead of the force and is NATO's highest-readiness element. Constantine Atlamazoglou, 'The NATO rapid-response unit created after Russia's 2014 invasion of Ukraine is being activated for first-of-its-kind mission', *Business Insider* (2 March 2022), https://www.businessinsider.com/nato-response-force-vjtf-first-defense-mission-russia-ukraine-2022-3.

[2] Heinrich Brauss, Ben Hodges, and Julian Lindley-French, *Moving Mountains for Europe's Defense* (Washington DC: CEPA, 2021), 18.

RESPONSIBILITY | According to NATO doctrine, **deployment is primarily a national responsibility**.[3] When units deploy abroad, individual member states are responsible for making the arrangements to ensure personnel, along with their vehicles, equipment, and supplies, assemble in designated locations ready to carry out military operations. At this point, they will be transferred from national to NATO command. In many cases, however, especially for smaller nations, movement will be planned and implemented by a larger partner nation, or other cooperative multinational solutions will be sought. NATO encourages this to ensure the maximum efficiency and effectiveness of the process and to assist to prioritise and deconflict movements.[4]

COMPLEXITY | The process of transforming deploying forces into forces capable of meeting the commander's operational requirements is known as **Reception, Staging, Onward Movement, and Integration** (RSOMI).[5] Military personnel, vehicles, equipment, and supplies usually travel from different destinations by different methods and routes – RSOMI is the **process which ensures all the pieces come together in the right place**, at the right time. RSOMI is a **complex process**, affected by factors such as the number of personnel, number and type of vehicles, structure of the organisation, location of departure, mode of reception (ground, sea, rail, or air), size of the advance party, level of coordination with the deploying element unit movement team, capabilities of the host nation, and others.[6] The loads to be moved – an important source of complexity – are broadly categorised into **personnel, vehicles, and containerised loads**.

→ **Personnel (and their personal equipment)** are typically deployed separately from their vehicles, equipment, and supplies, by military or civilian charter aircraft for strategic movement, and by a variety of means for operational movement.

→ **Vehicles can be divided into two categories:** (1) **Tracked and other heavy vehicles** cannot move independently on civilian road networks and must be transported on flat-bed rail cars, barges, or heavy equipment transporters (HETs). Their physical size and weight will make them unable to use certain road routes.[7] This is a problem especially in eastern Europe, where older roads were built to handle lighter Warsaw Pact equipment and newer roads have not always taken military requirements into account; in Poland, for example, many bridges are rated at only 50 or 60 tonnes.[8] (2) **Lighter vehicles**, such as soft-skinned lorries and utility vehicles, usually move under their own power, often in convoy at night.

→ **Containerised loads** in the form of **standard shipping containers** are used to transport almost all equipment and supplies. Equipment refers to items that are not consumed, such as weapon systems, communication systems, tools, and accommodation. Supplies refers to consumable items. Containers may be owned or leased by military organisations. They can be moved using a variety of road vehicles and rail rolling stock.

[3] NATO, 'Allied Joint Doctrine for the Conduct of Operations', AJP-3, Edition C, Version 1, November 2019, 2–11.

[4] NATO, 'Allied Joint Doctrine for the Deployment and Redeployment of Forces', AJP-3.13, Edition A, Version 1, May 2021, 1–2, https://usacac.army.mil/organizations/mccoe/call/publication/18-05.

[5] NATO, 'Allied Joint Doctrine for the Conduct of Operations', 2–12.

[6] Center for Army Lessons Learned (US), 'Special Study: Strategic Landpower in Europe. Special Study', no. 18-05, December 2017, 67, https://usacac.army.mil/organizations/mccoe/call/publication/18-05.

[7] An M1 Abrams tank fitted with an active protection system weighs around 68 tonnes, while a HET/trailer weighs as much as an additional 41 tonnes.

[8] Sydney J. Freedberg Jr, 'OMFV: The Army's Polish Bridge Problem', *Breaking Defense*, 6 February 2020, https://breakingdefense.com/2020/02/omfv-the-armys-polish-bridge-problem/.

COORDINATION | In a crisis, many units and their equipment may be moving at the same time towards the same locations and **competing for the same transportation resources**. While deployment is a national responsibility, NATO has organisations at various levels responsible for planning, prioritising, and deconflicting movements. The Allied Movement Coordination Centre deals with strategic movements (i.e. from home bases to operational theatres), while Joint Logistic Support Groups deal with various stages of operational movements (e.g. in the operation's rear area or in the operational area itself).[9] NATO Force Integration Units support the deployment of NATO's rapid reaction forces to Poland, the three Baltic states, and several other countries while each ally is required by NATO to have a National Movement Coordination Centre approve, coordinate, and control movements in their own territories.[10] Separately, the US Army, which by virtue of size and distance is likely to have the most stressing movement requirements, also maintains various organisations responsible for supporting military movement. The Military Surface Deployment and Distribution Command (SDDC) supports international movements[11] and the 21st Theater Sustainment Command (21st TSC) headquartered in Kaiserslautern, Germany, is tasked with sustaining US Army Europe and Africa forces, including all aspects of RSOMI.[12]

This **abundance of organisations with overlapping responsibilities adds to the complexity of military movement**. The challenge of moving armed forces of any significant size across Europe is exacerbated by the fact that large-scale deployments have been little exercised since the end of the Cold War.[13] Perhaps unsurprisingly, there is no clear picture, even amongst movement specialists of how the various actors will work together in a crisis to ensure an efficient RSOMI.[14] In practice, large-scale military movement is likely to involve a great deal of confusion, problem solving, ad hoc planning, and improvisation.

CONTRACTORISATION | Except for military airbases and some port facilities, **armed forces mostly use civilian-owned infrastructure, equipment, and services for military movement**. They will rely upon civilian airports and seaports, rail and road networks, and the services these facilities provide (e.g. cargo handling and storage). Also, it is not cost-effective for armed forces to own large quantities of the equipment necessary to support military movement. This dynamic means that smart ports and transportation infrastructure to be used for military movements are developed for civil use. Cargo and roll on/roll off (RO/RO) vessels, flat-bed rail cars able to transport heavy or tracked vehicles, HETs to move such vehicles on the roads, inland waterway barges, and their operators, are often provided through contracts with commercial

[9] Curtis M. Scaparrotti and Colleen B. Bell. *Moving Out. A Comprehensive Assessment of European Military Mobility* (Washington DC: The Atlantic Council, 2020), 12; Aaron Cornett. 'Multinational Operations. JLSG offers effective role with allies, partners', US Army, 16 January 2020, https://www.army.mil/article/231676/multinational_operations_jlsg_offers_effective_role_with_allies_partners.

[10] NATO, SHAPE, 'NATO Force Integration Units (NFIU)', accessed 27 April 2022, https://shape.nato.int/operations/nato-force-integration-units; NATO, 'Allied Joint Movement and Transportation Doctrine', AJP- 4.4, Edition B, Version 1, May 2013, 7–1.

[11] US Army, 'United States Army Military Surface Deployment and Distribution Command', accessed 19 April 2022, https://www.sddc.army.mil/Pages/default.aspx.

[12] US Army, '21st Theater Sustainment Command', accessed 19 April 2022, https://www.21tsc.army.mil/.

[13] During the Cold War, regular exercises such as the Reforger series saw tens of thousands of troops deploy to and move across Europe. In 2018, NATO rehearsed reinforcement for collective defence for the first time in many years in the exercise Trident Juncture. The US-led series of reinforcement exercises, Defender, began in 2020 and will take place annually.

[14] Ben Hodges, Tony Lawrence, and Ray Wojcik. *Until Something Moves. Reinforcing the Baltic Region in Crisis and War* (Tallinn: ICDS, 2020), 20.

organisations. Commercial organisations **rarely reserve these assets for military use and the military, a small customer of their services, must compete with civilian customers for access**.

REGULATIONS | Armed forces require special advance permissions to enter other territories and move along specified routes. In some cases, national authorities must also coordinate with regional authorities (e.g. the German federal states) whose requirements may differ. For some deploying nations, there will be customs requirements. While many procedures have been harmonised across the EU, they still impose a heavy bureaucratic load on deploying forces – a land move from Antwerp to Tallinn will cross five international borders and require the deploying nation to deal with six national authorities. In each of these, deploying forces will encounter different levels of support from the transit nation, different requirements for escort, different sophistication of technology and so on.[15]

[15] 'Transit nation' is the nation across whose territory the deploying force is moving.

2.2 Movement Channels

NATO forces will move to assembly areas in their destination countries by a variety of routes, which depend on factors such as contingency plans and usual national practice, availability of transportation assets, availability of military personnel with specialist skills and qualifications (e.g. rail head control operations), and existing contractual arrangements with service providers. In a large-scale military deployment, movement can be categorised as **strategic** (by air and by sea) and **operational** (by rail and by road). Transatlantic air and sea crossings as well as the air and sea crossings from the UK will generally be considered strategic movements, while all movement in continental Europe – the theatre of operations – will usually be considered operational movement. A selection of these movements is described below to illustrate some of the requirements for and challenges of the scenario.

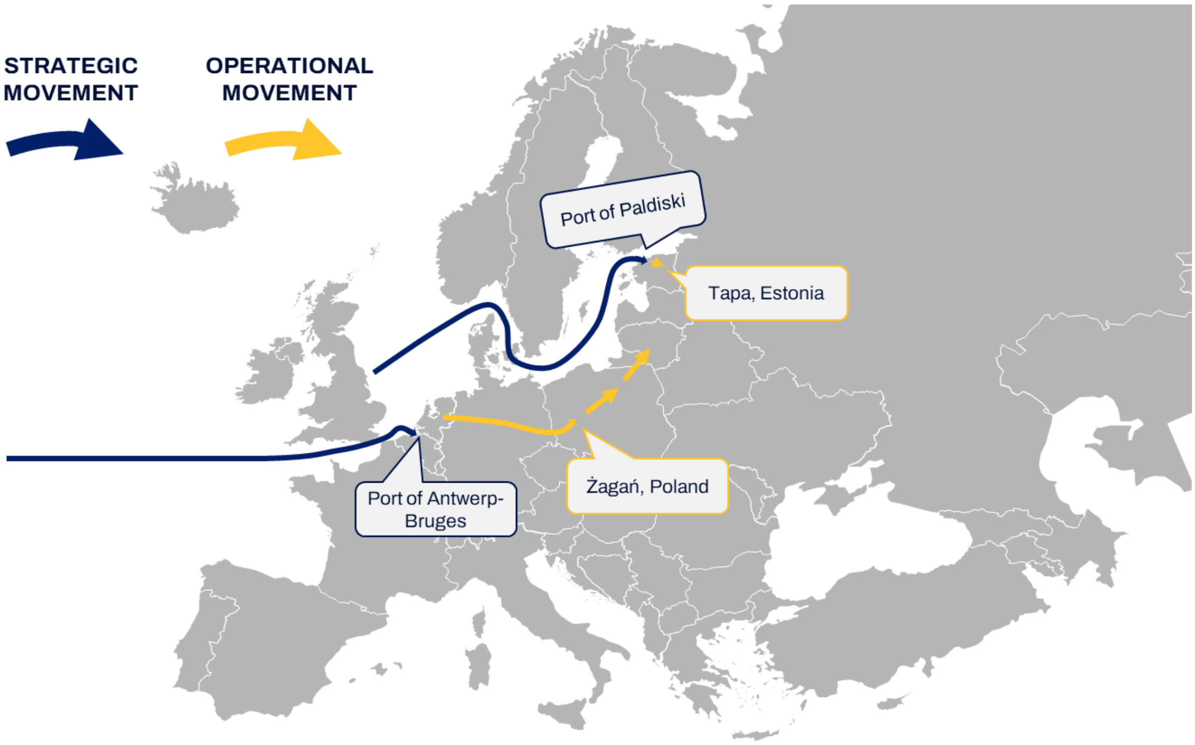


FIGURE 1. STRATEGIC AND OPERATIONAL MOVEMENT SCENARIOS

2.2.1 Strategic Movement

Most units will use their own vehicles, equipment, and supplies during the period of their deployment. These will need to be **transported from home bases to the assembly areas** by a combination of sea, rail, and road. Some US units, however, arrive in Europe by air to be linked up with vehicles, equipment, and other supplies drawn from US prepositioned stocks, for example, those stored at Coleman Barracks, Mannheim, Germany. This simplifies the strategic movement leg of deployment.

Movement by Air

Most personnel will be deployed by air, using either military transport aircraft or civilian charter aircraft. Personnel arriving by air will also travel with small amounts of personal equipment (e.g. clothing, food rations, personal weapons, and support weapons). This will be loaded onto standard military 463L pallets or civilian unit load devices, both of which will require handling services on arrival.[16] These services may be military or civilian contractors depending on the airport of debarkation. Both personnel and personal equipment will then require transportation, most likely by road, to staging or assembly areas.

Movement by Sea

In this scenario, the international situation is tense, but risks to shipping in the Baltic Sea are considered relatively low, and manageable with increased NATO naval presence on the Baltic Sea. This allows **some heavy and light vehicles and containerised goods** – principally those from the US and the UK, for whom sea transport is unavoidable – to be transported by RO/RO vessels directly to certain Baltic ports such as Klaipėda, Ventspils, and Paldiski. Other vehicles and containerised goods will arrive at several of Europe's North Sea ports, such as Antwerp or Bremerhaven.

1st ARMORED BCT (US) | The 1st Armored BCT will transport 3,000 pieces of equipment by sea to the Port of Antwerp, including 1,500 wheeled and 500 tracked vehicles, requiring four contracted cargo vessels.[17] This is a large number for military movement but still represents a tiny fraction of the vehicles handled by the port each year.[18] Most of the BCT's 3,500 personnel will travel separately by air and rendezvous with their vehicles and equipment. Heavy vehicles and equipment will be transported to their final destination by a variety of means, accompanied by small numbers of BCT personnel. The BCT will also detach personnel to Antwerp to receive most of the wheeled vehicles and drive them to Żagań. **The unloading of equipment in the Port of Antwerp and consequent road movement to Żagań will be relevant later as these two steps in the movement scenario act as a unifying thread throughout this report.**

Logistics troops from the SDDC and 21st TSC and their contractors will unload vehicles, oversee the unloading of containerised equipment and supplies, coordinate clearance procedures with local customs officers, and ready cargo for onward movement. While some heavy vehicles can be moved by rail, the limited capacity of the rail networks and the waiting time for rail cars will dictate that most movement will take place on Europe's already congested roads.[19] Other heavy vehicles will be loaded onto barges to travel by inland waterways to a rail head closer to their final destination.

Vehicles, equipment, and supplies will be checked, and records updated on the Global Combat Systems Support-Army (GCSS-Army, a US-national, automated, web-based, logistics and finance system).[20] To process and move onwards all the

[16] 'Military Pallets, Boxes and Containers – Part 6 Aircraft Pallets and Containers', Think Defence, 23 November 2014, https://www.thinkdefence.co.uk/2014/11/military-pallets-boxes-containers-part-6-aircraft-pallets-containers/.

[17] Benjamin Northcutt, '1st Armored Brigade Combat Team arrives in Europe in support of Atlantic Resolve', *Sealift*, March 2019, 3, https://issuu.com/militarysealiftcommand/docs/march_2019_sealift_issue_3_v2; 'Atlantic Resolve', US Army Europe and Africa Infographic, July 2021, https://www.europeafrica.army.mil/Portals/19/documents/Fact%20Sheets/AtlanticResolveInfographic.21.11.30.pdf?ver=zs-ekCq7l9DkTyTn-AIlkw%3d%3d. Parts of this scenario are based on a useful description of the 2019 move of this unit from Fort Riley to Żagań, Poland, in Eva Hagström Frisell (ed.), Robert Dalsjö, Jakob Gustafsson, and John Rydqvist, *Deterrence by Reinforcement: The Strengths and Weaknesses of NATO's Evolving Defence Strategy* (Stockholm: FoI, 2019), 38–44.

[18] Antwerp handled 902,477 vehicles (an average of more than 2,400 per day) in 2020, as well as more than 12 million twenty-foot equivalent (6.1 meters) unit containers (almost 33,000 per day). '2021 Facts and Figures', Port of Antwerp, 19, 13, https://www.portofantwerp.com/en/publications/brochures/facts-and-figures-2021.

[19] Hodges, Lawrence, and Wojcik, *Until Something Moves*, 16; Milda Vilikanskytė, 'Ekspertai: geležinkeliai karo metu – nepakeičiami, bet Lietuvos pajėgumai riboti [Experts: Railways are irreplaceable during war, but Lithuania's capabilities are limited]', LRT, 23 April 2022, https://www.lrt.lt/naujienos/eismas/7/1677306/ekspertai-gelezinkeliai-karo-metu-nepakeiciami-bet-lietuvos-pajegumai-riboti.

[20] Northrop Grumman, 'Global Combat Systems Support-Army (GCSS-Army)', https://www.northropgrumman.com/what-we-do/land/gcss-army/. Other Allies use the NATO-developed Logistics Functional Services (LOG FS) suite of tools.

vehicles, equipment and supplies will take several days, during which physical security will be provided by the Port of Antwerp, supplemented by Belgian military personnel.

