CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

Securing 5G Communication in Joint Operations Between NATO Partners

Bruno Dzogovic
Research Scientist / Associate Professor
Telenor ASA / Oslo Metropolitan University
Research & Innovation Department / Department of Computer Science
Oslo, Norway
bruno.dzogovic@telenor.com
bruno.dzogovic@oslomet.no

Silke Holtmanns
Telecommunication Security Expert
Helsinki, Finland
silke@holtmanns.eu

Abstract: NATO considers 5G a "priority area" and the NATO Communication and Information Agency has identified four key areas for the usage of 5G in defence. Currently, each NATO member and defence company has its own approach to using 5G, but it is clear that the defence sector will have to cooperate with public network operators. When using 5G in joint NATO activities, it is important to consider the 5G security approach of each allied partner.

A NATO 5G slice is one promising approach to facilitate cooperation among partners across countries and regions. Commonly, personnel who attend missions in other countries use roaming services. This may expose sensitive and classified information to third parties. Slicing can take place at the application layer, radio access network, core and/or transport level. We will describe the security trade-offs, including roaming and possible improvement approaches, based on the example of a joint NATO operation using 5G slicing. But 5G slicing is only one approach to improving the security of a joint operation. Other approaches include local private networks.

Private networks perform excellently in terms of flexibility, privacy, backhaul usage and reduced network administration. Therefore, military units can use private 5G deployments to connect battlefield units to Command & Control centres and share information among allied parties. This and the various technologies available (e.g., permanent identity protection, legacy usage, shared infrastructure and 5G security

feature usage) have a strong impact on the security and flexibility of the use of 5G in defence.

We will discuss the technology options and their realistic security and practical impacts. Many of those security aspects will be under the control of a public operator, not NATO.

Keywords: *5G security, slicing, joint operations*

1. INTRODUCTION – 5G IN DEFENCE

With the advent of 5G in the industrial and commercial sectors, many verticals have reaped the benefits of advanced connectivity. Be it the Internet of Things, sensors, fixed or mobile broadband, or other entities, industries are witnessing a wide range of applications being introduced into production, commercial operations, or research and development.

The defence sector too is expressing interest in the broad palette of advancements the 5G ecosystem offers. 5G can be customized for specific use scenarios – it offers broadband, low latency, high reliability and support for a large number of connected devices and sensors. With the potential to employ private mobile communications, the military can now deploy non-public 5G independent of mobile network operators or in conjunction and collaboration with them in what the 3rd Generation Partnership Project (3GPP), which defines telecommunications standards, calls a public network integrated – non-public network (PNI-NPN). NATO considers 5G and 6G a "priority area" and an "emerging and disruptive technology" [1].

There is a wide range of potential defence use scenarios, but the NATO Communications and Information (NCI) Agency has identified four key areas [2]:

1) Deployable communications and information systems (CIS) for expeditionary operations
2) Tactical operations
3) Maritime operations
4) Static communications

The NCI is now supporting the NATO Headquarters Consultation, Command and Control (C3) staff [3] and the Allied Command to:

1) formulate a consolidated strategy to create awareness and exercise influence on the civilian-led 5G ecosystem (specifically, influencing 5G standardization) and
2) investigate the benefits and enablers of 5G for military operations as well as to develop and validate concepts for NATO capabilities and drive digitalization in NATO, including the latest developments such as open radio access network (O-RAN).

These strategic considerations now need to be mapped against practical use and deployment.

In Section 2, we will dive into the practical use of 5G in defence, what we can expect in terms of use scenarios and what a joint operation might look like. Section 3 is about mobile technologies, how they work and what security they offer (e.g., 5G slicing). Section 4 tackles how security can be ensured in defence scenarios. Some of these methods are technical, while others are contractual. Section 5 applies the knowledge from Section 4 to the example of a joint operation. Section 6 summarizes this article.

2. PRACTICAL USE OF 5G IN DEFENCE

A. Use Scenarios for 5G in Defence

Defence system manufacturers usually focus on the use of 5G as a communications channel to a local command and control centre, as part of a CIS. But the strength of the NATO alliance lies in its cooperation, which implies that 5G technology is used by different partners, in different countries and in different ways. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) studied [4] the different use scenarios and identified potential risks of using 5G to support military movements in a joint operation.

Defence system vendors started creating 5G prototypes for various scenarios. Mobile network-enabled drones are now common [5] and are an important tool for both sides in the Ukrainian war. Here, even the choice of the subscriber identity module (SIM) card becomes a strategic question [6]. A Ukrainian SIM card allows the drone to operate in areas that only have Ukrainian mobile network coverage, thus bypassing some protection mechanisms Ukrainian mobile network operators have put in place [7]. 5G applications are being used in unmanned ground vehicles [8], local networks [9], maritime communication [10], aircraft [11], terrestrial trunked radio replacement [12], and more. Combining mobile 5G networks with satellite communication brings further potential benefits and use scenarios that are being actively researched [13], [14], [3] in the context of 5G advanced and 6G.

Many of the 5G usages in the defence sector are prototypes or testbeds. While they offer important lessons, typically, a proof of concept is created to explore the potential of a certain technology and evaluate its possibilities and usage. Security is rarely on the agenda for a prototype. 5G networks were not designed to meet defence security requirements, but now they are being used for such purposes.

Articles on 5G use in defence scenarios are often accompanied by a note of caution or questions about the resilience and security of the system. After all, 5G is an open standard with application programming interface (API) details published as part of the standards for civil use, not a secret proprietary technology for high-risk scenarios [15]. The defence sector is aware [16], [17] of the general security challenges related to 5G and is working to improve the situation. For example, funding has been provided for a challenge created by the NATO Defence Innovation Accelerator for the North Atlantic [18] to foster innovation and startups to create a security industry that ensures new emerging and disruptive technologies are secure.

B. Practical Considerations in Using 5G in Defence

In the past, security concerns focused on radio jamming and attacks using the interconnection network between mobile operators for spying attacks. The attack scenarios in 5G are now much more complex and diverse due to the evolution of technology that uses virtualization and the opening of public networks to partners. Each 5G defence use case has its own attack and risk profile, depending on the architecture and the nature of the usage. 5G brings many advantages in terms of high-speed, low-latency and secure communication. Nevertheless, these benefits must be balanced against security repercussions, which are of paramount significance.

There is substantial scope to implement 5G in non-public networks. Private 5G can be instituted for public protection, disaster relief and first responders amid catastrophic events that may impair the functioning of society. It can also be used in conflict and war when the military requires important communication resources to support the extensive range of military applications with adequate quality of service (QoS). Such private 5G applications can be deployed tactically, and so are valuable for the defence sector. Today, we already have QoS classes for emergencies. If a person establishes an emergency call and the network is congested, then another person is “kicked out” as the emergency call has higher priority.

One of the key features of 5G is the possibility to use commercial off-the-shelf user equipment (COTS UE) and standardized network functions. A major advantage of COTS UE is its reduced cost, which can substantially reduce overall military expenses in various scenarios. An example of successful COTS UE use in conflict [19] and war settings is in the Russo-Ukrainian war, where mobile communications have proven

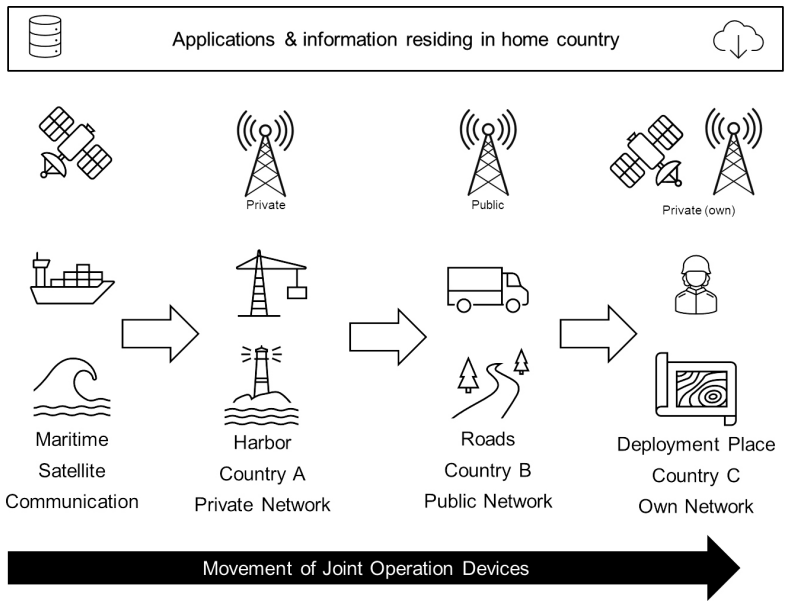
to be an efficient way to collect evidence and intelligence, and exchange tactical information between troops and command centres, providing location services, the ability to stay informed on the battlefield and even performing counter-intelligence operations.

C. Joint Operation Usage Scenario

The scenario we will use to study 5G's security impacts and their solutions is a joint operation strongly aligned with the CCDCOE report [4]. The joint operation has participants from various countries who will bring devices such as unmanned vehicles, phones, and drones with embedded SIMs that belong to different networks. We assume that the devices and the SIM cards are 5G-enabled.

In our scenario, the devices arrive on a ship in country A at a local harbour with a private network and then cross the border into country B by rail or road. The devices reach the site of deployment in country C, where they interact with applications in their home country as well as with partners and their devices from other countries. The partners' devices also potentially use applications in their country of origin (see Figure 1).

FIGURE 1: 5G DEFENCE SCENARIO FOR JOINT OPERATION



3. MOBILE NETWORK TECHNOLOGIES

In our scenario, the device arrives first at the harbour's private network (also called a dedicated or non-public network). Let us assume that it is a 5G network that offers "guest access" to the harbour's customers. After this, the device may temporarily connect to a public network while on the road or rail. That public network could be a long-term evolution (LTE) network (4G), a 5G non-standalone (NSA) network, a 5G standalone (SA) network or a 5G SA network that supports network slicing. The device then crosses the border into country B and switches to a different public network.