12 ARMOURED BCT (UK) | The UK, meanwhile, will deploy the 12 Armoured BCT, a unit of 3 (UK) Division, to reinforce its presence in Estonia.[21] The BCT's vehicles, equipment, and supplies will mostly be transported by RO/RO to Paldiski, from where they will move by rail and road to Tapa. Because of the unusually large amounts of cargo to be moved – a BCT will bring more than 1,000 containers of equipment and supplies – one vessel will unload at the port of Muuga. The RO/ROs will be unloaded by stevedores under commercial contract and by military vehicle specialists and cargo handlers. This well-rehearsed operation can be completed in a few hours, but it will take several days for all the vehicles, equipment, and supplies to be transported on to Tapa. Physical security again will be provided by the ports and the local defence forces.

Consignment tracking for UK movements will be carried out using the, by now dated, visibility in transit asset logging (VITAL) system.[22] This is a cellular connectivity enabled system that uses a combination of barcode and radio frequency identification reader inputs to update the status of consignments at supply chain nodes. It is not connected to any commercial network but operates over a secure satellite link.

2.2.2 Operational Movement

Most Allies, whose home bases are located in the operation's rear and forward areas, need to deal only with operational movement. Even so, operational movement – from either port of debarkation for vehicles and equipment arriving by sea or, for units based in Europe, from home bases to destinations in the Baltic states – is **a multi-dimensional logistical challenge**. Relevant factors include the availability of rail cars and HETs, the readiness of escorts, the quality of the transport network, and a desire to spread movement across routes, both to avoid choke points and vulnerabilities and to minimise disruption to civilian movement. Therefore, **vehicles and containerised equipment will be spread across many routes** for periods of time measured in weeks.

The degree to which these factors will help or hinder deploying forces will vary from transit nation to transit nation. NATO does, however, attempt to ensure basic standards are in place through its seven baseline requirements for national resilience, which include requirements for resilient civil communications systems and resilient transport systems.[23]

Movement by Rail

In 2030, Germany will be the lead nation for NATO's VJTF, providing NATO's most rapid reaction capability with around 5,000 ground forces personnel, plus land, sea, and special forces elements, required to be ready to operate in two to three days. Deployment will be arranged to Latvia where the heavier elements of the 37 Armoured Infantry Brigade would be moved from Veitshöchheim, Bavaria by six trains.[24] This move will be made much easier by the recent completion of the long-delayed Rail Baltica project, which removes a notorious bottleneck from the North

[21] UK Army, '3 (UK) Division. 12 Armoured Brigade Combat Team', accessed 22 April 2022, https://www.army.mod.uk/future-army/unit-details/3-uk-division/12-armoured-brigade-combat-team/.

[22] UK Ministry of Defence, 'JSP886 Defence Logistic Support Chain Manual. Volume 3: Supply Chain Management. Part 7. Consignment Tracking', [archived] 38–40.

[23] NATO, 'Resilience and Article 3', 11 June 2021, https://www.nato.int/cps/en/natohq/topics_132722.htm.

[24] Bundeswehr, '10 Armoured Division', accessed 20 April 2022, https://www.bundeswehr.de/en/organization/army/organization/10-armoured-division.

Sea–Baltic corridor.[25] The difference in rail gauge between Poland and the Baltic states had previously required vehicles to be transferred from one train to another just north of the Polish–Lithuanian border.[26]

While many of the VJTF's vehicles and equipment can travel by rail as far as Riga, thereafter they will be transported by road to their assembly area close to Latvia's eastern border. Germany's permanent forward presence in the Baltic region is in Rukla, Lithuania, where it has over the years established infrastructure (e.g. bulk fuel storage), equipment (e.g. military HETs), and contract arrangements to support the regular deployment and redeployment of German units. For this move to Latvia, where Germany has no such presence, the German contingent will have to rely more heavily on the NATO Force Integration Unit and Latvia's National Movement Coordination Centre to secure the services of civilian contractors to provide equipment for unloading and handling cargo and vehicles for onward movement, and on the permanent infrastructure built by NATO after 2014 to support possible operations in the Baltic region.

Railway systems traditionally rely on dedicated secure control and communication solutions which, when combined with 5G networks in the future, will provide the same type of risks and benefits to military movement as smart ports. Railway 5G communication use cases and related threat analyses have therefore not been considered further in this study.

Movement by Road

The VJTF is a multinational force. Apart from the core elements which will travel from Germany by rail, other elements will travel **from a variety of locations across Europe to the assembly areas**. Most of these movements, like that of the 1st Armored BCT (US) from Antwerp to Poland and 12 Armoured BCT (UK) from Paldiski and Muuga to Tapa, will take place by road.

Some road movements are 'line haul' – longer (more than one day) movements by which cargo loads are transported independently from home base or port of debarkation to their destination. However, for reasons of control and security, most military road movements are **organised into convoys**. These will be made up of tracked and other heavy vehicles loaded onto HETs, containerised equipment and supplies loaded onto a variety of container-carrying vehicles, and self-moving wheeled military vehicles. Depending on transit nation regulations, as few as five vehicles moving together may be considered a convoy. Because the requirements on convoys will vary between types of loads, they are wherever possible comprised of similar vehicle types. HETs and container vehicles may be either military or civilian contractor owned and operated. Dedicated HETs and military vehicles essentially rely on military communication systems and, according to the authors' opinions, will not be equipped with 5G based assistive technologies by 2030. The civil vehicles, however, by 2030 will likely be equipped with certain safety and fuel saving systems relying on 5G cellular networks that may be vulnerable to cyberattacks during military movements.

Many convoys – around 40% of the total – will need to be escorted for the purposes of traffic management and physical security. Those requiring escorts will include HET-transported tracked and heavy vehicles, dangerous goods, and other sensitive loads. Convoy escorts must be provided by the transit nation and responsibility handed over at national borders where jurisdictions change. The limited availability of escort capacity, which may include military police, medical and force protection

[25] The North Sea–Baltic corridor is one of several priority routes eligible for funding from the EU's Trans-European Transport Networks (TEN-T) programme, which aims to develop a Europe-wide network of interconnected transport solutions.

[26] Hodges, Lawrence, and Wojcik, *Until Something Moves*, 16.

elements will slow the overall movement of military units. Convoys must also secure advanced permission to cross international borders, where they will go through inspection and clearance procedures. They must plan refuelling locations and safe havens – locations for rest stops that offer opportunities to provide adequate physical security. It is expected that services provided by 5G-enabled intelligent transportation systems (ITS) will improve traffic safety and smoothness of transit, and reduce the environmental impact of convoys.

Movement Planning

A main concern for NATO at this early stage of an operation is prioritising and deconflicting movement. In 2027, ahead of time and under budget, NATO delivered its Enablement Support Services (ESS) suite of software tools to support the planning and execution of logistics activities including movements. As with its predecessor, LOGFAS, NATO requires all Allies to submit movement planning and tracking data through ESS to NATO's Movement Coordination Hub in Ulm, Germany. While some Allies use only ESS, others, such as the US and the UK, continue to use national systems in addition to bespoke solutions to translate data between the two.[27]

2.2.3 Technological Considerations

Despite the complexity of the military movement scenario, many aspects of the management and control of international movement, both civilian and military, **are expected to remain rather low tech**. As of today, information systems are often dated and rely on manual input. Real-time tracking of goods or equipment is rare. Military communication systems are often not connected to or reliant on civilian networks. In times of crisis, options may be further limited as security requirements demand the use of classified military computer networks. Although the armed forces are often not among the first adopters of technology developed in the commercial sector, the current report still considers relevant cases where adopting or interacting with new assistive technological solutions would be plausible.

Cybersecurity for movements is shared between the moving armed forces (for their own systems) and the various operators of contracted movement services in the transit nations, e.g. for rail movement in Germany, the rail operator Deutsche Bahn, and for port operations in Antwerp, the Port Authority of the Port of Antwerp-Bruges. Furthermore, military movement relies heavily on civilian actors for transport infrastructure and services but is only a small customer for these services and has little leverage over the implementation of their cybersecurity practices.

For **NATO-level consignment tracking,** NATO will also put communications and information systems (CIS) in place to support any operation, in addition to national CIS. The Commander of JTF (COM JTF), with the support of the NATO communications and information agency and NATO communication and information systems group, is tasked with providing adequate (NATO-level) CIS support, including for all possible movement schemes, and with assessing 'the adequacy and security of networks used to manage, store, manipulate and transmit operational and logistic data'. [28] However, CIS resources are limited and in the early stages of this operation, the full use of CIS to support NATO's movement will be constrained by the lack of a robust communications network.

[27] Eleanor Prohaska, 'Parlez-Vous LOGFAS? U.S. and Allies Speak the Same Language When It Comes to Logistics', US Army, 17 June 2021, https://www.army.mil/article/248593/parlez_vous_logfas_u_s_and_allies_speak_the_same_language_when_it_comes_to_logistics.

[28] NATO, 'Allied Joint Doctrine for the Deployment and Redeployment of Forces', 3–6.

2.2.4 Relationship to 5G and Scope of Further Analysis

Going forward, this report focuses on the use of 5G networking and services in the given military movement scenario. However, this is not a comprehensive report in that out of the four movement channels, sea (notably in the unloading phase in ports) and road have been chosen to illustrate the risks and opportunities of 5G technology through representative use cases. The selection of these strategic (sea) and operational (road) movement channels was made to align the current report to the scope of the report published by CCDCOE in 2021 titled 'Supply Chain and Network Security for Military 5G Networks'. Importantly, to keep the selected movement channels connected to the described scenario, and to illustrate in a hypothetical but practical way the 5G-related use cases as well as risks, **the unloading of equipment in the Port of Antwerp and consequent road movement to Żagań by the** 1st Armoured BCT will be the two concrete movement stages which the discussion from Chapter 3 is related to.

2.3 Technology Enablers for Military Application

Before diving into the concrete use cases 5G technology will have in the military mobility scenario for sea and road transportation, it is worth highlighting the main general 5G technology enablers that collectively or separately may bring significant opportunities, but also risks, for military applications in 2030.[29]

2.3.1 5G Radio Spectrum Allocation

5G radio technology is an enhancement of previous generation LTE cellular techniques. 5G technology supports beamforming, active antennas, and other measures for interference reduction. Furthermore, it foresees the use of dedicated or virtual combined radio channels (network slicing) for specific applications and service quality levels, essentially supporting the implementation of limited area private networks, i.e. inside of ports, and even unlicensed non-cellular 5G networks (DECT-2020)[30] in a legacy dedicated 1.9 GHz DECT frequency band. The 3rd Generation Partnership Project (3GPP), a standardisation body for cellular communication, specifies 5G operation in two frequency ranges: Frequency Range 1 (FR1 – 410 to 7,125 MHz) and Frequency Range 2 (FR2 – 24.25 to 52.60 GHz). For practical use, three frequency bands may be presented:

- **Bands above 20 GHz** (FR2 bands or mmWaves). High bands are suitable for highest throughput (>1 Gbps/device) short-range (<50 m) communication, especially suitable for dense areas and indoor communication. High frequency radio signals can be used for precise GPS-like localisation. In the time frame of 4–5 years, mmWave 5G will enable sub-metre accuracy positioning indoors, GPS signal shielded tunnels and warehouses, etc. The second important property is that due to the weak propagation of FR2 signals they are preferred for implementing private 5G networks from the regulatory side.
- **Bands between 1.5 and 7 GHz** (medium bands). Medium bands provide a good trade-off between coverage (several kilometres) and capacity (>100 Mbps/device). Newly added higher frequencies increase the total cell throughput. In some European countries including the Netherlands and Germany,

[29] Potential of 5G Technologies to Military Application, NCI Agency, https://www.mindev.gov.gr/wp-content/uploads/2020/11/Enclosure-2-Working-paper-Potential-of-5G-technologies-for-military-application.pdf

[30] 'Digital Enhanced Cordless Telecommunications (DECT)', ETSI, https://www.etsi.org/technologies/dect.

private networks can be implemented in frequencies around 3.7–3.8 GHz, which is attractive cost-wise for high density areas like RO/RO harbours. DECT-2020, which operates in the licence-exempt 1.9 GHz band, may have certain uses in short-range Internet of things (IoT) applications, possibly at harbours.

- **Bands below 1 GHz (low bands).** Low bands provide macro coverage features to 5G (>20 km) supported by the lowest energy consumption but also the smallest throughput of 26 kbps (downlink). Low band devices may be used, for instance, for smart road IoT sensor applications. Such battery-powered devices usually operate in deep duty cycling mode, meaning extensive use of cellular network infrastructure.

2.3.2 5G Core Network (CN)

5G communication provides different data transmission profiles according to user needs: 5G eMBB (enhanced mobile broadband) for high-throughput low-latency communication, for 4+K video streaming and VR applications; URLLC (ultra-reliable low-latency communication) for real-time lower throughput communication in industrial and vehicular control use cases; and mMTC (massive machine-type communications) supporting hundreds of thousands of low-power smart environment IoT devices sharing the available radio bandwidth. As cost-efficiency and scalability are drivers for 5G development, 5G CN provides a scalable network solution flexible enough to support all of those different usage requirements. In recent trends towards 6G technology development, attention is paid to the energy efficiency of network implementations, also applicable to upcoming 5G realisations. The most noteworthy 5G CN technical features are:

- **Network Slicing.** This is a network orchestration technique that allows MNOs to define subsets of the main network (a slice), each of which can be optimised for a particular service and performance target and/or to a specific customer. Network slices are cross-layer abstractions that include the RAN and where resources can be assigned flexibly. This is an end-to-end technology requiring specific functionality from the user equipment (UE), radio access network, and 5G Core network. End-to-end slicing is expected from 3GPP Release 17 onwards. Slicing can provide certain guaranteed connectivity services for ambulance vehicles and remotely controlled autonomous vehicles in public networks, for instance.
- **Multi-access Edge Computing (MEC).** As 5G's virtualisation approach allows advanced concepts such as mobile cloud computing (MCC), the resource pool can be de-centralised (distributed MCC) to the edge (the RAN) devices. This enables low latency at the application level and autonomous operation of 5G clusters (with no backhaul connection), by running a fully independent 5G CN and a small RAN using an MCC cluster. MEC is crucial for further smart transportation features like image driven operation of autonomous vehicles in factories, logistics centres and roads, enabling automated road crossings, collaborative obstacle classification, and so on. From another point of view, offloading certain network core functions to edge devices and including user application software in the MEC introduces new high risks for malicious behaviour and cyberattacks because of user application software installed directly on cellular network components.

A 5G private network is an enterprise or government network for **an organisation's exclusive use**. A private network provides high network performance levels, data management capacity, reliability, quality of service (QoS), low latency, security, and flexible coverage. As a 5G private network operates on a licensed spectrum, QoS can be guaranteed. Information assets are protected using network isolation, data protection and device/user authentication to protect information assets. With a private 5G network, the network owner can control data retention and data sovereignty policies. The 3GPP 5G standard [31] distinguishes two types of 5G private networks: a standalone non-public network (SNPN) and a non-public network (NPN) in conjunction with a public network. Consequently, a 5G private network can be deployed as a **full on-premises deployment** of a radio access network (RAN) and a CN; a **local deployment** of a dedicated RAN and a shared centralised CN; or by **network slicing** in a public network.

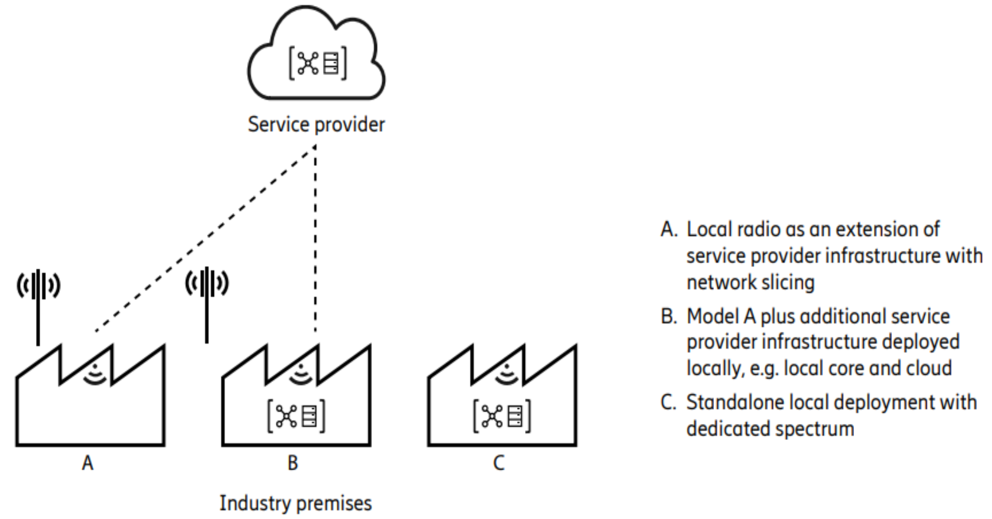

Service provider
A
B
C
Industry premises
A. Local radio as an extension of service provider infrastructure with network slicing
B. Model A plus additional service provider infrastructure deployed locally, e.g. local core and cloud
C. Standalone local deployment with dedicated spectrum

FIGURE 2. MAIN NETWORK INTEGRATION OPTIONS

Figure 2 demonstrates the **main options for network integration into the public network**. Model A shows a network where the only element added is private usage via a private service access point name (APN), while all user plane and control plane elements are provided by the public network offered by the service provider. Model B shows a network with a local dedicated RAN and control plane elements that are shared with the public network. Model C is the isolated network, where the whole network is deployed on-premises as a standalone NPN.