We face the following technology challenges in this scenario:

- 4G and 5G interworking network architectures
- SA and NSA networks
- Networks with slicing support and ones with no slicing support
- Private networks and public networks

A. 4G versus 5G

The device may connect to a legacy public network (4G LTE network) when it leaves the harbour. 4G networks have a consumer market-focused security approach. The 4G network itself is considered a security zone whose main security perimeters are the air interface and, to some degree, the interconnection link to other mobile operators. The devices are authenticated, and in most countries, the confidentiality and integrity of the communication between the network and the devices is protected. But 4G does, in some cases, use a permanent international mobile subscriber identity (IMSI) over the air interface, which allows tracking of individual devices. This poses the risk of military equipment movements and potentially targeted strikes being monitored. Also, on the interconnection link, so-called Signalling System No. 7 (SS7) protocol or diameter protocol attacks can be used for location tracking, one-time password interception or data interception [20].

5G has improved security that prevents user tracking on the air interface [21]. While 5G has also improved the security of interconnection between operators, many challenges remain in that area due to intermediaries (interconnection providers, IPX) and the fact that commercial rollout of 5G APIs to operators is still not expected in the near future. Today, user traffic between public mobile networks is not cryptographically protected and passes several IPX providers between the visited mobile network operator and the home mobile network operator, raising questions about confidentiality. The routes of the traffic are usually determined by the cost of data transport. We will assume that

the roaming interface is not properly protected and that various threat vectors will potentially conduct attacks in the future.

B. SA versus NSA Network

Public mobile network operators in our scenario can deploy 5G in SA and NSA modes (i.e., a 4G core with a 5G radio network). In SA mode, that 5G new-radio access is deployed along a fully functional 5G core network, so the communication is considered exclusively 5G. SA mode does not support older devices with 3G and 4G LTE interfaces. It utilizes new types of universal SIM (USIM) cards to support its new security procedures. These new security procedures consist of subscription concealed identifier or subscription permanent identifier (SUCI/SUPI) key pairs that conceal the permanent identity (IMSI) of the user. An SA mode 5G network is required to provide high protection against IMSI catchers and location tracking, and so uses the SUCI/SUPI authentication enhancement.

The mobile operators in the home countries of the joint operation participants in our scenario may issue USIM cards that support 5G SA mode, or they may only issue legacy 4G USIM cards. It is worth noting that the new 5G USIM modules, which support SUCI/SUPI concealment, are backward compatible with 4G LTE networks and NSA modes of operation. Therefore, it is possible that some members of the joint operation are not protected against location tracking using IMSI catchers.

An NSA network comprises 5G base stations that are connected to a 4G or combined 4G/5G core network. An NSA network supports all devices and SIM cards, and operators may decide to gradually roll out 5G using the NSA infrastructure, which has the older authentication procedures and security features. This is done to support a wider range of devices. We expect that many operators support legacy cards through a combined 4G/5G core that lets them serve high-revenue inbound roamers. For the joint operation, it is important to understand what kind of air security the mobile operator of the connected network has and evaluate the risks.

C. Use of Slicing

Slicing is often seen as a solution to isolate sensitive customers inside the network [22]. A slice is a logical and potentially physical division of the network and its resources to provide a specific functionality or service, as in the case of the joint operation. Many parts of the network can be sliced [23]:

- **Device slicing** can be done on the modem, operating system or application level. Currently, we use modem-centric slicing, and this is not expected to change soon. Device slicing isolates information flows inside the device.

- **Transport network slicing** works inside of the mobile operator network. This is currently not common and could potentially be achieved through data network protocols [24], but discussions with progressive operators show that we cannot expect this to be widely supported. Manipulating transport networks dynamically requires substantial automation mechanisms involving software-defined networks (SDNs) and obtaining network intelligence for automatic management, reconfiguration and autoscaling.
- **Radio access network (RAN) slicing** is the most common form of slicing and if slicing is supported by an operator, it is often in the form of RAN slicing to serve specific customer segments with bandwidth- or latency-related QoS requirements. While this gives good availability and latency, and also offers isolation on the radio path of the communication, user communication in the core network is still unencrypted and not isolated between customers.
- **5G core slicing** provides the slice with a dedicated network function, but since most networks still use 4G nodes, 5G core slicing is not so common. To gain most of the benefits of slicing and automation at the core network, 5G infrastructure needs to be deployed in SA mode.
- **Roaming slicing** relies on common attributes as defined in GSM Association (GSMA) specification NG.116 [25] and end-to-end slicing agreements between operators that follow NG.135 [26]. While there is some guidance, we expect there to be many non-standardized variants in the future due to the variety of use cases.

  The different slicing options have different market penetration and security trade-offs as described in Table I.

TABLE I: 5G SLICING OPTIONS AND IMPACTS

	Device slicing	Transport network slicing	RAN slicing	5G core slicing	Roaming slicing
Market	Not available	Not available, but technically possible	Most common type of slicing	Not widely available	Not available commercially
Security trade-offs	Complex implementation in the device	Expensive for operator, especially if no return on investment	Medium complexity	Legacy core elements cannot be used; expensive for operator	Impacts roaming networks all over the world
Security gain	Isolation against other device applications	Isolation against other data flows on transport layer	Isolation on air interface	Isolation against other customers	Isolation independent of network (if properly standardized)

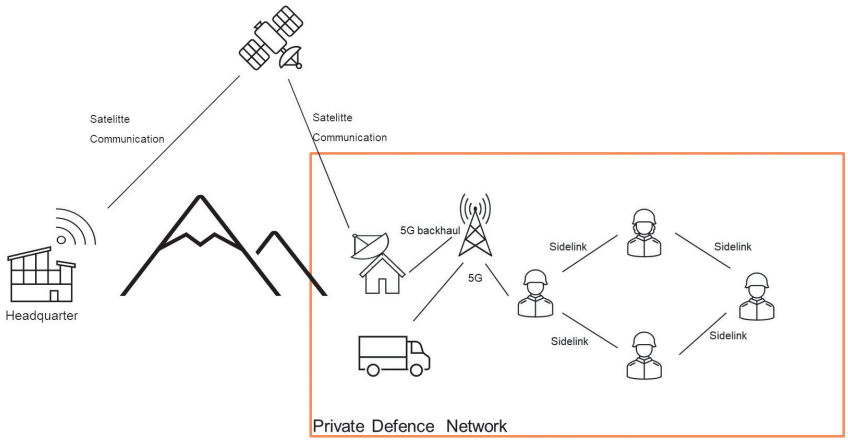
A combination of RAN and core slicing is sometimes called end-to-end slicing, but the term is used loosely. This slicing approach is not risk-free, especially if used in combination with legacy infrastructure [27], [28] or if no end-to-end slicing is considered. In those cases, no real end-to-end security can be guaranteed. In addition, 5G networks rely heavily on cloud and virtualization, which is a new technological leap for the telecommunications industry and poses a potential risk.

D. Private 5G Deployments

Private 5G networks can have different architectures. It can be a dedicated network that is not connected to any public mobile network operators, satellites or even the internet. This kind of dedicated network would be like an isolated bubble. The term dedicated network is also used for private networks that do not connect to any public mobile networks or satellites but do have a data connection to the internet. This form of internet-connected private network is the most common private network today, but it has the drawback that the connection is lost if the user is out of coverage of the private network.

In the joint operation, the devices that arrive at the harbour may use the guest access to the harbour's private network to connect to the internet and applications in their home countries (Figure 1). The joint operation may have its own dedicated network. In this dedicated private network, the ground forces may use 5G sidelink (direct link communication) and satellite communication to headquarters (HQ) (Figure 2).

FIGURE 2: PRIVATE DEFENCE NETWORK AT THE PLACE OF DEPLOYMENT



As an alternative to the satellite link, the private network can also be connected to a public mobile network to offer constant connectivity. This can be achieved either

through a dedicated virtual private network (VPN) or through a roaming connection and the interconnection network (IPX). In the first case, the "donating" public operator could offer roaming via its network, while in the second, the private network would be like any other public network connected to the IPX roaming network. If the private network is connected to the IPX like a normal public network, it can be targeted by SS7 attacks, which are common on IPX. If it is connected via a VPN, attacks may be executed via the "donating" operator.

In general, satellite communications are considered insecure. There are commercial devices that support direct satellite connections, and some operators use satellite communications for the link between the base station and the core (called backhaul) to connect base stations in remote areas. These non-terrestrial networks are an active standardization item in the 3GPP and a discussion of their security would need a separate article.

4. AVAILABLE SECURITY FEATURES AND THEIR USE

While there are many threat angles and risks to consider, there are also many countermeasures that can mitigate them. We will list a range of methods to reduce the risks for joint operations, but there is no silver bullet if existing public networks are used.

A. Protection Against Location Tracking on the Air Interface

Devices should support 5G and the SA mode, which ensures a device only connects to a network that supports the location, privacy and identity protection feature of 5G and safeguards against location tracking and identity theft through IMSI catchers. This prevents the use of disabled location privacy in cases of NSA deployments. There are initial devices [29] that allow explicit monitoring of whether 5G SA is used and restrict communication to the availability of the SA mode. This should be considered for the procurement of SIMs and embedded universal integrated circuit cards for military devices.

B. Protection Against Data Sniffing in the Core Network and Between Networks

Mobile data is secured on the air interface, but after that it is protected at best hop-by-hop between the various network elements. In many cases, such as NSA, 4G and non-5G roaming networks, the mobile data of the user will not in any way be protected between the network elements, which may even belong to different operators and might be routed through the territory of "unfriendly entities". Besides ensuring that the operator partners actually switch on their security features and protocols, application

or transport layer security (i.e., VPN, transport layer security version 1.3) is strongly recommended.