The interworking and roaming between the private and public networks provide **tight integration that enables service continuity and facilitates the operation and maintenance** of the private network.

For instance, in the standalone model, these activities need to be arranged for the NPN, while in the public network integrated model, the public network operator may take care of part of these services, according to the integration level. However, the corresponding reliance on the network operator also **increases third-party risks** for critical services and the potential for information leakage.

As LTE, 5G supports multiple operator core (MOC) and mobile virtual operator (MVNO) networks that provide separation between different mobile service providers – the more sophisticated MOC technology employs user data stream separation at the early base station (or MEC) level and MVNO at the host network operator level. Both solutions provide an additional security level for connected clients (with their own SIM cards) and are significantly less costly compared to creating a dedicated private radio network infrastructure.

[31] 3GPP TS 23.501: 'System architecture for the 5G System', https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-h40.zip.

According to the results of the European BroadWay project of the cross-border integration of critical cellular networks, the use of MOC and MVNO solutions may be considered for 5G connected vehicles performing military mobility operations across Europe.

Modern vehicular communication units for traffic safety services like eCall contain eSIM (embedded SIM) or iSIM (integrated SIM) microchips for subscriber identification (IMSI) and profiling for specific network services. With the support of NATO, it is advisable to investigate and develop European-wide technical and legal frameworks for remote reconfiguration of eSIM/iSIM user profiles to route client data through the trusted CNs – possibly owned by member state authorities – and make it possible to control the ProSe V2X services as described in the next chapter.

2.3.3 Proximity Services (ProSe)

In 3GPP, ProSe address communications between user equipment without the intervention of the 5G RAN or 5G CN, meaning that 5G radio devices can communicate in peer-to-peer mode, without mobile network infrastructure. Previously, ProSe were enabled by device-to-device (D2D) communications. D2D was first introduced in 3GPP's Release 12 (as LTE technology) but had limited use cases and was not implemented by industry. In 5G, 3GPP refers to D2D technology as **5G Sidelink or PC5 link**, which is now seen as attractive for cell coverage extension, emergency/public safety, and machine-to-machine interaction. The latter includes vehicle-to-vehicle (V2V, estimated share of ~40% of use cases), vehicle-to-(roadside)-infrastructure (V2I, estimated share of use cases ~30%), and vehicle-to-pedestrians (V2P, estimated share of ~20%) data exchange, all together known as V2X data exchange. ProSe communication is secure and provides data integrity checks. ProSe operates at a frequency of 5.9 GHz, similar to the competing Dedicated Short-Range Communication (DSRC) technology exclusively developed for V2V use cases and has been standardised as IEEE 802.11p radio technology. According to technical benchmarking, PC5 C-V2X outperforms IEEE 802.11p with respect to coverage, latency, reliability, and scalability.[32] Another study also shows improvements in C-V2X coverage over the DSRC V2X of at least 33% for highway scenarios (at 70 km/h) and of at least 18% for dense urban scenarios.[33] It can be foreseen that LTE Sidelink based C-V2X communication will win the competition with other technologies in the long run. However, during the next few years, incompatible DSRC and C-V2X technologies will exist in parallel and the service coverage of C-V2X will be weaker.

PC55 is naturally limited in range but provides the shortest latencies required for collaborative traffic management and industrial control applications. Using ProSe introduces certain specific security aspects because the actual data exchange between UEs is not under the control of the MNOs during the operation. Essentially, PC5 supports different connectivity modes like unicast (single device-to-device communication), groupcast (for specific group members), and broadcast (for all ProSe capable devices in proximity). Specific PC5 services, for example, enabling or disabling V2V communication, and appropriate connection group modes must be identified in IMSI user profiles, technically stored in the SIM cards. Reconfigurable PC5 communication is crucial to minimise dependency on external vehicular services and to disable broadcasting radio messages during the military road movements.

[32] P. Apostolos and A. Khoryaev, 'Cellular V2X as the essential enabler of superior global connected transportation services', IEEE 5G Tech Focus 1, no. 2 (2017): 1–2.

[33] 3GPP, H. Seo (rapporteur), 'TR 36.885 "Study on LTE-based V2X Services (Release 14), 3GPP Technical Specification Group Radio Access Network", V14.0.0', 2016.

2.4 Importance of 5G Use Cases in Military Applications

Current 5G roll-out plans will provide **growing opportunities for the development of 5G-related use cases** in European countries. The first examples of smart seaports and intelligent transportation systems relying on V2V communication are already in place. Although it is unrealistic to implement military purpose only 5G physical infrastructure due to the magnitude of the required investment, the commercial – both private and public solutions must be adapted for actual use. The armed forces' exposure to the risks and opportunities these 5G solutions present will thus primarily come from the use of civil 5G networks and civil contractors providing the movement services.

It is nevertheless important to address the use cases, the system architecture, and technical requirements for future purposes, to **eliminate any potential risks and threats**. With the continuing development of 5G infrastructure, all details need to be considered in today's planning phase, and both policy and decision makers must have a clear view and understanding of the underlying systems that will be in place with 5G implementation. Therefore, the report takes the approach that **both smart seaport and intelligent transportation system 5G use cases will be fully developed**. These sections will describe how these use cases will help to change the military movement value chain, and the positive contribution to the military, as well as risks and cybersecurity threats. **The unloading of equipment in the Port of Antwerp and consequent road movement to Żagań by the** 1st Armoured BCT will be used as an actionable example.

3. Smart Seaport Use Case

3.1 Smart Seaports in 2030

Seaports are important for the development of the global economy while terminal operators are under pressure to provide **even greater agility and faster turnaround times** to accommodate a market in which container traffic is expected to double by 2050.[34] By 2030, ships will be larger, goods will move faster, and new challenges with digitalisation and cybersecurity will affect ports worldwide. Digital technologies and automation will be adopted, thereby making ports 'smart'.

The most important container ports will have taken the strides in automation, enabled by 5G adoption by 2030. In these smart ports, digital transformation will enable higher levels of integration in information flows between parties in the logistics chain: from manufacturing to consumers or end-users. Currently, seaport communication systems are a mix of industry control systems with industrial Ethernet, Wi-Fi, and bespoke technologies. Embracing 5G will enable the next level of automation through technologies like big data and AI using connected IoT sensors, which will significantly enhance port operations and make them more efficient in terms of costs and speed. Essential features of 5G communication include support for ultra-reliable low-latency communication (URLLC), guaranteeing >=99.99% connection service availability and latencies below 20 ms which are crucial for the safe operation of harbour equipment. By 2030, automated and integrated logistics solutions will be adopted by leading seaports in automated seaport operations (image-based object recognition and operation), automated transport solutions (autonomous vehicles performing transportation from vessels to logistics centres to the destination; automated cranes, drones for packages distribution and security surveillance), and automated information management (IoT and AI-enabled sensor networks; predictive maintenance of machinery). Further implementations of mmWave 5G networks (compliant to 3GPP Release 17 and newer specifications) will enable sub-metre accuracy positioning in GNSS denied areas that may be relevant to smart harbour use cases as well. Many of these solutions and their use cases are outlined in Table 1.

There is evident motivation for harbours to install their own private 5G networks, which is possible in the broad range of FR2 (mmWave) frequencies across Europe and in dedicated FR1 frequencies available in some EU countries. A private network allows harbour users to isolate (possibly heavy) cellular data traffic from the data traffic required for the harbour's internal operation and eliminate the subscription costs of public MNOs. Indicative minimum investment to set up a private 5G network in a restricted harbour area is around one million euros today with the trend rapidly decreasing. In addition to the physical radio infrastructure installation cost, another major cost article estimated at around 0.5 million euros is 5G core software. Therefore, increasing interest to use open-source 5G core network software among the open-source radio access network (ORAN) solutions in active development can be foreseen around the globe.

[34] 'LTE/5G pervasive industrial wireless and the digital transformation of port terminals', Nokia, https://wpassets.porttechnology.org/wp-content/uploads/2021/11/18194220/Nokia_LTE_5G_for_port_terminals_White_Paper_EN.pdf

3.1.1 Overview of Use Cases

As the 1st Armoured BCT arrives in Antwerp, the port, like most other important commercial ports, will have fully embraced 5G-enabled solutions and become ‘smart’. The most relevant 5G use cases that will be in place are illustrated in Figure 3.

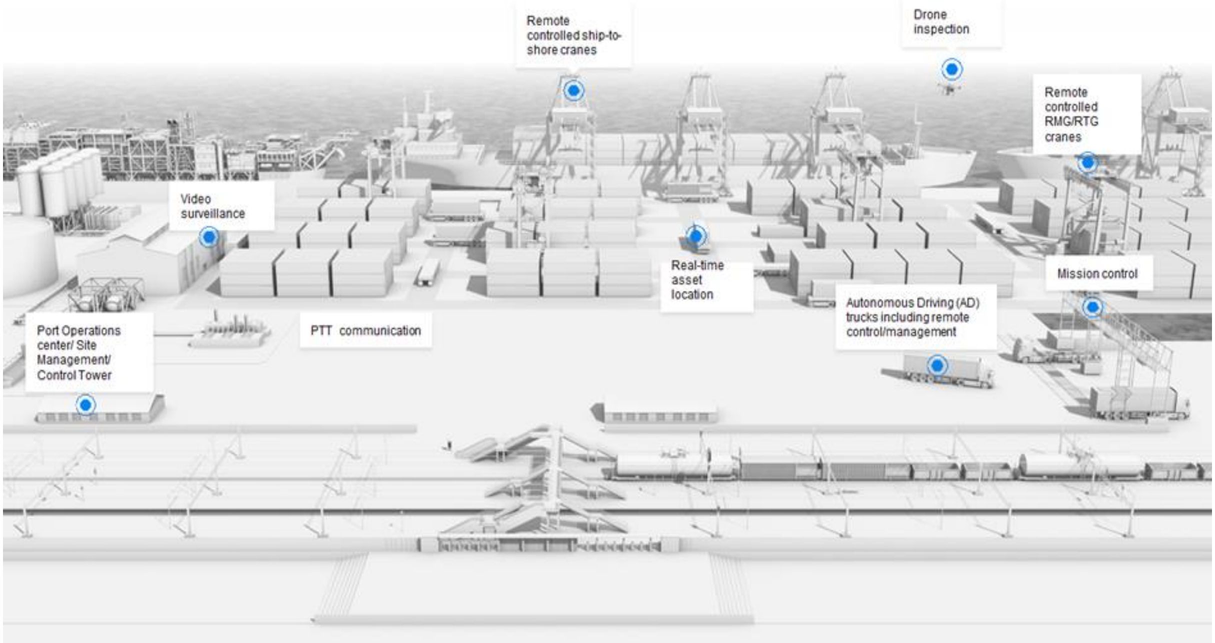

Remote controlled ship-to-shore cranes
Drone inspection
Remote controlled RMG/RTG cranes
Video surveillance
Real-time asset location
Mission control
Autonomous Driving (AD) trucks including remote control/management
Port Operations center/ Site Management/ Control Tower
PTT communication

FIGURE 3. SMART PORT USE CASES

Descriptions of the major smart seaports use cases, including their 5G connectivity enablers are provided in Table 1. The common high-level requirements for all the use cases described are **high throughput and availability** (eMBB) crucial for reliable high-quality video transmission; and **high reliability, resilience, and low latency** (URLLC) crucial for real-time remote operation.

TABLE 1. SMART PORT USE CASES WIDELY EMBRACED BY 2030

Use cases	Description	Military movement benefits
Remote-controlled ship-to-shore cranes	Ship-to-shore (STS) cranes loading and unloading containers between ship and dock. This operation demands communication to ensure the right containers move to their designated positions. Each dockside container crane needs sensors and high-definition (HD) cameras. Enabled by a 5G network with its low video transmission latency in combination with AI-supported applications, the crane operator can monitor and control the cranes remotely from a control room with high precision when needed for manual operations. Through the full visibility of operations in the remote-control room monitors, this use case	Faster, safer, and more reliable unloading of goods, including military equipment.

	enables more efficient operations via automated operations, shorter lead-times, and higher precision. **Connectivity requirements |** Enhanced mobile broadband (eMBB) massive IoT, critical IoT, and ultra-reliable low-latency communication (URLLC).	
Automated gantry cranes	Mobile gantry cranes are used for equipment transferring and flexible operations. Enabled by safety controllers, 3D-sensors/cameras and positioning devices, automated gantry cranes can conduct stacking operations automatically. Whenever any irregularity occurs, a remote operator can take over control via remote-control. **Connectivity requirements |** Critical IoT, ultra-reliable low-latency communication (URLLC), and enhanced mobile broadband (eMBB).	Faster, safer, and more efficient organisation of unloaded goods, including military equipment.
Automated guided vehicles (AGVs)	Automated guided vehicles (AGVs) and remote-operated vehicles require connectivity for drive instructions. When the vehicles are in autonomous driving operation mode, the route and its characteristics are downloaded to the vehicle from the route planning systems to the on-board vehicle platform. The on-board vehicle information consists of IoT sensor data and actuation with real-time characteristics and non-real-time data. Ultra-low-latency and accurate positioning are required for emergency stop functions and collision warnings, and for geo-fencing. Up-link video streams and haptic feedback to the remote driver are important when the vehicle is remotely operated. **Connectivity requirements |** Critical IoT, enhanced mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and real-time positioning.	Faster and safer movement of unloaded equipment to clearance.
Condition monitoring of harbour machinery and predictive maintenance	Condition monitoring of equipment using IoT sensors increases efficiency, lowers maintenance costs, and reduces downtime. For condition monitoring, the network needs to be able to manage high connection density and transfer data in real-time with high reliability. **Connectivity requirements |** Massive IoT (mMTC), critical IoT, and ultra-reliable low-latency communication (URLLC).	More reliable port services due to decrease of port equipment failure rates and faster operations.
Asset tracking	Asset tracking is to monitor and locate equipment thereby optimising operations. IoT sensors with embedded modems can be used to find equipment on-demand or upon alarms set by	Faster and more efficient organisation of unloaded

	sensors (temperature, mechanical impact, unintended displacement). Long battery life and positioning capabilities are important. In many cases it is also viable to use optical object recognition or scanning of QR codes. A special form of asset tracking is cyber-physical representations in digital twins. **Connectivity requirements |** Massive IoT (mMTC) and real-time positioning.	equipment in the port and faster clearing times and increased cargo security.
Drones for surveillance and inspection	Security has become a major concern for ports. Thefts of cargo are common, resulting in disrupted supply chains. Operated by a pilot remotely, drones can be deployed effectively for security, surveillance, and inspections. The drones require a network that can accommodate high-resolution video and provide high accuracy positioning with high bandwidth and low latency. **Connectivity requirements |** Critical IoT, ultra-reliable low-latency communication (URLLC), enhanced mobile broadband (eMBB), and Real-time positioning.	Increased physical and cargo security.

3.1.2 Military Interaction with the Smart Port Use Cases

These use cases represent both the opportunities and risks for the movement of the 1st Armored BCT. While the 5G-enabled Antwerp smart port has now increased its terminal TEU throughput by 7–10%, reduced its spending on maintenance by 10–15%, improved its safety risk management and reduced its safety alarm rate by 25%, and increased the efficiency of the Terminal Operations System by 30%, the transformation has been driven by commercial objectives. This is most prominently achieved by the private 5G networks that guarantee reliable services and allow to avoid network subscription fees.

As the cargo of the 1st Armored BCT arrives in Antwerp, containers will be unloaded by remote-controlled ship-to-shore cranes and stacked by automated gantry cranes, relying on 5G connectivity. Some cargo may be organised with the help of automated guided vehicles (AGVs), improving harbour operational safety and speed. Unloading procedures will be identical to those for handling civil goods. This potentially brings benefits in operational efficiency to the BCT as the containerised equipment is unloaded faster and with higher reliability than in the pre-5G era. The portside cargo will be organised faster and more precisely, therefore customs will be cleared faster. Drones add an extra layer of security to both personnel engaged in port operations as well as portside equipment. However, the large number of high-resolution cameras and sensor devices used for smart ports raise concerns regarding leakage of classified information, i.e. high-quality images of offloaded goods.

It is not expected that the use of 5G-enabled port infrastructure will significantly speed up landing processes of military goods. As described in Chapter 1, it takes several days for the 1st Armored BCT to get moving from the Port of Antwerp, but the delay is caused mainly by the lack of personnel, escorts, HET, and other necessary equipment, but also by checking, recording, and uploading the information for vehicles, equipment, and supplies on the US web-based logistics and finance system GCSS-Army. Therefore, it might be feasible to equip certain cargo items with real-time location and/or condition monitoring for this period. In such cases, installation of harbour owned preconfigured 5G IoT devices may be feasible.