C. Protection Against Jamming and Advanced Interception Attacks

In the long term, we must study whether transmission security (TRANSEC) can be used for mobile network communications at the site of deployment. TRANSEC is a component of communications security and refers to the methods and measures implemented to safeguard communications against interception, cryptoanalysis and in general compromising factors that can help the adversary. The three key components of TRANSEC are:

- Low probability of interception
- Low probability of detection
- Resistance to jamming – electronic protective measures (EPM) and electronic counter countermeasures (ECCM)

By making the system emit lower electromagnetic signatures, it is possible to reduce the probability of communications detection and interception. The communications systems can be targeted by long-range means such as guided missiles, cruise missiles or artillery systems. Therefore, it is of prime importance to reduce the probability of the source of battlefield communications being detected, as the adversary can take advantage of this to intercept communications and engage in decryption or exploit various vulnerabilities in the system. It is possible to use electronic warfare, such as communications jammers, which emit a high-power signal, to jam the communications source and perform denial of service for battlefield communications. For that, the system should be designed with jamming resilience in mind, providing multiple mechanisms to mitigate threats of a similar nature. While TRANSEC provides many advantages, interoperability with public mobile networks and the COTS UE cost advantage might be lost.

D. Mobile Operator Partnering and Selection

Defence manufacturers often partner with mobile network operators [30]. Security should be seen as an integral part of such contracts. The mobile operator should adhere to best security practices. Besides enabling the technical features mentioned in the preceding sections, this could mean vetting the operator according to the 5G Security Control Matrix [31] and the 5G Toolbox [32], auditing its cloud infrastructure, enabling core network internal security, using interconnection firewalls with the latest threat intelligence, pen-testing (core, RAN, cloud, transport, external interfaces, roaming) the network, securing the supply chain, and ensuring a software bill of material is in place and that suppliers (e.g., cloud providers) adhere to highest security standards

and standardized secure software development practices for the entire lifecycle of their products.

The mobile operator should only use certified equipment. Alongside the 3GPP Security Capability Assurance Standards (SCAS) [33], several security certifications and regulations are available or are under development in the European Union that improve the security of 5G networks, such as the EU Cyber Resilience Act, NIS2, EU Common Criteria Certification, EU Cloud Services Certification and EU 5G Certification. They should ensure that the integrity of the subscriber profile is protected and should raise the alarm if sensitive parameters change in a way that might allow attacks (e.g., group memberships, data traffic or SMS/data redirects).

On an operational level, the partnering mobile operator should provide dedicated QoS classes for defence purposes. Potentially, different subcategories can be established depending on the defence situation. For joint operations, the path that the mobile data travels between the visited network and the home network of the device is important. The operator should ensure that the data only travels through friendly nations, ideally through direct connections. SDNs and suitable roaming routes can make this possible.

E. Use of Slicing for a NATO 5G to Extend Coverage and Availability

Private 5G can also be combined to use the public network to extend the connectivity and coverage. On site, the private network would be used, and outside it, the dedicated NATO slice of the public network would be used.

In PNI-NPN, the private component of the network can be controlled, managed and provisioned by the mobile network operator on behalf of the defence owner of the private 5G slice. The responsibility for the management of the PNI-NPN slice can be delegated to the entities involved from the private component of the network and the mobile network operator in parallel, based on a service level agreement (SLA). PNI-NPN mobility with public networks is a relatively new feature (Release 18) in 3GPP and might not be widely available for some time.

F. Use of Slicing Security

The GSMA specifies the "descriptors" of slices in their document NG.116 [26]. These descriptors (generic network slice templates) include attributes such as uplink and downlink bandwidth, as well as aspects such as isolation and 3GPP mission-critical service support. While some aspects are explained sufficiently, others are still slated "for further study", and some have not been considered at all.

For example, isolation can take place at the physical level, transport level, RAN level, core network (user and control plane) level and roaming level. In addition, the

isolation can be logical, through containers, ports and virtual machines, or physical, through different servers and infrastructure. Often when operators mention "slicing", the focus is on RAN slicing only, but that would not offer a sufficiently high degree of isolation for a NATO slice. These aspects are currently not defined and require further work. Aspects such as QoS, priority level and simultaneous use of the network slice attributes can be used to secure a NATO joint operation slice. A NATO slice should at least be logically isolated on the RAN and core network level. Physical isolation is expensive, and while isolation on the transport level is technically possible, general interest in it is currently low.

Security aspects, such as the granularity of OAuth tokens (down to the IMSI and slice level), are currently not part of NG.116. Classes for "legacy" are also not defined, so if a node or intermediate network does not support 5G slicing, it lowers the security level. Other features, such as UE route selection policy to ensure the special handling of defence traffic, would need to be supported by the operator for proper traffic isolation if modem-based device slicing is used.

Partnering public operators should discuss with NATO the required level of granularity and the security aspects, so that the right attributes can be defined in GSMA. General support for 5G protocols on the roaming interface is not expected in the near future. Measures such as end-to-end security between operators (i.e., not hop-by-hop) and "pinning" of routing through friendly nations could be part of a GSMA NG.135 [25] in the future. Currently, roaming routes are determined by factors such as costs and reliability but not security. NATO could consider different requirements for different confidentiality classes.

In their report [34] on network slicing, the US National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) describe key design criteria for network slices that can be combined with the aspects mentioned above to create a secure NATO joint operation slice.

G. Private Network Security Improvements

Mobile networks were not designed for military purposes; therefore, the security standards and processes are potentially not up to the level expected for military use. While there are standards to ensure a baseline degree of security for mobile networks, those standards do not cover all elements of the network and they are indeed only a baseline. Nevertheless, a private network used by the military should conform to the basic product security standards of 3GPP SCAS [33]. Any kind of self-declared security compliance from vendors should be validated either by the defence entities themselves or by an independent third party. The European Union has several good guidelines and documents to improve the security of public mobile networks, which

can be customized and applied to some degree to mobile networks used for defence (e.g., 5G Security Control Matrix [31], 5G Toolbox [32]). For private networks, the same certification considerations apply as for public mobile network equipment.

For mobility and extended coverage, a connection to a public mobile operator network is essential. Using a VPN in a direct link to an operator with good security measures reduces the risk of being attacked via IPX. The security measures of the mobile operator should be validated through compliance audits and an SLA, which should explicitly define the measures the operator must have in place (e.g., signalling firewall with threat intelligence, SIP firewall, cloud security controls, e.g., [35] / C5 [36] or similar compliance). Currently, standards such as C5 have been brought into NATO [37] to protect information. Up-to-date interconnection signalling firewalls are of special importance, as this is a commonly used line of attack today to track persons of interest.

Consequently, the zero-trust model should be considered a long-term goal over the standard perimeter security model. We think of 5G/6G infrastructure as a dynamic, heterogeneous network, and the complexity of such structures renders the perimeter model insufficient and obsolete. The dynamism and scalability of the next-generation networks require more stringent security measures, and thus the zero-trust paradigm becomes an important aspect of security considerations. The US National Security Agency and CISA described further the need for the zero-trust model to provide architectural specifications that introduce additional security layers for deployments that carry confidential traffic, noting that the capabilities and options for a network slice may vary by operator and this method does not address zero trust beyond the slice. A baseline of security-related network slicing features must be established for day-to-day operations. Those features must support confidentiality, integrity and availability requirements. The zero-trust architecture methodology can be implemented to ensure the secure activation, supervision, reporting, modification and de-activation of a slice [34].

5. SECURING THE PATH

Coming back to our example, how can our joint operation be secured? Before the joint operation takes place, we must ensure that the devices have enabled SA mode. A clear policy should be in place that clarifies the communication patterns, security requirements and matching classifications. Here we outline one way to secure the communications. There are many possible variations on this, and as technology and security features advance, better ways of securing the path will become possible.

The devices arrive at the harbour of a friendly country. That harbour has a 4G LTE network with internet access. Some devices are allowed to connect to it for low-security-classification communication. They use a VPN to connect to applications and communicate through the internet access provided by the harbour. Other devices with SA mode enabled note that this is a 4G network, which is prohibited by their policy, and so do not connect to it.

When leaving the harbour, the devices enter the coverage area of a partner public network operator that provides a specific QoS and a dedicated slice in a 5G SA network for the joint operation. This operator also has a sufficient level of security, ensured through an SLA according to the suggestions made above, and has also been audited to ensure the deployment of those security features. The devices connect to this public network slice, and the connections are additionally secured with application and transport layer security.

When arriving at the place of deployment, the ground troops and devices use a private network and direct device-to-device communication – a new radio sidelink or PC5 link (sometimes called direct communication). As far as technically feasible, the devices use TRANSEC. This private network is owned and operated by the joint operation defence team. The private network connects to a communications satellite to link with HQ and has additional security measures as the satellite link is not considered secure.

6. CONCLUSION

A joint operation that uses 5G will face many security challenges. The use of 5G in defence needs to be planned carefully. 5G was designed for civilian use, and the standards and guidelines provide only a limited level of security. But for the defence sector, clear guidance from NATO members on the security expectations and the related use is paramount. The risk involved in each approach needs to be studied and mapped against the NATO security classifications and use. Detailed SLAs with operators and cloud partners need to be created to ensure secure interworking and use of public networks and managed private networks.

Slicing offers some degree of isolation and security for a joint operation, but it requires very specific security support from the mobile network operator hosting the slice. Many of the required security features and slicing attributes are not yet widely available or commonly supported by public mobile networks. The availability of those features depends strongly on market demand and the return on investment. Many mobile operators act when they see a clear market need. This is also true for

the security requirements of the defence sector. Cooperation with mobile operators to work on those features jointly would potentially improve availability.