As described before, it is not expected that in the next ten years military vehicles will be equipped with 5G UE. Therefore, it is not foreseen that military vehicles or any other equipment will use local 5G services provided by the port. Hence, the main risks of military transportation are related to information confidentiality and safe operation of port equipment. It is imperative that these risks are understood and mitigated when circumventing 5G solutions is likely not possible in the port (e.g. if the port no longer has pre-5G era cranes and corresponding process capability in place). The next chapter introduces 5G systems in place in ports; the risks and corresponding mitigation measures are underlined in Chapter 5.

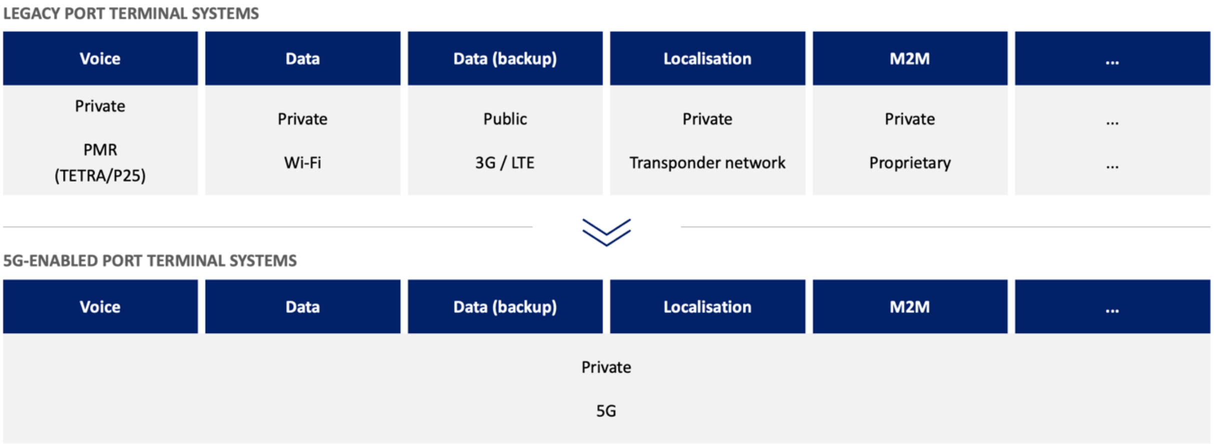
3.2 Underlying Communication Technologies at Ports

3.2.1 Transformation of Connectivity Solutions

To understand the technology the 1st Armored BCT will encounter in port operations in 2030, it is important to discuss legacy systems used in the beginning of 2020s. The legacy systems are fragmented and not fit for new generation digital solutions. In the last decades, digital solutions have been implemented gradually, resulting in the deployment of a variety of wireless network technologies: a professional mobile radio (PMR) platform based on TETRA or Project 25, Wi-Fi derivates, wireless sensor networks (WSNs) and industrial Internet of Things (IIoT) networks (i.e. IEEE802.15.4), low-power wide area networks (LPWA) for 2+km connectivity, and proprietary wireless technologies to support machine-to-machine (M2M) communications. While most of these wireless technologies had specific applications for general wireless data communications and especially for supporting the Terminal Operations System (TOS), most port terminals had implemented Wi-Fi, as shown in Figure 4.A public 3G or LTE service of a mobile network operator was also leveraged as the fallback option for general wireless data communications.[35]

Such legacy and stovepipe solutions hampered efficient automation in seaports due to a mix of different bespoke network solutions and technologies. The digital infrastructure of seaports must be able to handle the large amounts of data generated by sensors and actuators for cranes, vehicles, etc. Performance requirements set by IoT applications and operational management systems must be fulfilled. The requirements vary from Industry 4.0 IoT devices with low latency to enhanced mobile broadband for high bandwidth video sensors. In addition, the network infrastructure had to be reliable and resilient in case of cyberattacks. A convergence of wireless networks enabled by 5G technology, as demonstrated in Figure 4, was a perquisite for achieving these requirements.

[35] 'LTE/5G pervasive industrial wireless and the digital transformation of port terminals', Nokia, https://wpassets.porttechnology.org/wp-content/uploads/2021/11/18194220/Nokia_LTE_5G_for_port_terminals_White_Paper_EN.pdf.



LEGACY PORT TERMINAL SYSTEMS

Voice	Data	Data (backup)	Localisation	M2M	...
Private PMR (TETRA/P25)	Private Wi-Fi	Public 3G / LTE	Private Transponder network	Private Proprietary	... ...

5G-ENABLED PORT TERMINAL SYSTEMS

Voice	Data	Data (backup)	Localisation	M2M	...
Private 5G					

FIGURE 4. COMPARISON OF WIRELESS NETWORKS IN PORT TERMINALS

To forge the digitally connected seaports of the future, 5G technology provided a solution that fulfilled the seaports' requirements for efficiency, cost reduction, and security. A 5G network has **security 'by design'** and performance characteristics optimised for IoT.

3.2.2 5G Technology Framework for Smart Seaports

Figure 5 presents a **logical architecture for interactions** between the **smart port applications**, the **communications infrastructure,** and **possible external points of interaction of a** 5G-based connectivity solution. The port and usage specific requirements are as follows:

- Private closed 5G networks are preferred to guarantee high throughput for high-resolution video streaming and other eMBB services, fully excluding erroneous network access by UEs with external SIM cards.
- Private networks in size limited port areas are feasible to minimise user subscription fees.
- There is preference to combine network infrastructure equipment from several hardware vendors due to specific, nonconventional needs: a harsh industrial environment with bad radio signal propagation leading to microcells use, and a broad range of application needs from low-power IoT connectivity to high throughput image-based control and high-resolution positioning.
- There is preference to use open-source and third-party software (open radio access network (ORAN), 5G Core, and mobile edge computing (MEC) software). ORAN simplifies integrating hardware from different vendors, custom 5G core is more cost-effective and flexible, and MEC is crucial in the context of URLLC applications serving latency critical tasks directly in the base station or on-site hardware.
- There is high motivation to use the virtualised network functions (VNF) and cloud-native functions (CNF) of the 5G Core, because in private 5G networks there is no demand for central services like roaming management and user identity (SIM card) management, especially compared to local MEC-assisted tasks.

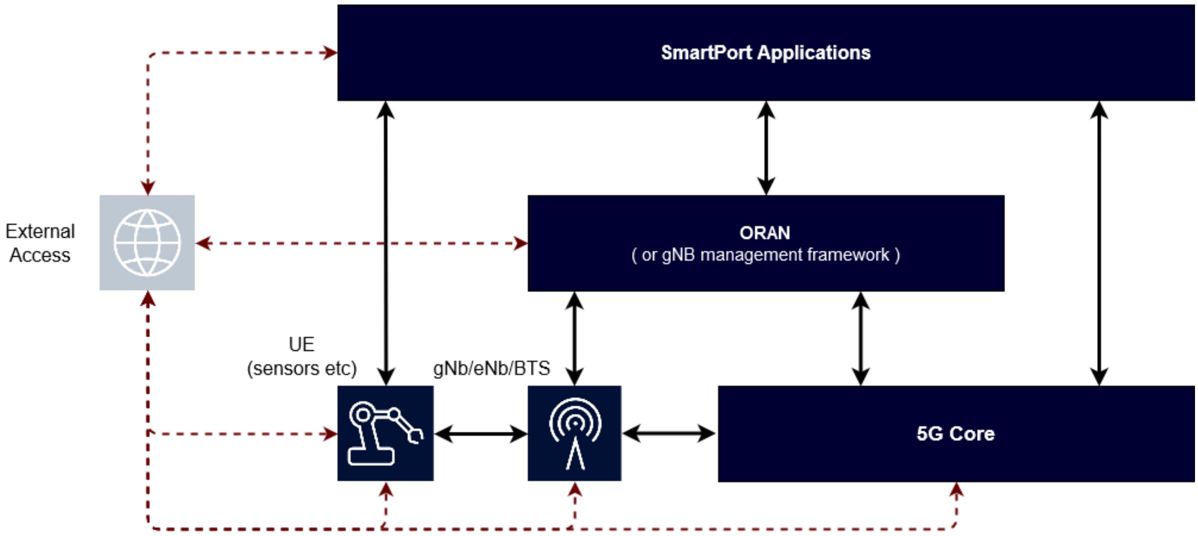


FIGURE 5. SMART PORT 5G/ORAN ARCHITECTURE

Such a system would be deployed via a **mix of bare-metal and cloud deployments**. The physical location of the data centres can vary from locally controlled to managed services, such as Amazon Web Services, Azure etc. It is assumed that the 5G Core, Applications and necessary parts of the ORAN management are **deployed in those data centres as (VNF)/ cloud-native functions (CNF)/ bare-metal applications**. **Base stations**, specifically the 5G gNB or 4G eNB, are assumed in the context of this report to be **a mix of bare-metal** (providing MEC services for low-latency operations) **and 'cloud' node devices**. For more modern systems, the software parts would be virtualised in a mix of on-device cloud provisioning with secured network connections to other gNB components running elsewhere, thus creating a 'virtualised' or 'distributed' device. **User equipment** (UE) characterises any sensor, device, or other equipment with access (but not necessarily authorisation) to the private network being deployed.

External access refers to **points outside of the private network being deployed**. This may be in the form of public interfaces (e.g. webpages, APIs) providing services to external parties, or in the form of unauthorised access to the system. External access here not only represents the wider Internet, but also **points of connection** between this network and other private networks. For example, incoming ships may run their own private networks on-board and either private network may allow interaction between these networks for data transfer related reasons.

The system perimeter is defined as the point where the control and data flows **cross from the private network to the Internet** at large. Within this private network, establishing the **security and identity of all devices joining and utilising that network** is required. This extends to the **data centre(s)** providing core and edge cloud functionality, the **devices and other hardware elements** providing gNB/radio functionality, the **user equipment** connecting to the network, and **other (private) networks**. It is expected that the vast majority of data generated in a private 5G port network is high-resolution streaming video intended for internal use in remote operation of machinery and surveillance.

Finally, establishing the **provenance of devices** and the **integrity of software** (e.g. containers, VNF) that are providing the system functionality is required. For example, 5G core deployment by container requires that the containers are from reputable sources and are untampered with at the point they are loaded into the cloud and deployment at run-time.

3.2.3 Smart Seaport Architecture and Characteristics

The design of a smart port follows the typical **IoT-edge-data centre / MEC approach**. The specific orchestration of edge devices or clouds, representing different instrumentations of MECs and IoT elements may vary in complexity as required. It is assumed for the examples here that the IoT devices connect to the private networks deployed within the port area, and this traffic is routed via the relevant endpoints and services provided by the edge and centralised clouds.

Figure 6 illustrates an example of a possible smart port architecture and communication network for 4G/5G networks. In this example, access points are deployed in the FR1 mid-band (3–6 GHz) licensed and and/or unlicensed spectrum, and certain applications like high precision network-based positioning still require the use of FR2 mmWave technology. For machine-type connections URLLC should be used. There is also a potential need for a very high-capacity wireless link which provides high-quality video (4K, 360° degree, augmented/virtual reality) for monitoring the remote port operations. For these applications, high-capacity access with 5G mmWave deployment is the optimum choice, perhaps complemented with Wi-Fi access. Ship-to-shore satellite communication could also be part of the network architecture.

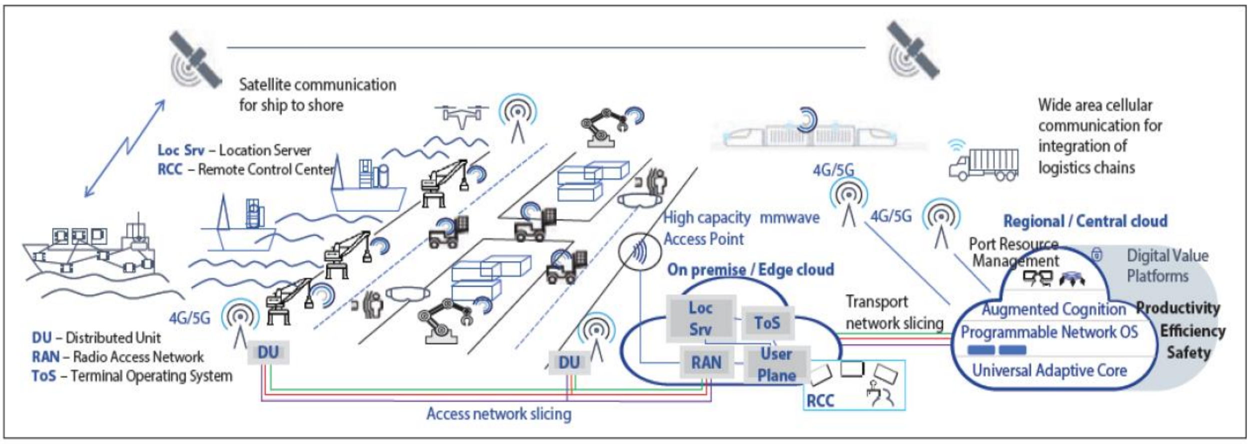


FIGURE 6. EXAMPLE OF A POSSIBLE SMART PORT ARCHITECTURE

While the architecture of the smart seaport environment follows a common IoT-Edge-Central Cloud structure, there are characteristics, particularly pertaining to the **prior knowledge of devices**, unique to this environment.

First, the port consists of a **'fixed' set of systems relating to the physical infrastructure** such as cranes, cameras, and port division (implying some form of network and system segmentation) with some form of centralised, though possibly federated, control. The use of edge technologies can be driven by efficiency and responsibility requirements but in this case **edge and network segmentation (slicing)** is preferred as an important mechanism for providing security. Network slicing is an alternative method to guarantee required data throughput but does not address the issues related to network security. However, slicing **effectively isolates the command and control of the systems**, thereby mitigating the amount of interference and damage in case of attack. This serves as an **overlap between security and resiliency** in a system.

The second defining characteristic is the **dynamicity of the system**. For example, ships with private on-board networks are required to 'join' and communicate with the smart seaport systems. Furthermore, as elements such as containers themselves become 'smarter', they are also required to **join and communicate with the smart port systems**. While this provides efficiency benefits and allows for new use cases related to IoT solutions, it also introduces the **threat of untrusted**

and unknown devices entering the smart port networks. These devices or systems can become compromised in either actively generating attacks or being misconfigured and producing incorrect or untrustworthy information. Countermeasures for these potential downsides will be covered in Chapter 5.

3.2.4 Recommendations for Implementing 5G Private Networks at Smart Seaports

Smart seaports should employ 5G private networks to improve the operational efficiency independent of the cargo type to be handled. It is also advisable not to open the network services to external users, including travellers or any kind of civil or military vehicles in general. Alternatively, network slicing of public networks can be used to guarantee throughput communication, but this approach does not solve the security concerns and may be even more costly to port operators in terms of subscription costs. Hence, there is a clear technological and economic motivation to use private 5G networks in smart ports. The advantages of 5G private networks for smart seaports can be summarised as follows:

- → **High availability and reliability** by having control of network resources and priority settings
- → **Security** via full end-to-end security enablement control
- → **Quality of service (QoS)** by system performance and resource use for different services tailored to their specific needs
- → **Open ecosystem** with economies of scale thanks to standards-based solutions.

The **open ecosystem** allows integration of 5G devices and application development leveraging communication infrastructure capabilities and it is also possible to select specific options such as specific security modules or new 3GPP features not yet available in commercial mobile networks. However, port authorities may not be sufficiently competent to analyse and maintain open ecosystems that contain a variety of hardware and software components. Certain security concerns of ORAN have been presented in a recent report by NIS Cooperation Group.[36] It is recommended that private port networks are set up and maintained by certified telecom systems providers and the 5G implementations are regularly audited by responsible national authorities.

From an economic perspective, non-public (NPN) private network architecture with remote cloud-based core services is more efficient than standalone (SNPN) local implementation. This is especially true assuming that for URLLC, an extensive use of MEC services is mandatory at ports for eMBB operations. However, it introduces additional security concerns due to hosting and servicing issues.

The interworking and roaming between the private and public networks provide **tight integration that enables service continuity and facilitates the operation and maintenance** of the private network. For instance, in the standalone model, these activities need to be arranged for the NPN, while in the public network integrated model, the public network operator may take care of a part of these services, according to the integration level. However, the corresponding reliance on the network operator also **increases third-party risks** and would ideally be avoided in seaports delivering critical services, including military assets. In general, from the perspectives of the reliable operation of smart port infrastructure and the confidentiality of military operations, data exchange between private and public networks should be minimised and (mainly imaging) data, used for machine operations and surveillance **should not be propagated outside**

[36] 'Report on Cybersecurity of Open RAN', NIS Cooperation Group, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks

of the private port network, including to physical data storage.

Life cycle management of network infrastructure, introduction of new features and backwards compatibility for applications are other keys to guarantee seaport operations. **Trusted hardware vendors and competent system integrators** with full control of the supply chain used for all components are essential both for functional behaviour and to mitigate cybersecurity issues (see Chapter 5.3).