Other useful security features are still not fully standardized, and the standardization process would benefit from concrete inputs from the defence sector on their requirements to enable the production of standardized, economical COTS UE that can be used in sensitive and high-risk environments. We did not discuss O-RAN in this article, as a proper security discussion of O-RAN in defence would require a separate article due to the complexity of the ecosystem. Many challenges remain for 5G, such as missing standardized features, support from operators, example contracts and security measurement performance indicators, but if 5G for defence wants to use public standards and public networks, those challenges must be addressed.

REFERENCES

[1] "Emerging and disruptive technologies". NATO. Accessed: Jun. 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_184303.htm#policy

[2] NATO Communications and Information (NCI) Agency. "NATO tech Agency explores the potential of 5G for the Alliance". NCIA. Accessed: Jan. 2021. [Online]. Available: https://www.ncia.nato.int/about-us/newsroom/nato-tech-agency-explores-the-potential-of-5g-for-the-alliance.html

[3] G. Capela, "NIC Agency Update on 5G Work", *NITECH NATO Innovation and Technology Journal*, no. 9, pp. 88–89, July 2023. [Online]. Available: https://issuu.com/globalmediapartners/docs/nitech9_-_full_pdf_final?fr=xPf81NTU

[4] V. Oeselg et al., *Research Report Military Movement Risks from 5G Networks*, Tallinn: NATO CCDCOE, 2022. [Online]. Available: https://ccdcoe.org/library/publications/research-report-military-movement-risks-from-5g-networks/

[5] "Lockheed Martin, Verizon demonstrate 5G-powered ISR capabilities for Department of Defense". Lockheed Martin. Accessed: Sep. 2022. [Online]. Available: https://news.lockheedmartin.com/2022-09-28-Lockheed-Martin-Verizon-demonstrate-5G-powered-ISR-Capabilities-for-Department-of-Defense

[6] E. Priezkalns. "Russian attack drone had Ukrainian network SIM for guidance or remote control". Commsrisk. Accessed: Dec. 2023. [Online]. Available: https://commsrisk.com/russian-attack-drone-had-ukrainian-sim-believed-to-have-been-used-for-guidance-and-control/

[7] C. McDaid. "The mobile network battlefield in Ukraine—Part 1". ENEA. Accessed: Mar. 2022. [Online]. Available: https://www.enea.com/insights/the-mobile-network-battlefield-in-ukraine-part-1/

[8] "Protected mobility and defence systems autonomous systems". Patria Group. Accessed: Dec. 2023. [Online]. Available: https://www.patriagroup.com/products-and-services/protected-mobility-and-defence-systems/autonomous-systems

[9] P. Tucker, "The US Navy is testing 5G for future forward operating bases". Defense One. Accessed: Jul. 2022. [Online]. Available: https://www.defenseone.com/technology/2022/07/navy-testing-5g-future-forward-operating-bases/375164/

[10] "LMT, RBF to bring maritime 5G to the Baltic Sea". RCS Wireless News. Accessed: Jun. 2022. [Online]. Available: https://www.rcrwireless.com/20220615/5g/lmt-rbf-to-bring-maritime-5g-to-the-baltic-sea

[11] "Lockheed Martin, AT&T demonstrate 5G high speed transfer of Black Hawk data to 5G.MIL® Pilot Network". AT&T. Accessed: Sep. 2022. [Online]. Available: https://about.att.com/story/2022/5g-lockheed-martin.html

[12] M. Pulliainen, "Virve hyppää 5g-aikaan: Viranomaisten laajakaistaisen mobiiliverkon käyttöönotto alkaa 2022". Tekniikka & Talous. Accessed: Dec. 2021. [Online]. Available: https://www.tekniikkatalous.fi/uutiset/virve-hyppaa-5g-aikaan-viranomaisten-laajakaistaisen-mobiiliverkon-kayttoonotto-alkaa-2022/a3f260b0-0129-40f0-8d45-b284ce0b6951

[13] "Features of 5G from space". Lockheed Martin. Accessed: Dec. 2023. [Online]. Available: https://www.lockheedmartin.com/en-us/products/5g-from-space.html

[14] M. Alleven, “Ericsson, Qualcomm test space-based 5G with Thales”. Fierce Wireless. Accessed: Jul. 2022. [Online]. Available: https://www.fiercewireless.com/tech/ericsson-qualcomm-test-space-based-5g-thales
[15] M. DeGrasse, “5G for defense: U.S. military wants open interfaces, compact infrastructure”. Fierce Wireless. Accessed: Mar. 2023. [Online]. Available: https://www.fiercewireless.com/5g/5g-defense-us-military-wants-open-interfaces-compact-infrastructure
[16] S. Aken. “What does the military’s move to 5G mean for security?” Spiceworks. Accessed: Jul. 2022. [Online]. Available: https://www.spiceworks.com/tech/networking/guest-article/what-does-the-militarys-move-to-5g-mean-for-security/
[17] “Report on national security implications of 5G networks”. US Naval Institute. Accessed: Mar. 2023. [Online]. Available: https://news.usni.org/2023/03/17/report-on-national-security-implications-of-5g-networks-2
[18] “NATO’s innovation accelerator becomes operational and launches first challenges”. NATO. Accessed: Jun. 2023. [Online]. Available: https://www.nato.int/cps/en/natohq/news_215792.htm
[19] K. Freese, “Tradoc: Smart phones playing prominent role in Russia-Ukraine war”. Operational Environment Enterprise. Accessed: Aug. 2023. [Online]. Available: https://oe.tradoc.army.mil/2023/08/10/smart-phones-playing-prominent-role-in-russia-ukraine-war/
[20] P. Donegan, “Threat intelligence in telecoms”. Harden Stance. Accessed: Jul. 2022. [Online]. Available: https://www.hardenstance.com/wp-content/uploads/2022/07/HardenStance-Briefing-Using-Threat-Intelligence-in-Telecoms-2022-FINAL-Subscribers.pdf
[21] P. K. Nakarmi, O. Ohlsson, and P. Hedman. “Fighting IMSI catchers: A look at 5G cellular paging privacy”. Ericsson. Accessed: May 2019. [Online]. Available: https://www.ericsson.com/en/blog/2019/5/fighting-imsi-catchers-5g-cellular-paging-privacy
[22] M. Malik, A. Kothari, and R. A. Pandhare. “Network slicing in 5G: Possible military exclusive slice”. International Conference on the Paradigm Shifts in Communication, Embedded Systems, Machine Learning and Signal Processing (PCEMS), June 2022. Accessed: [Online]. Available: https://ieeexplore.ieee.org/document/9807927
[23] CISA. “5G network slicing: Security consideration for design, deployment and maintenance”. U.S. Department of Defense. Accessed: Jul. 2023. [Online]. Available: https://media.defense.gov/2023/Jul/17/2003260829/-1/-1/0/ESF%205G%20NETWORK%20SLICING-SECURITY%20CONSIDERATIONS%20FOR%20DESIGN,%20DEPLOYMENT,%20AND%20MAINTENANCE_FINAL.PDF
[24] A. Farrel et al. “A framework for network slices in networks built from IETF technologies”. Internet Engineering Task Force (IETF). Accessed: Oct. 2023. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-teas-ietf-network-slices/
[25] GSM Association (GSMA), “NG.135 E2E network slicing requirements”, Version 3.0, Jun. 2023.
[26] GSM Association (GSMA), “NG.116 generic network slice template”, Version 8.0, Jan. 2023.
[27] S. Holtmanns and C. McDaid. “5G Network Slicing Security in 5G Core Networks”. ENEA. Accessed: Mar. 2021. [Online]. Available: https://www.enea.com/insights/white-paper-slicing-security-in-5g/
[28] NSA and CISA. “ESF Potential Threats to 5G Network Slicing”. U.S. Department of Defense. Accessed: Dec. 2022. [Online]. Available: https://media.defense.gov/2022/Dec/13/2003132073/-1/-1/0/POTENTIAL%20THREATS%20TO%205G%20NETWORK%20SLICING_508C_FINAL.PDF
[29] “How to turn on 5G standalone mode in iOS 16.4 and enable its advantages”. Mac Observer. Accessed: Feb. 2023. [Online]. Available: https://www.macobserver.com/tips/how-to/turn-on-5g-standalone-mode-enable-advantages/
[30] D. Mortimore. “Launch of secure maritime 5G”. NPS America’s SLAMR. Accessed: Aug. 2022. [Online]. Available: https://nps.edu/web/slamr/-/secure-maritime-5g-ribbon-cutting
[31] “5G security control matrix”. ENISA. Accessed: May 2023. [Online]. Available: https://www.enisa.europa.eu/publications/5g-security-controls-matrix
[32] “5G toolbox”. ENISA. Accessed: Jan. 2020. [Online]. Available: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/telecoms/5g
[33] “Security assurance specifications (SCAS)”. 3GPP. Accessed: Dec. 2023. [Online]. Available: https://portal.3gpp.org/Specifications.aspx?q=1&WiUid=790015
[34] NSA and CISA. “5G network slicing: Security considerations for design, deployment, and maintenance”. CISA. Accessed: Jul. 2023. [Online]. Available: https://www.cisa.gov/news-events/alerts/2023/07/17/nsa-cisa-release-guidance-security-considerations-5g-network-slicing
[35] “Cloud security control matrix”. Cloud Security Alliance (CSA). Accessed: Dec. 2023. [Online]. Available: https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[36] “Cloud computing C5 criteria catalogue”. Federal Office for Information Security (BSI). Accessed: 2020. [Online]. Available: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

[37] S. Niedtfeld, “BSI and NATO: Shaping cloud security in the Alliance”, *BSI Magazine 2022/2: Security in focus*, pp. 45–46, Feb. 2022.