3.3 5G Network Implications to Military Activities in Smart Ports

In the context of the military movement scenario, most, if not all, ports that the military cargo moves through are **commercially owned** running a mix of public and private 5G networks. Furthermore, for the **strategic movement of equipment, the military will still heavily rely on private sector companies** that offer stevedoring services. By 2030, most probably the 5G solutions (both practical use cases and underlying technology) in smart ports would not be developed or modified specifically for military use or linked in a distinct way to existing military networks. Also, there is expectation of a minimal immediate interaction in terms of data exchange between transported military equipment and vehicles and smart seaport 5G infrastructure.

On the one hand, this means that **the military will be reliant on the 5G systems in place in smart ports by 2030**, including the security, reliability, and risk management attributes of these commercial smart port systems. An overview of cybersecurity risks and risk mitigation measures will be presented in Chapter 5. On the other hand, **the military can still reap benefits from the commercial adoption of 5G solutions in smart ports**. Potential benefits of the main smart port 5G use cases to the military have been highlighted next to use cases.

Overall, the military will benefit from **the increased efficiency, throughput, reliability and security of 5G-powered smart ports** and these benefits will translate into some operational efficiency and safety improvements in the movement scenario. For example, as the 1st Armored BCT transports 3,000 pieces of equipment to the Port of Antwerp, the new 5G-supported automated cargo handling solutions (such as remote-controlled ship-to-shore cranes, guided vehicles) will likely increase the speed at which the (especially containerised) equipment and supplies are unloaded and asset-tracking IoT devices will increase the efficiency and speed of clearance procedures with local customs officers. At the same time, the 5G-connected drones will provide additional physical security. Altogether, the 5G solutions used in ports by 2030 will potentially **make cargoes ready for onward movement faster and with less operational risk than today**. In other words, it is expected that the use of 5G technologies at smart seaports will improve the operational efficiency of the ports. However, the upside specific to military operations is only marginal as true bottlenecks lie elsewhere. Still, it is a given that military transportation operations will rely on new 5G-enabled equipment in ports in 2030 and hence **be exposed to the risks** that come with these commercially developed modern technologies and the large amount of information produced during port operations. These risks (described in Chapter 5) must be acknowledged and prepared for.

4. Smart Roads Use Case

4.1 Smart Roads in 2030

Commercial mobile network operators (MNOs) are rolling out 5G cellular networks across Europe and the US, including NATO member states. It is expected that **by 2030, fully functional 5G new stand-alone (SA) networks will be deployed**, enabling the use of the most advanced services for low-latency high-reliability high-throughput cellular communication. The European Commission is investing heavily[37] to speed up the buildout of 5G infrastructure and the development of advanced digital services utilising the capacities of 5G communication technologies, specifically for 5G use cases in transportation, including intelligent transportation system (ITS) solutions.

Road transportation and its value chain ties with the future of military movement scenarios that will heavily rely on novel ITS technologies, which allow for the optimisation and cost-effectiveness of the logistical processes. Future military transportation will also be more efficient, smoother, and more environmentally friendly. For the current scenario, **the cargo and machinery loaded onto trucks, partially rented from the civil sector, at the Antwerp smart seaport together with wheeled vehicles will now head onto the roads**. With 5G use cases in road transportation, the vehicles will form a platoon (tight convoy) and move in unison while gathering and using information from different road and transportation solutions users.

One of the most important enablers for future ITS services is cellular vehicle to everything (C-V2X) communication, which creates a system of hard real-time situational awareness about all parties involved in traffic. The overall idea of V2X is to enable real-time information sharing between vehicles, react to changing traffic and road conditions in a timely way according to road sensors, safely collaborate with vulnerable road users (VRUs), i.e. pedestrians and cyclists, and more. C-V2X with its low latency and high reliability is ideal to address road safety, fuel economy – especially for heavy vehicles – and overall traffic efficiency.[38] Specific applications highlighted in the literature include driver assistance for crash avoidance,[39] cooperative behaviour (platooning, cooperative cruise control),[40] and advanced/remote driving that improves overall situational awareness in traffic.

4.1.1 Overview of V2X Use Cases

An overview of 3GPP identified C-V2X use cases is presented in the bulleted list below. The links to different road transportation use cases are illustrated in Figure 7.

[37] Connecting Europe Facility, accessed 10 February 2022, https://cinea.ec.europa.eu/connecting-europe-facility_en.

[38] Lili Miao, John Jethro Virtusio, and Kai-Lung Hua. 'PC5-based cellular-V2X evolution and deployment', *Sensors* 21, no. 3 (2021): 843.

[39] Takeshi Hirai and Tutomu Murase, 'Performance evaluations of PC5-based cellular-V2X mode 4 for feasibility analysis of driver assistance systems with crash warning'. *Sensors* 20, no. 10 (2020): 2950.

[40] Giovanni Nardini, Antonio Virdis, Claudia Campolo, Antonella Molinaro, and Giovanni Stea, 'Cellular-V2X communications for platooning: Design and evaluation', *Sensors* 18, no. 5 (2018): 1527.

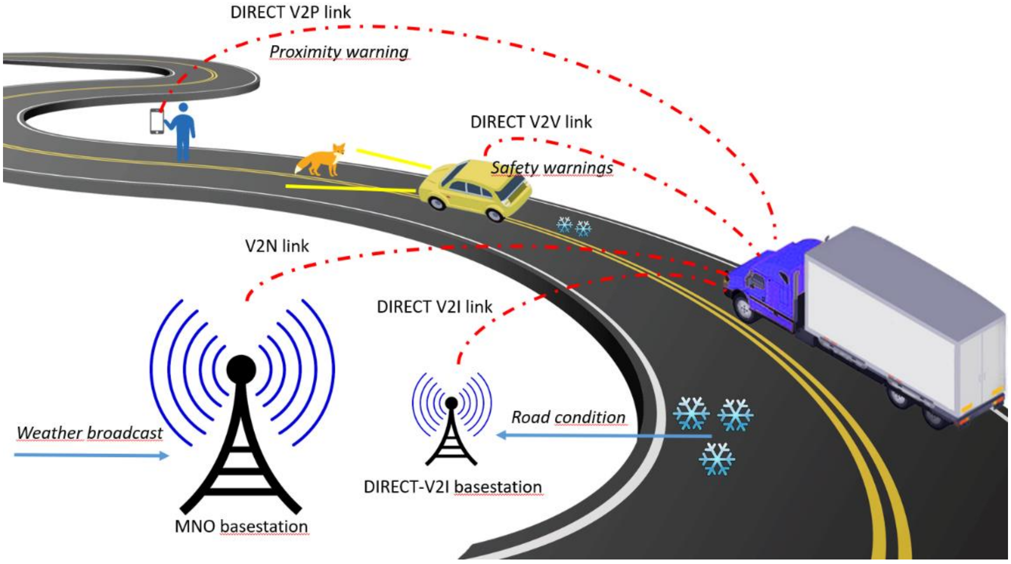


FIGURE 7. OVERVIEW OF V2X USE CASES

The 3GPP standards organisation has defined and described four main C-V2X use cases:[41]

- **Vehicle platooning** that enables the vehicles to dynamically form a platoon that is travelling together.
- **Extended sensors** that enable the exchange of raw or processed data gathered through local sensors or live video from vehicles, road site units, devices of VRUs, and V2X application servers.
- **Advanced driving** that in the long run enables semi-automated or full-automated driving.
- **Remote driving** that enables a remote driver or a V2X application to operate a vehicle for those passengers who cannot drive by themselves, or remote operation of vehicles located in dangerous or unreachable environments.

In general, the use cases foresee that by 2030, a significant portion of truck transportation will take place on bigger highways in semi or fully automated vehicles that drive in a platoon. In this case, a group of transportation vehicles drive close together (distance down to a few metres) in a coordinated manner to save fuel, have full awareness of the traffic around them and get information directly from road users using V2X communication channels.

In terms of computationally sophisticated C-V2X applications, especially support for autonomous vehicles, the high importance of MEC is foreseen[42] to offload certain tasks from vehicles to computationally powerful cellular network connected devices and benefit from the data collected from multiple sources in real time. Naturally, providing information or relying on external (MEC) services does introduce certain new security concerns, which did not exist prior to the ITS era.

[41] M. Jalal Khan, Manzoor Ahmed Khan, Azam Beg, Sumbal Malik, and Hesham El-Sayed, ‘An overview of the 3GPP identified Use Cases for V2X Services’, *Procedia Computer Science* 198 (2022): 750–756.

[42] Shaoshan Liu, Liangkai Liu, Jie Tang, Bo Yu, Yifan Wang, and Weisong Shi, ‘Edge computing for autonomous driving: Opportunities and challenges’, *Proceedings of the IEEE* 107, no. 8 (2019): 1697–1716.

Taking into account a more detailed approach and potential by the 5GAA Association, the transportation and logistics related use cases can be related to one or more applications group[43] highly relevant to military transportation, as presented in Table 2.

TABLE 2. ROAD TRANSPORTATION USE CASES WIDELY EMBRACED IN 2030

Use cases	**Description**	**Military movement benefits**
Vehicle platooning	A group of transportation vehicles driving close together in a coordinated manner. All the vehicles in the platoon obtain information from the head vehicle (HV) to manage the platoon.	Increased fuel efficiency, logistics speed, safety, and traffic smoothness
Obstructed view assist	A vehicle needs an unobstructed view to proceed safely. This view is provided by a camera or other vehicles or roadside infrastructure. The vehicles can increase the perception of their environment beyond what their own sensors can detect and have a broader and more holistic view of the local situation.	Better situation awareness and potential threat monitoring
Cooperative automated (lateral) parking	A vehicle cooperates with neighbouring vehicles and VRUs to inform them about roadside parking manoeuvres.	Faster movement of unloaded equipment to clearance
Interactive VRU crossing	A VRU, such as a pedestrian or cyclist, signals its intention to cross a road and interacts with vehicles approaching the crossing area.	Increased security and traffic smoothness
Tele-operated driving	A remote driver undertakes the control of the vehicle and drives it continuously. An autonomous vehicle temporarily requests remote operation to resolve a situation with high uncertainty.	In case of emergencies or attacks, operation can be taken over by human control
Semi-automated or fully automated driving	Each vehicle and/or roadside unit (RSU) shares its own perception data obtained from its local sensors with vehicles in proximity and that allows vehicles to synchronise and coordinate their trajectories or manoeuvres. Each vehicle shares its driving intention with vehicles in proximity.	Increased situational awareness and security through joint movements

[43] 5GAA, ed. T. Linget, ‘C-V2X Use Cases Volume II: Examples and Service Level Requirements’, 2020.

Cooperative manoeuvres of autonomous vehicles in emergency situations	An autonomous vehicle (AV) identifies a dangerous situation and undertakes to coordinate with nearby AVs to decide and proceed joint manoeuvres.	Increased security and threat avoidance
Automated intersection crossing	An autonomous vehicle goes through an intersection with traffic lights considering the timings of the lights.	Faster movement of unloaded equipment to clearance and end destination, increased fuel efficiency
Accident reporting	In case of a traffic incident, a report containing a time-windowed recording of vehicle sensor data, environmental information, and available vehicle's camera views is sent to a dedicated data centre.	Fast response and situation awareness in convoys

4.1.2 Military Interaction with the Smart Road Use Cases

In the context of the military movement scenario, once the equipment leaves the smart seaport in Antwerp, it travels by road towards the destination in Żagań, Poland. It is assumed that by 2030, the roadside 5G infrastructure enabling C-V2X has been installed on the roads traversed. As Chapter 1 underlined, the vehicles moving will be made up of tracked and other heavy vehicles loaded onto HETs, container-carrying vehicles loaded with containerised equipment and supplies, and lighter, self-moving wheeled vehicles (such as soft-skinned lorries and utility vehicles). While HET's are specialised vehicles for transporting oversized loads, sometimes commissioned, and built according to military specifications, it is possible that container-carrying vehicles and lighter vehicles were built according to commercial specifications and therefore already have C-V2X connectivity capability built in by 2030. This is even more likely to be the case, as some of the vehicles are not owned by the military but instead outsourced to commercial parties. The military is not likely to have any control over the detailed specifications of the outsourced vehicles in regard to whether or not they have 5G capabilities.

If at least some of the vehicles moving from Antwerp to Żagań have 5G capabilities, and the roadside infrastructure is in place, the military is faced with a similar risk-reward situation regarding 5G as described in Chapter 1. On the one hand, there are advantages to gain from the 5G capabilities. Using new technological solutions allows the military to **move their equipment and vehicles faster and more efficiently, while increasing road safety, traffic smoothness by creating less traffic congestion,** and at the same time **decreasing the environmental impact** that the military movement creates. The convoys moving towards Żagań could in theory reduce their fuel consumption and decrease the possibility of collisions with platooning technology, reduce the risk of potential external threats to the convoy by better anticipating these threats with obstructed view assist and cooperative manoeuvres in emergency situations, as well as to relay relevant information faster to all convoy members with accident reporting. It could even be possible to reduce personnel needed to move the convoy using automated or tele-operated driving capabilities. There is clearly an upside to smart road technologies for military use as they enable the convoys to be more coordinated, flexible, spend less resources (both natural and human) on the movement, and reduce risk of human error. However, these 5G enabled opportunities may not be fully realisable without the relaxation of current military requirements for transportation, regarding convoy speeds, routes, technical and safety requirements etc.

Nevertheless, using 5G technologies comes with risks for the convoy. By 2030, 5G roll-out will be completed for road transportation use cases with the development driven by commercial and public incentives. Military movement needs to account for the transportation value chain that is set up by private civil contractors. It is not plausible, for example, that 5G military networks and infrastructure will be set up in parallel to the public networks and infrastructure managed by MNOs. In other words, the 5G base stations will be built for everyone to share which constitutes a security risk if mission-critical equipment relies on them. Therefore, similarly to smart ports, there are significant downside risks (more thoroughly explained in Chapter 5) with 5G technology that the military must grapple with. However, it is also noteworthy that **risk mitigation in the smart road scenario is conceptually different to that in the smart port scenario**. The 5G-powered Port of Antwerp most likely uses a private or at least a slicing-supported 5G network for its multiple operational use cases and the military objects are not connected to the port 5G network, highlighting information leakage as the main security concern. During the road transportation activities, the military cannot avoid interacting with public 5G networks serving specific ITS services. It might be possible for the military convoy to disconnect itself from the public 5G services to minimise V2X related cybersecurity risks but such an approach, besides disabling useful features like platooning and increasing the probability of traffic accidents, may not be technically possible for civil rental vehicles. It is not advisable to make disabling ITS and V2X services a straightforward task for military movements at a national and EU level and try to find a technological compromise between military cybersecurity concerns and public road safety and efficiency. It is important that the 5G systems, including potential benefits and related risks are understood so that correct decisions can be made well before 2030. To understand the technicalities behind the underlying technology, the following chapter gives an overview of 5G networks and standards that will be in use with the roll-out of 5G and use cases in road transportation. Risks and mitigation strategies are covered in Chapter 5.

4.2 Underlying Technology

The underlying road transportation use case will rely on C-V2X technology enabling further ITS services. C-V2X combines V2N (vehicle-to-network) connectivity – conventional data exchange through the cellular networking infrastructure and device-to-device (D2D) communication providing a direct link between two UE devices without engagement of cellular infrastructure during the data exchange. The D2D radio interface, described previously as ProSe or a PC5 link, is crucial to provide short latencies below ten milliseconds of intervehicle messaging, establish communication between vehicles and VRUs, and provide strictly local information from roadside sensors and traffic signs.

Compared to the seaport use case, which will take place in a private/ hybrid network with extra security added, V2N services of smart road transportation will rely on existing public cellular network infrastructure to provide 5G-driven ITS services. Due to setup costs, it would be unrealistic to operate road transportation in a separate private network, therefore, the military needs to rely on public networks, taking into the account relevant cybersecurity risks.

For the platooning scenario, as the core use case for the military transportation, the supportive system will be based on a public 5G network with fully or partially enabled C-V2X services and MEC services for local area networking and distributed computing. A general overview of the system architecture is depicted in Figure 8. The convoy with movable military goods travels along a predetermined path using C-V2V technology to maintain the correct direction and optimal distance between vehicles (inside the red square in Figure 8). Within the convoy of vehicles, there will be a driver allocated at least to the very first vehicle, if not to others. In such a case, a situation may arise where the first vehicle with the driver is detached from the main convoy and a convoy member vehicle receives (malicious) emergency condition messages through the V2X channel, etc.

D-V2V PC5 communication is used between the vehicles to maintain the distance between the vehicles. From a security perspective, it must be kept in mind that in 'default' mode, PC5 operates in broadcast mode meaning that connections are established with all neighbouring parties. PC5 V2V communication supports a selection of modes, as broadcast, groupcast, unicast and can be disabled through the IMSI (SIM card) settings. The PC5 link mode control helps to reduce risks related to malicious behaviour of captured road sensors or fake VRU devices. In addition to D-V2V communication, the convoy, at least the head/escort vehicles, also should be able to communicate over C-V2N channels to receive centrally provided information. The system uses the services of several mobile operators in the public network on roads to ensure the availability.

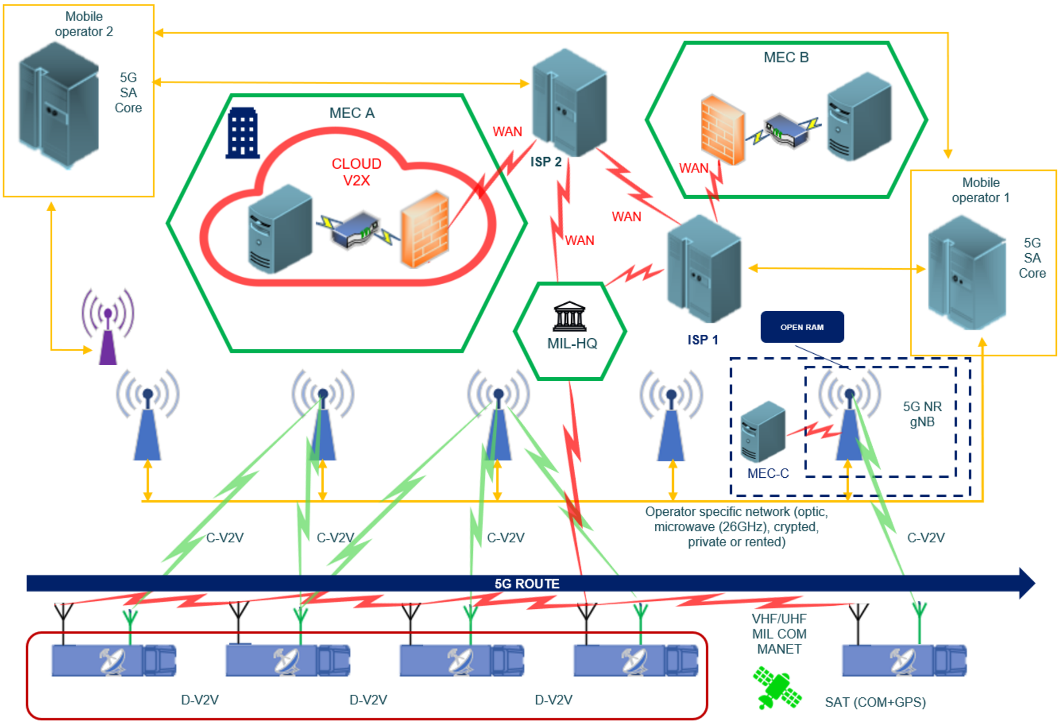


FIGURE 8. C-V2X SYSTEM ARCHITECTURE WITH A FOCUS ON A PLATOONING APPLICATION

For conventional, civil use cases, shared MEC computing is enabled for computationally demanding and shared tasks. The multi-access edge computing (MEC) solution is used to operate and manage the V2V and V2N systems. The components of the MEC system can be in various locations in the architecture, depending on the tasks assigned to them. When maintaining the distance between vehicles, the MEC must be located either inside the vehicle or integrated into the base station. The general convoy management can also take place over a wider area network as real-time functionality is not as important. If the convoy moves in different regions, so-called regional MECs may exist (MEC-B in Figure 8). In addition, regional MECs may be orchestrated by a global, pan-European MEC system (MEC-A in Figure 8). As orchestrating MECs can happen in different countries, depending on where the convoy is located, different ISPs (internet service providers) are also involved (ISP1 and ISP2 in Figure 8).

Going forward with cybersecurity aspects, the following is considered: It is assumed that 5G networks are significantly more secure than current state-of-the-art solutions and the wireless 5G network by design is significantly secured (green links in Figure 8). According to the network design, connections between different MNOs are also sufficiently secure since they are separate data channels (yellow links in Figure 8). MECs in various locations are most likely to be affected by cyber threats. They can be hacked over a wide area network, in some cases have unknown freeware, or be attacked by denial-of-service (DoS) type attacks etc. Public ISPs and their 49

associated MECs plays a key role in the aspect of cybersecurity here, and that is why Chapter 5 on risks will focus on these aspects. However, in addition to specific MEC threats, the aspects of cybersecurity that may be related to the overall security level of 5G networks and their implications at a general level will be covered to address their significance.

4.3 5G Network Implications on Military Activities in Road Transportation

In the military movement scenario of the equipment, the military will still heavily rely on civil private sector companies that offer road transportation services. By 2030, it will most probably not be the case that the 5G solutions (both practical use cases and underlying technology) would be developed or modified specifically for military use or linked in a special way to existing military networks.

On the one hand, this means that **the military will be reliant on public 5G networks in place that pose higher risks and threats that need to be taken into account when planning for the military movement scenarios.** An overview and mitigation measures of cybersecurity risks will be presented in Chapter 5.

On the other hand, **the military can reap significant benefits from the commercial adoption of 5G solutions in road transportation**. Potential benefits of the road transportation and platooning 5G use cases to the military include **increased efficiency, reliability, and security** and these benefits will translate into operational improvements in the movement scenario. For example, after the successful debarkation of the military equipment in smart seaports, described above, the 1st Armoured BCT can transport the necessary equipment to its destination significantly faster and more cost-effectively, while decreasing the effect on traffic congestion and the environment. Altogether, the 5G solutions in use in 2030 will **make military movement faster and face less risk than would be expected today**.

5. Military Movement-Related Cybersecurity Risks and Mitigation

5.1 Risks Associated with Military Movement Scenarios

In this section of the report, the aim is to give a systematic and high-level security analysis of the use cases given in the previous sections. Threat modelling approaches suit this purpose as they are utilised for comprehending possible threats at the initial stages of development life cycles, even though they can also be helpful in later phases or hypothetical use cases. More specifically, the STRIDE (a mnemonic for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) approach applied to many software developments projects [44] and adopted into complex cyber-physical systems in numerous studies is used.[45] The risks listed below were identified by this method, however, the specific approach is not described to ensure the simplicity of the document.

Both seaports and road transportation solutions are part of the critical infrastructure for logistics and need to have high demands on data security for functional safety and reliable connectivity. The exchanged data and information can be considered as sensitive assets that need to be protected from cyberattacks and enemy exploitation. Both the smart seaport and smart road transportation assets with a risk exposure to cyberattacks include:

→ **information assets**: data in transit, user data, control signalling, network management data, and data stored in data centres;

→ **infrastructure assets**: systems, hardware, platforms, and applications.

Threat actors include organised cybercriminals, nation states, hacktivists, terrorists, and insiders. These attackers are generally motivated by three main factors: money by ransom blackmail, stealing of business sensitive information and data, and finally sabotage. Exploited security weaknesses are:

→ improperly designed IT security policy that is also not enforced, monitored or constantly tested;

→ lack of hardening and insecure configuration of the network;

→ operational procedures;

→ lack of visibility, control, and monitoring.

Figure 9 shows the attack surfaces on network infrastructure that can be exploited by a cyberattacker. Cyberattacks can have severe implications on smart transportation infrastructure and use cases with high cost for protection and mitigation, and unknown losses due to stolen property (data) and losses in productivity. The impacts of cyberattacks in severe conditions could be devastating for logistics and transport solutions vital for the military movement.

[44] Michael Howard and Steve Lipner, *The security development lifecycle*, Vol. 8 (Redmond: Microsoft Press, 2006).

[45] Wenjun Xiong and Robert Lagerström, ‘Threat modelling – A systematic literature review’, *Computers & Security* 84 (2019): 53–69.

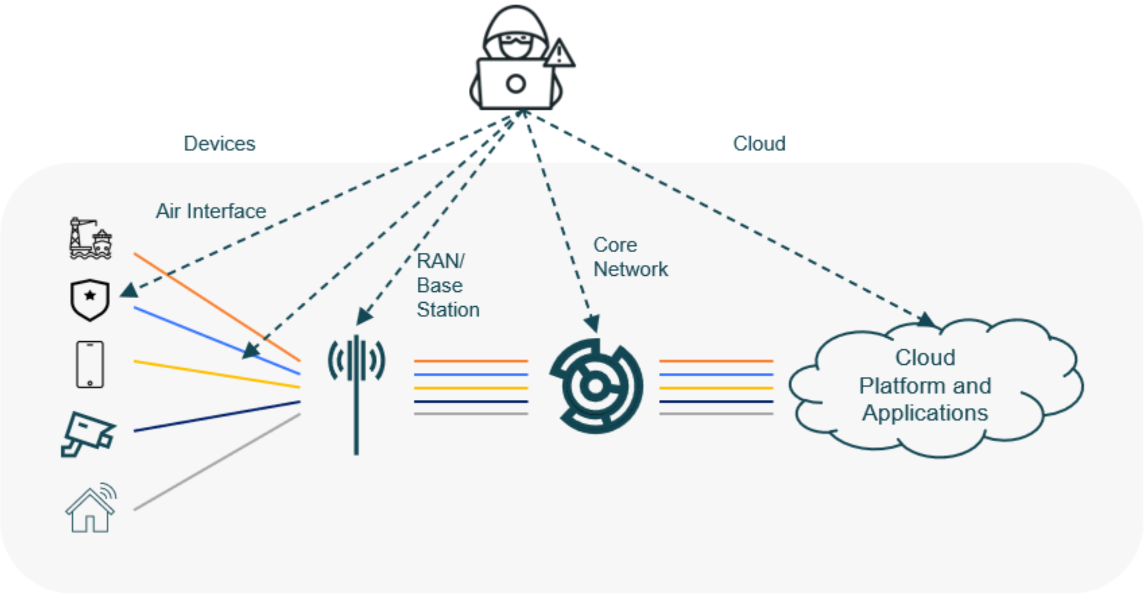


FIGURE 9. CYBERSECURITY ATTACK PLATFORMS

In addition to general 5G network-related risks, there exist a multitude of different types of risks related to 5G Core, RAN, cloud services and even from an operational security perspective, as shown in Figure 10. For example, attacks against 5G RAN via jamming operational systems could cause convoys and port machinery to halt operations and cause system shutdowns; and malicious interception can reveal information about military unit locations, their composition, and route. It is therefore important to stress the fact that UE networking and MEC related threats, that are the key element of this research report, are not the only risks and threats but are analysed to the extent of the report's scope as the military transportation related use cases will be based on multi-access edge computing.

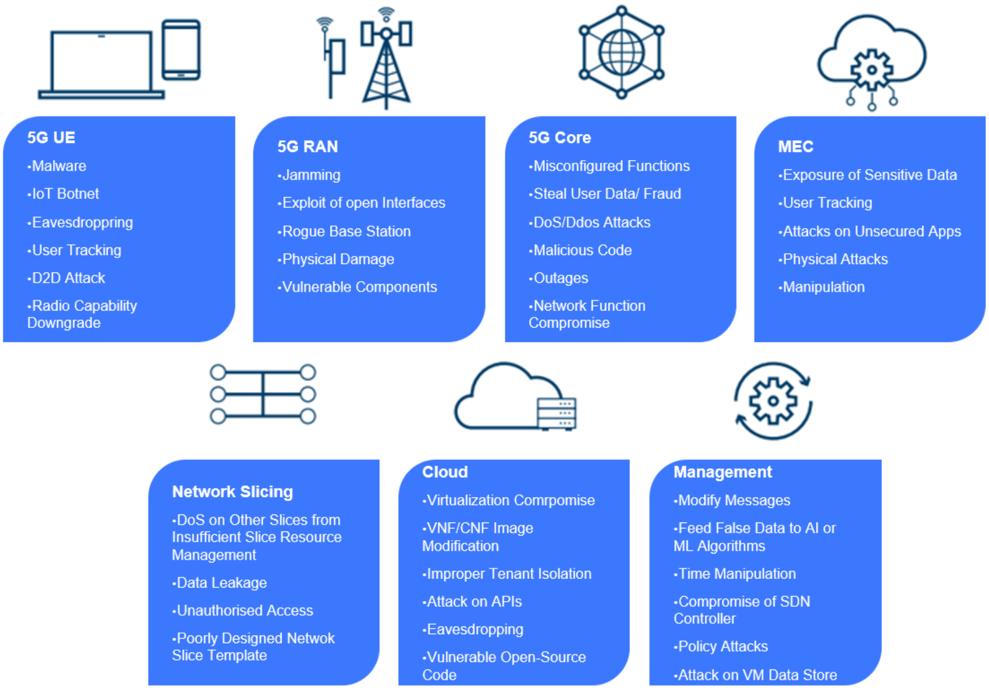


FIGURE 10. THREATS RELATED TO 5G SUBSYSTEMS, ENISA THREAT LANDSCAPE FOR 5G NETWORKS

5.2 Multi-Access Edge Computing Related Cybersecurity Risks

According to the network architecture and the use case specificity, both the smart seaport and smart road transportation use cases will rely on multi-access edge computing technology due to the demand for reliable low-latency data exchange and extensive processing. For smart road transportation, there is evident need for ProSe device-to-device communication relying on a PC5 link channel. When relying on MEC technology, a variety of risks in addition to generic 5G network-related risks need to be taken into account to ensure a high level of security. As for the MEC technology, the computational part, i.e. real-time safety camera stream processing, will move closer to the user and occur at the edge of the network, and third-party attacks and threats can be directly linked to the vehicles and equipment that are used for the transportation of military assets. Therefore, at every stage of the value chain, certain types of risks that can harm both the systems, monitor the movement, or even damage the assets, need to be evaluated. Below is a list of detailed vulnerabilities relevant to MEC.[46]

- Improper mechanisms for monitoring, collecting, and storing secure data and transmitting data between devices, which lead to unauthorised access to data and potential fraud committed by the attackers.
- Improper access control to information, where the MEC platform should only provide the mobile edge application with authorised information. If the platform is not secured properly, unauthorised parties can access secure data and confidential information.
- Lack of or improperly implemented DDoS protection. Due to the distributed nature of edge computing deployments, appropriate DdoS mechanisms may be impractical to deploy. Alternative protection mechanisms, therefore, need to be implemented to deter attacks. In the case of a DdoS attack, the attacker can shut down the whole system and halt or alter the convoys transporting the military assets.
- Improper isolation of resources whereby both physical and logical resources should not be shared with other parties/components which have different level of criticality. This means there should be a different level of criticality and security for military-related activities in transportation cases, otherwise there is a high risk of unauthorised access, interception, and eavesdropping by attackers.
- Improper physical and environmental security of edge computing facilities. Edge computing facilities are, by their nature, seated in locations distributed geographically. Normally, the first choice will be communications shelters already operated by the MNO. While communications shelters have physical security controls in place, these are calibrated to risks associated with the communication equipment. Improper security can lead to the destruction of edge computing facilities, causing the connection to shut down and may lead to unlawful interception or loss of data.
- Vulnerabilities in MEC applications that may be used as an entry point for attacks aiming to exploit the virtualisation environments, provide unauthorised access to data, elevate privileges or bring about denial of service, potentially halting equipment loading in ports or halting the platooning convoys on roads.
- Use of a system function without successful authentication based on the user identity and at least one authentication attribute (e.g.

[46] European Union Agency for Cybersecurity (ENISA), 'Threat Landscape for 5G Networks', https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/.

password, certificate) opens up opportunities for exploitation and limits accountability, which can lead to information leakage to the attacker regarding the equipment being transported or the location and route of the convoys.

- Security log troubleshooting failure where compromised VNFs are used to generate a massive amount of logged data on the hypervisor, overriding the initial and relevant log entries and making the analysis of logged data futile.
- Software vulnerabilities: Execution of code that exploits existing vulnerabilities on running software and flaws within the MEC system such as buffer overflow. Data overflow can cause unpredictable changes in the system that can potentially halt the military use cases, causing shutdowns in ports and in convoys.
- Data exfiltration/destruction where the data from a compromised entity is transferred or destroyed without the required authorisation, affecting the system backend and necessary documentation.
- Malicious code injection where a malicious piece of code is injected into an active service by the attacker, or an executable file being transferred causing a loss of system integrity, availability, and confidentiality of data.

All relevant stakeholders, including NATO and the military, need to take into account the multiple risks that arise with MEC technology. As this report demonstrates, NATO countries need to deal with continuous risk assessment about vulnerabilities, threats, and the high risks associated with untrusted 5G vendors, technology, and infrastructure. Improper system design and lack of continuous risk monitoring leaves an open gap for potential attackers to penetrate systems and get access to high-confidentiality military data and potentially damage military assets when equipment is being unloaded in ports or transported via road.

The following chapter proposes multiple mitigation measures for cybersecurity related risks, which if followed, can significantly decrease the potential of malignant attacks on military infrastructure and assets.

5.3 Cybersecurity Related Risk and Threat Mitigation Measures

Cybersecurity solutions require collaboration between different actors and understanding of the system and data flows, not only between automated equipment but also to computationally and power limited IoT sensors, site operations centres and control centres for remote management and tele-operations. To define efficient mitigations for the cybersecurity threats to transportation solutions, threat modelling is the key. With the continuous 5G roll-out plan already at the system design phase, the solutions need to follow the ‘secure by design’ principle. Efficient end-to-end security control on 5G infrastructure should be realised through continuous vulnerability assessments and mitigation solutions applied to the components/systems at risk.

In addition, efficient end-to-end security controls on the infrastructure and the network itself should be realised through continuous vulnerability assessments and mitigation solutions applied to the system. Figure 11 shows the relationships between threat actors, cybersecurity risks and the systems/items at risk.

The European Union has released a toolbox called ‘Cyber security of 5G networks – EU Toolbox of risk mitigating measures’[47] providing recommendations that can also be applicable to secure military movement related information. The objectives of this toolbox are to identify a possible common set of measures to mitigate the main cybersecurity risks of 5G networks, and to provide guidance on

[47] ‘Cyber security of 5G networks – EU Toolbox of risk mitigating measures’, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468.

prioritising measures in mitigation plans at a national and European Union level.

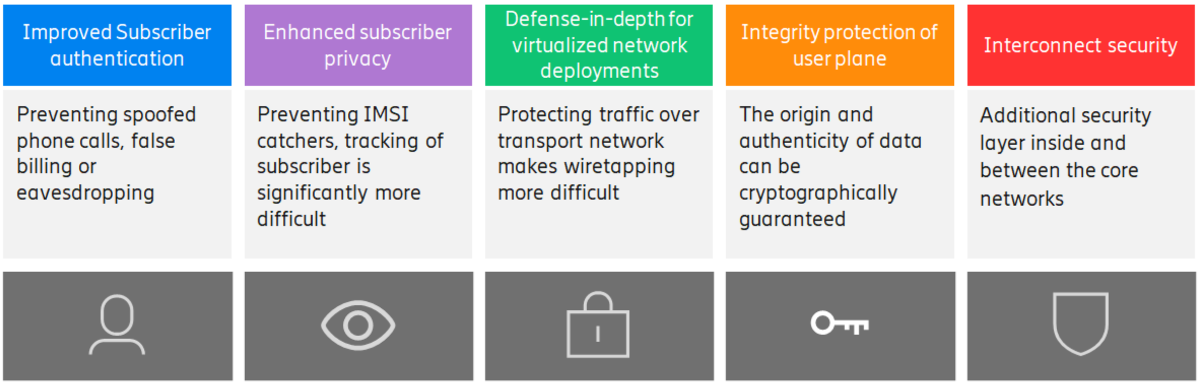
In the following chapter, insights on risk mitigation solutions are provided from the following perspectives:

- mitigation through compliance with global security standards;
- mitigation through holistic end-to-end security management;
- mitigation by securing the digital infrastructure supply chain.

5.3.1 Compliance to Global Security Standards

To ensure the security and safety of both the military assets and information related to the military movement, the system and processes need to follow and comply to relevant security standards. The 5G security architecture, as defined by 3GPP,[48] comprises security solutions from several different standardisation organisations: the Internet Engineering Task Force (IETF[49]) defines security protocols such as Internet Protocol Security (Ipsec), Extensible Authentication Protocol (EAP), and Transport Layer Security (TLS) which are incorporated into the 5G security architecture. A 5G network is built using cloud and virtualisation technologies, and ETSI ISG NFV[50] defines security for network function virtualisation.[51] Cryptographic solutions such as the Advanced Encryption Standard (AES) are standardised by the National Institute of Standards and Technology (NIST), and the recently approved Network Equipment Security Assurance Scheme framework (NESAS) for security assurance is a joint effort between 3GPP and GSMA.[52] All of these different components together form the security standard for 5G.

In the latest releases of the 3GPP 5G security standards, improvements have been introduced to provide the 5G system architecture with the needed flexibility, security, and dependability tailored for specific industries with mission-critical demands such as seaports. Figure 11 gives a summary of the security improvements defined by 3GPP for 5G release 15.



Improved Subscriber authentication

Preventing spoofed phone calls, false billing or eavesdropping

Enhanced subscriber privacy

Preventing IMSI catchers, tracking of subscriber is significantly more difficult

Defense-in-depth for virtualized network deployments

Protecting traffic over transport network makes wiretapping more difficult

Integrity protection of user plane

The origin and authenticity of data can be cryptographically guaranteed

Interconnect security

Additional security layer inside and between the core networks

FIGURE 11. 3GPP SECURITY IMPROVEMENTS FOR 5G

[48] 3GPP TS 33.501, 'Security architecture and procedures for 5G system', https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h50.zip.

[49] Internet Engineering Task Force (IETF), https://www.ietf.org/.

[50] ETSI ISG NFV: the European Telecommunications Standards Institute (ETSI), Industry Specification Group (ISG), Network Function Virtualization (NFV).

[51] '**Error! Hyperlink reference not valid.**Network Functions Virtualization (NFV)', Ericsson, https://www.ericsson.com/en/nfv.

[52] Global System for Mobile Communications, GSMA, https://www.gsma.com/.

5.3.2 End-to-End Security Management

For mission-critical communication networks, the full end-to-end approach must be taken to mitigate security threats. Misconfigured devices or insecure settings may allow hackers to gain a foothold in the network, from which they can move laterally, infiltrate valuable data and establish command and control channels. Devices used in the seaports or platooning use cases increase the attack surface. Therefore, every time a new device is added to the network, it must be provisioned by a set of standards and processes, secured, and managed. Furthermore, it must be kept in mind that V2X hardware components like IoT modules, and handheld devices of VRUs can be physically hacked. Therefore, disabling certain (V2X) services is essential for military transportation use cases performed by civil vehicles.

As shown in Figure 12, the security architecture for the digital infrastructure of transportation solutions must be managed end-to-end.

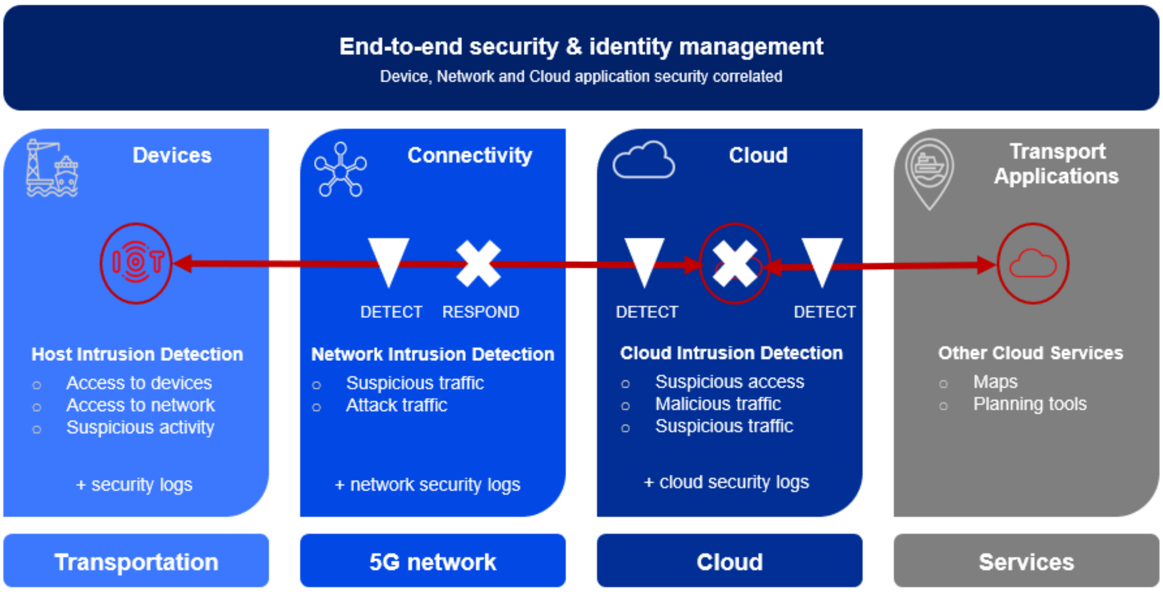


FIGURE 12. END-TO-END SECURITY & IDENTITY MANAGEMENT FOR TRANSPORTATION USE CASES

Security functions such as encryption and integrity protection at the end points prevent malicious attacks like eavesdropping and data modification. 5G connectivity, including PC5, supports both required security features.

Security management allows continuous monitoring and reporting of the security status. Tools like automation and automated orchestration make security operations manageable. End-to-end security and identity management monitors the security of the devices, the network, the cloud, and the application services:

- → Identity and access management with zero-trust architecture, where from a security perspective, implicit trust between parties is eliminated and every step in the digital interaction is validated.
- → Security policy and compliance of each domain (devices, connectivity, and cloud). For each domain, security management monitors and audits security functions against defined security policy standards.
- → Risk, threat, and vulnerability management including monitoring of security functions (security logs) and performing analytics. Threat detection is carried out via intrusion detection systems for each domain.
- → End-to-end identity life cycle management, whereby identities can be used for security association between domains.

For 5G private networks used for smart logistics, for instance, for seaports and road transportation, network security automation is highly important and provides advantages in scaling the security. Security automation enables tailored security for different network slices targeting different industries including mission-critical enterprises like seaports.

Figure 13 describes how security automation can be achieved through risk orchestration. Security risk orchestration provides dynamic risk and trust management for the different domains of the digital infrastructure and is based on five main pillar security blocks: Identify (Risk), Protection, Detection, Response and Recovery. These pillars are considered best practice for managing cybersecurity risks and are referenced in the NIST cybersecurity framework, [53] described more thoroughly in Table 3.

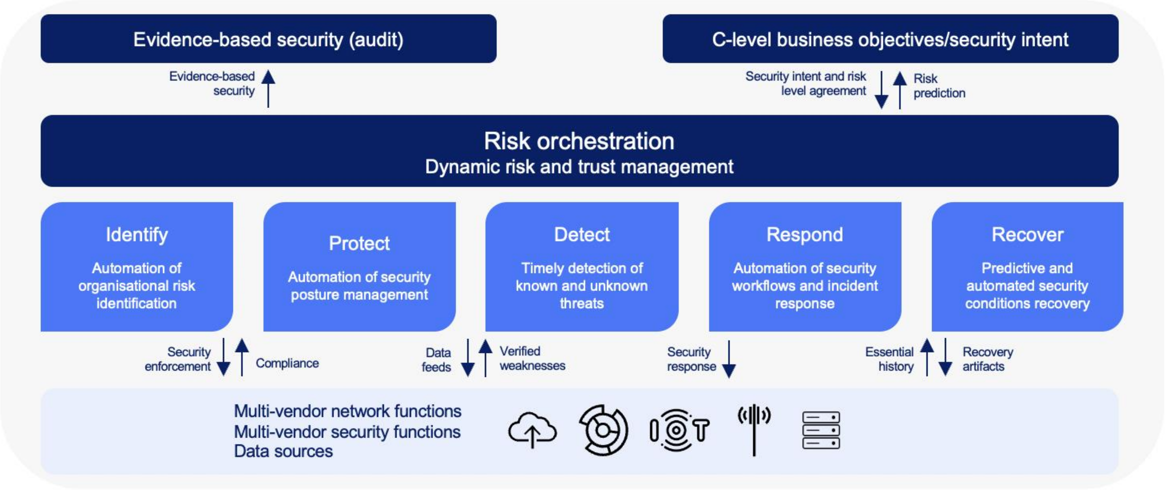

Evidence-based security (audit)
C-level business objectives/security intent
Evidence-based security
Security intent and risk level agreement
Risk prediction
Risk orchestration
Dynamic risk and trust management
Identify
Automation of organisational risk identification
Protect
Automation of security posture management
Detect
Timely detection of known and unknown threats
Respond
Automation of security workflows and incident response
Recover
Predictive and automated security conditions recovery
Security enforcement
Compliance
Data feeds
Verified weaknesses
Security response
Essential history
Recovery artifacts
Multi-vendor network functions
Multi-vendor security functions
Data sources

FIGURE 13. SECURITY AUTOMATION THROUGH RISK ORCHESTRATION

[53] NIST, 'Framework for Improving Critical Infrastructure Cybersecurity', Version 1.1, 16 April 2018, https://doi.org/10.6028/NIST.CSWP.04162018.

Table 3. Five main cybersecurity pillars

Identify	Cybersecurity is about cyber risk reduction, Thus, accurate risk identification from a safety and business perspective is essential for efficient allocation of resources. The identify function develops the organisational understanding to manage the cybersecurity risk to systems, assets, data, and capabilities.
Protect	Protection challenges are the introduction of dynamic and distributed networks in cloud environments. This challenge is solved with automation and security orchestration, where fit-for-purpose security policies are automatically set into the network infrastructure. Security policies ensure that the infrastructure has the desired and consistent security level across domains. This means policies enabling holistic security, e.g. identity and access security, data and traffic protection, and valid certificates. Furthermore, the automation ensures solid configurations of the network across domains, making intrusion or lateral movement for an attacker difficult.
Detect	Once the actual protection of the network is established, and under control, the focus moves to detection of threats and vulnerabilities. A vulnerability analysis is performed to verify the security characteristics and security configuration of the product/ solution and identifies new vulnerabilities through both black-box and white-box testing. Multiple tools and techniques can be used, such as vulnerability scanning, fuzzing and dynamic web application testing, and pen testing. Comprehensive security monitoring of both known and unknown threats with varying attacker tactics, techniques, and procedures is essential for keeping the network as secure as possible.
Respond	A successful security strategy must include detection of domain-specific threats and vulnerabilities followed by a response. Resources have the right domain knowledge to analyse threats at a deeper level based on data and insights from security tools, understand what is going on, and decide what actions need to be taken. Breaches and incidents also provide feedback to the security solution for continuous improvements, e.g. leading to new or enhanced security policies. To respond quickly, security automation needs to be integrated closely with network management platforms and network orchestration platforms including user plane monitoring (data monitoring) functions. The organisation also needs to have rehearsed digital forensics and incident response processes suitable for critical infrastructure with safety implications.
Recover	A recovery strategy helps an organisation to maintain or quickly resume its mission-critical functions after a disaster generally caused by a cyberattack. It is used to facilitate preventive planning and execution for catastrophic events that can significantly damage the infrastructure and the network assets. Predictive and automated security conditions recovery can significantly reduce the losses to critical systems that can be caused by cyberattacks and provide the system with the necessary resilience for operational continuity. Recovery processes and systems must be regularly tested especially against ransomware.

5.4 Trusted Supply Chain for Network and Infrastructure

It is of vital importance to develop and implement methods for comprehensive cybersecurity testing of the five pillars described above. The methods should be based on the new standards for cybersecurity engineering [54] and security for automated driving systems.[55] Trust in the supply chain is fundamental for building cybersecure solutions. All components must come from a trusted supply chain. This includes the 5G networks, the devices, and the applications used for operations of the smart seaport's digital infrastructure. End-to-end transparency throughout the supply chain is key for certification and compliance to regulatory security frameworks. This mitigation measure is built on regulations and recommendations set by NATO member countries, where specific components from certain companies or countries, or specific equipment itself is prohibited for use in 5G networks.

To address the risks relevant to the military movement scenario and the 5G use cases that the military will use both in smart ports and on roads, it is essential that safety must come first, in relation to people, processes, and technologies for cybersecurity management. This requires specific operational technology, cybersecurity practices, and adapted designs characteristic of the solutions. To achieve security in the transformation of the digital infrastructure, strategic objectives and tactical tools are recommended.

Based on the risk analysis done by Ericsson, the following steps are recommended when developing a 5G network and infrastructure for smart seaports and/or smart road systems:

→ **Develop a holistic end-to-end security model**

The number of incidents increases constantly, which means security must be made a priority. To tailor the prevention level to suit different use cases, granular detection solutions are needed to capture end-to-end security threats. Real-time network-based security detection and monitoring must be supported when developing the security model.

→ **Define a comprehensive cybersecurity strategy**

Automation of security management becomes essential, as manual handling of incidents would take too long time to provide effective mitigation. Whatever is possible to automate, should be automated. AI technologies will play an increased role in preventive detection.

→ **Define future proof technology requirements**

The 5G evolution of standardised network capabilities provides a scalable framework for future proof development. New technology capabilities must be easy to adopt by application developers. Adopting 5G for the digital infrastructure gives security 'by design' with built-in security functions including identity and access management via standardised interfaces and APIs.

→ **Design for zero-trust**

5G has built-in support for zero-trust architecture. It provides an identity for authentication and access control for authorisation. Device-to-device and many other access flows are by default blocked which limits attackers' capabilities to move laterally and get unauthorised access to network resources.

Both use cases described in this document need to be designed with a future evolution in mind to cater for future demands but at the same time handle

[54] ISO - ISO/SAE 21434:2021—Road vehicles—Cybersecurity engineering, https://www.iso.org/standard/70918.html?msclkid=675ec005c66b11ec8890a7e90ab8523a.

[55] ISO - ISO/AWI TS 5083—Road vehicles—Safety for automated driving systems—Design, verification, and validation, https://www.iso.org/standard/81920.html?msclkid=a490eee1c66b11ecb27bae63b072cf77.

potential disruption or avoidance of use for some use cases that will operate using public networks.

→ **Define trusted supply chain strategy**

All network products must be verified and tested to meet product security requirements. Verified suppliers of all components are essential for protection against supply chain attacks. Procurement of support services needs to be made with cyber threats in mind. Trusted partners that can manage the digital infrastructure are key to sustain seaport operations also in adverse conditions.

→ **Define and evolve the threat model to the specific needs**

Network and infrastructure owners need to be constantly aware of the changes in their specific threat landscape and update the cybersecurity defence accordingly. This includes understanding of specific or possible threat actors and their intents towards the infrastructure. For instance, defence against sabotage may be quite different to defence against espionage or ransomware. This links cybersecurity with the physical security as many attack vectors require physical access to devices or servers.

The described attack vectors above may hit any part of the digital infrastructure and information flows. That includes devices, communication infrastructure, and applications, as well as the wide-area connectivity (Internet) to cloud-based services. Prevention is central in any cybersecurity solution, and depending on the threat model, different levels of prevention will be chosen.

→ **Implement processes and operational instructions**

Network operations of critical infrastructure have several challenges. From a cybersecurity perspective, the digital infrastructure including networks, applications and suppliers must fulfil product security requirements. It is vital to include associated services for the digital infrastructure operations such as software upgrades, patch updates, and administrative services such as adding devices, network, and reconfiguration.

6. Recommendations

It is essential in cybersecurity management that security comes first in relation to people, processes, and technologies. This requires specific operational technology, cybersecurity practices, and adapted design characteristic of the solutions. By 2030, it is expected that 5G roll-out will be widespread and many new use cases will have emerged. Even if many industries see no potential in 5G applications, 5G networks will revolutionise our society, including the way we move military assets. Even though military movement will likely maintain a low level of adoption of direct use of 5G technology – automation and seamless data integration will still increase the speed, efficiency, and observability aspects of asset movements, and decrease maintenance costs and environmental impact. But if NATO member country militaries rely on civil third-party contractors for the movement of assets, the change towards 5G based solutions will happen one way or the other because civilian use cases will surpass the military with their level of 5G technology adoption. With these developments, major cybersecurity challenges will arise, and the value chain needs to take that into account.

6.1 Policies and Standards

Military and policymakers need to be knowledgeable about the possibilities of technology, including what 5G provides for military movement in the pursuit of closer cooperation on policies and standards. NATO will need to address the potential vulnerabilities of the new generation networks with a specific goal to assure that next generation networks will be secure. To ensure the interoperability and cyber safety of military-related use cases, NATO and EU member states should adopt policies and standards that are harmonised between countries related to approval and auditing of available hardware and software solutions used in private 5G networks. However, as NATO has no direct power over creating regulations and standards, certain favourable guidelines should be created directed towards member countries to implement within the jurisdiction of the National Regulative Authorities. As the created 5G network should be end-to-end secure by design, following internationally set standards, it is advisable that NATO jointly with EU authorities evaluate the feasibility of creation/use of trusted (virtual) mobile network operators for military transportation operations. As the big MNOs that are responsible for public 5G networks have considerable power over respective agencies and institutions responsible for creating the standards, NATO should be in close cooperation with different authorities and MNOs. It is feasible to develop European scale technical and legal solutions together with MNOs for on-demand deactivating of certain vulnerable ITS services during military movements. The specific vulnerabilities and risk levels must be identified through specific analysis and studies, possibly within EU research and development projects. All risks related to the implementation need to be considered from the start of the use case development phase. Even though the military is more conservative regarding changes to culture and operational practice compared to the commercial sector, technological developments will inevitably reach the operational phase.

6.2 System Security

To mitigate risks related to 5G system security, the interested parties, most notably NATO and EU member states, must be proactive in planning, be engaged in commercial development, as well as be stringent in monitoring and enforcement. These aims can be achieved through the following three recommendations:

DEVELOP A COMPREHENSIVE 5G CYBERSECURITY STRATEGY | As the military will interact with the rapidly developing 5G ecosystem, NATO will have to develop a comprehensive cybersecurity strategy by mapping out the various forms of interactions, corresponding risks, and adequate responses. In the strategy, all military movement needs must be identified, infrastructure enabling the movement must be mapped and its technological composition evaluated. Based on that mapping, all the opportunities and risks related to the intersection of future military movement and 5G development should be highlighted with recommendations developed by military and technological experts. The strategy would facilitate making Alliance-wide strategic decisions regarding 5G-use, including recommendations to private 5G network owners and intelligent transportation system providers. Given that security management will become essential in handling ongoing threats and risks, a proactive plan for the security management cannot be developed before a comprehensive cybersecurity strategy is in place.

ENGAGE IN BUILDING SECURE SYSTEMS AND 5G NETWORKS FROM THE BEGINNING | The commercial 5G systems that the military will interact with in the future are being built now. It is imperative that these systems and 5G networks are being built in a secure manner from the start. NATO, in close cooperation with the EU member countries and their regulative authorities, should take a proactive stance in the development process and strongly recommend certain guidelines to its commercial partners regarding the military-related security needs both for vendors and MNOs. Shaping the development process to security priorities as it happens is more convenient and cheaper than coming up with risk management measures retrospectively in a reactive manner. For this, it would be advisable to create a list of security-approved 5G RAN devices or vendors at a national or EU level as it is possible industrial enterprises or even MNOs might not be aware of possible security issues for specific hardware components.

ADOPT STRINGENT MONITORING AND SECURITY ENFORCEMENT PROCESSES | When fully operational, all relevant parties need to run frequent and structured risk analysis to assess the security of the systems and to avoid any potential risks or threats that might arise. Upon the installation or design of the system, the underlying report can be used for auditing purposes if all the necessary steps have been followed (see Chapter 5.3). As NATO will be relying mostly on the private sector, companies as logistical partners are strongly advised to follow policy recommendations as collectively agreed in NATO and in cooperation with the EU. For that, the NATO Standardization Office could be responsible developing such requirements. The first step of which would be to consider how the current 3GPP standards address the security requirements of the military. NATO Allies should cooperate in assessing and certifying hardware and software products, processes, and services associated with 5G technology according to jointly agreed criteria, consider the existing certification schemes, and assess their value and sufficiency. Upon the completion of the requirements, companies should be encouraged to meet a set of standards in order to provide any services to NATO related military movement. This also means that NATO should provide the guidelines to and lobby national governments who will need to be active in communicating and monitoring the fulfilment of these requirements.

6.3 Recommendations Related to Use Cases

Based on the case studies of smart seaports and road transportation presented, the 5G-enabled use cases carry both increased opportunities as well as risks. Therefore, for each use case, the military must (in the previously suggested cybersecurity strategy) conduct a systematic and professional risk analysis weighing the potential advantages of technology adoption against the disadvantages of increased risk. The risk analysis must conclude where the advantages outweigh the disadvantages, or the upside is high enough to take on the downside risk. It is not predicted that dedicated military vehicles will extensively interact over 5G networks in given timeframe up until 2030. The risks are related to services provided by civil infrastructure – both at ports and on roads – and contracted vehicles. Having said that, the current analysis concludes with the following recommendations for supply chain security of the two case studies.

SMART SEAPORTS | Based on technological and economical needs, the allied forces are recommended to use smart seaports that are using closed private 5G networks that are separate from the public 5G infrastructure or, at least, use the advantages of network slicing provided by 5G technology. Private networks allow for increased security and help control data retention and data sovereignty which further mitigates potential risks and threats relevant to military movement. Due to specific needs for smart port automation and surveillance, certain interests may use ORAN network equipment, multi-vendor user devices, and open-source software. From one side, this creates opportunities for European SMEs, but it also introduces considerable security and privacy concerns, especially related to technologies of third countries. EU should set appropriate regional/national regulations relating to selecting and validating vendors and components for 5G private networks. Additionally, identifying protocols for periodic independent auditing procedures may be appropriate for specific installations depending on the risk analysis. Creating a set of unified requirements standards between NATO members that are targeted to port operators is further advised. These set criteria will serve as a basis to ensure the network safety in port territories. The use of separate private networks in ports is evident already in the current phase where the first 5G smart seaports are continuing with their roll-out.

SMART ROADS | In contrast, the smart road transportation use case will rely on 5G public networks due to practical feasibility. It is not realistic to create a separate network for military purposes or ITS applications in general. The main benefits for military transportation can be seen from the platooning application. An optimum balance between improved traffic safety and efficiency provided by the V2X and MEC and security concerns must be investigated, possibly at the EU level. With road transportation use cases operating using public networks, the military needs to consider the potential that in some cases certain applications should be disabled to avoid any potential information leaks or effects on transportation activities. Over the air reconfigurable cellular network user (IMSI) profiles provide sufficiently flexible control methods to disable more vulnerable services like roadside and pedestrian data exchange, broadcasting of V2V messages, and use of MEC applications. Technological mechanisms and legal frameworks to enable/upload secure or stealth cellular connectivity modes of 5G-enabled vehicles must be developed. Given that military movements are cross border movements and affect traffic safety, IMSI profile switching regulations should be agreed on at the European level.

6.4 Further Research

To further this research, this report suggests both exploring existing and creating new multinational and cross-organisational (including military–private interaction) pilot programmes, which would encompass co-development of 5G systems, use cases and evaluate particular vulnerability risks of smart transportation use cases, V2X and MEC applications use. Such pilots would serve as an effective way to gain practical expertise and develop broader rules, processes, and policies to help guide small and medium sized European enterprises in 5G technology development. In addition, this would also develop NATO’s organisational knowledge in working together with the private sector, allied countries, and academia to develop technological solutions which would have a value proposition attractive enough for both the military and its commercial partners.

7. References

- 3GPP TS 33.501. 'Security architecture and procedures for 5G system'. https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h50.zip.
- 3GPP, H. Seo (rapporteur). 'TR 36.885 "Study on LTE-based V2X Services (Release 14), 3GPP Technical Specification Group Radio Access Network", V14.0.0' (2016).
- 5GAA, ed. T. Linget. 'C-V2X Use Cases Volume II: Examples and Service Level Requirements' (2020).
- Apostolos, P. and A. Khoryaev. 'Cellular V2X as the essential enabler of superior global connected transportation services'. *IEEE 5G Tech Focus* 1, no. 2 (2017): 1–2.
- Atlamazoglou, Constantine. 'The NATO rapid-response unit created after Russia's 2014 invasion of Ukraine is being activated for first-of-its-kind mission'. *Business Insider* (2022). https://www.businessinsider.com/nato-response-force-vjtf-first-defense-mission-russia-ukraine-2022-3.
- Brauss, Heinrich, Ben Hodges, and Julian Lindley-French. *Moving Mountains for Europe's Defense*. Washington DC: CEPA, 2021.
- Bundeswehr. '10 Armoured Division' (2022). Accessed 20 April 2022. https://www.bundeswehr.de/en/organization/army/organization/10-armoured-division.
- Center for Army Lessons Learned (US), 'Special Study: Strategic Landpower in Europe', no. 18-05 (December 2017). https://usacac.army.mil/organizations/mccoe/call/publication/18-05.
- Cornett, Aaron. 'Multinational Operations. JLSG offers effective role with allies, partners'. US Army, 2020.
- European Commission. 'Connecting Europe Facility'. Accessed 10 February 2022. https://cinea.ec.europa.eu/connecting-europe-facility_en.
- European Union Agency for Cybersecurity (ENISA). 'Threat Landscape for 5G Networks'. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/.
- Freedberg Jr., Sydney J. 'OMFV: The Army's Polish Bridge Problem'. *Breaking Defense* (2020). https://breakingdefense.com/2020/02/omfv-the-armys-polish-bridge-problem/.
- Global System for Mobile Communications (GSMA), https://www.gsma.com/.
- Hagström Frisell, Eva (ed.), Robert Dalsjö, Jakob Gustafsson, and John Rydqvist, *Deterrence by Reinforcement. The Strengths and Weaknesses of NATO's Evolving Defence Strategy*. Stockholm: FoI, 2019.
- Hirai, Takeshi and Tutomu Murase. 'Performance evaluations of PC5-based cellular-V2X mode 4 for feasibility analysis of driver assistance systems with crash warning'. *Sensors* 20, no. 10 (2020).
- Hodges, Ben, Tony Lawrence, and Ray Wojcik. *Until Something Moves. Reinforcing the Baltic Region in Crisis and War*. Tallinn: ICDS, 2020.
- Howard, Michael and Steve Lipner. *The security development lifecycle*. Vol. 8. Redmond: Microsoft Press, 2006. https://doi.org/10.6028/NIST.CSWP.04162018.
- Khan, M. Jalal, Manzoor Ahmed Khan, Azam Beg, Sumbal Malik, and Hesham El-Sayed. 'An overview of the 3GPP identified Use Cases for V2X Services'. *Procedia Computer Science* 198 (2022): 750–756.
- Khan, Rafiullah, et al. 'STRIDE-based threat modeling for cyber-physical systems'. *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe* (ISGT-Europe). IEEE (2017).
- Liu, Shaoshan, Liangkai Liu, Jie Tang, Bo Yu, Yifan Wang, and Weisong Shi. 'Edge computing for autonomous driving: Opportunities and challenges'. *Proceedings of the IEEE* 107, no. 8 (2019): 1697–1716.
- Miao, Lili, John Jethro Virtusio, and Kai-Lung Hua. 'Pc5-based cellular-v2x evolution and deployment'. *Sensors* 21, no. 3 (2021): 843.

- Nardini, Giovanni, Antonio Virdis, Claudia Campolo, Antonella Molinaro, and Giovanni Stea. ‘Cellular-V2X communications for platooning: Design and evaluation’. *Sensors* 18, no. 5 (2018): 1527.
- NATO, SHAPE. ‘NATO Force Integration Units (NFIU)’. Accessed 27 April 2022. https://shape.nato.int/operations/nato-force-integration-units.
- NATO. ‘Allied Joint Doctrine for the Conduct of Operations’, AJP-3, Edition C, Version 1, 2019, 2–11.
- NATO. ‘Allied Joint Doctrine for the Deployment and Redeployment of Forces’, AJP-3.13, Edition A, Version 1, 2021, 1–2.
- NATO. ‘Allied Joint Movement and Transportation Doctrine’, AJP- 4.4, Edition B, Version 1, 2013, 7–1.
- NATO. ‘Resilience and Article 3’. 2021. https://www.nato.int/cps/en/natohq/topics_132722.htm.
- NIS Cooperation Group. ‘Report on Cybersecurity of Open RAN’. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks
- NIST. ‘Framework for Improving Critical Infrastructure Cybersecurity’, Version 1.1, 16 April 2018. https://doi.org/10.6028/NIST.CSWP.04162018.
- Nokia. ‘LTE/5G pervasive industrial wireless and the digital transformation of port terminals’. https://wpassets.porttechnology.org/wp content/uploads/2021/11/18194220/Nokia_LTE_5G_for_port_terminals_White_Paper_EN.pdf
- Northcutt, Benjamin. ‘1st Armored Brigade Combat Team arrives in Europe in support of Atlantic Resolve’, *Sealift* (March 2019). https://issuu.com/militarysealiftcommand/docs/march_2019_sealift_issue_3_v2
- Northrop Grumman. ‘Global Combat Systems Support-Army (GCSS-Army)’. https://www.northropgrumman.com/what-we-do/land/gcss-army/.
- Port of Antwerp. ‘2021 Facts and Figures’. https://www.portofantwerp.com/en/publications/brochures/facts-and-figures-2021.
- Prohaska, Eleanor. ‘Parlez-Vous LOGFAS? U.S. and Allies Speak the Same Language When It Comes to Logistics’. US Army, 2021.
- Scaparrotti, Curtis M., Colleen B. Bell. *Moving Out. A Comprehensive Assessment of European Military Mobility*. Washington DC: The Atlantic Council, 2020.
- Think Defence. ‘Military Pallets, Boxes and Containers – Part 6 Aircraft Pallets and Containers’. 2014. https://www.thinkdefence.co.uk/2014/11/military-pallets-boxes-containers-part-6-aircraft-pallets-containers/.
- UK Army. ‘3 (UK) Division. 12 Armoured Brigade Combat Team’. Accessed 22 April 2022. https://www.army.mod.uk/future-army/unit-details/3-uk-division/12-armoured-brigade-combat-team/.
- UK Ministry of Defence. ‘JSP886 Defence Logistic Support Chain Manual. Volume 3: Supply Chain Management. Part 7. Consignment Tracking’. [Archived].
- US Army Europe and Africa. ‘Atlantic Resolve’ (July 2021). https://www.europeafrica.army.mil/Portals/19/documents/Fact%20Sheets/AtlanticResolveInfographic.21.11.30.pdf?ver=zs-ekCq7l9DkTyTn-AIlkw%3d%3d.
- US Army. ‘21st Theater Sustainment Command’. Accessed 19 April 2022. https://www.21tsc.army.mil/.
- US Army. ‘United States Army Military Surface Deployment and Distribution Command’. Accessed 19 April 2022. https://www.sddc.army.mil/Pages/default.aspx
- Vilikanskytė, Milda. ‘Ekspertai: geležinkeliai karo metu – nepakeičiami, bet Lietuvos pajėgumai riboti [Experts: Railways are irreplaceable during war, but Lithuania’s capabilities are limited]’. LRT. 23 April 2022. https://www.lrt.lt/naujienos/eismas/7/1677306/ekspertai-gelezinkeliai-karo-metu-nepakeiciami-bet-lietuvos-pajegumai-riboti.
- Xiong, Wenjun and Robert Lagerström. ‘Threat modeling—A systematic literature review’. *Computers & Security* 84 (2019): 53–69.