Cybersecurity for tactical 6G networks: Threats, architecture, and intelligence

Suomalainen, Jani; Ahmad, Ijaz; Shajan, Annette; Savunen, Tapio

Published in:
Future Generation Computer Systems

DOI:
10.1016/j.future.2024.107500

Published: 01/01/2025

Document Version
Publisher's final version

Future Generation Computer Systems 162 (2025) 107500

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Cybersecurity for tactical 6G networks: Threats, architecture, and intelligence

Jani Suomalainen [a,*], Ijaz Ahmad [a], Annette Shajan [a], Tapio Savunen [b]

[a] VTT Technical Research Centre of Finland, 02044 Espoo, Finland
[b] Aalto University, 02150 Espoo, Finland

ARTICLE INFO

Keywords:
Mission-critical communications
Tactical network
Public safety
Edge intelligence
6G
Threats
Risk analysis
Security solutions
Survey
Security
Cybersecurity

ABSTRACT

Edge intelligence, network autonomy, broadband satellite connectivity, and other concepts for private 6G networks are enabling new applications for public safety authorities, e.g., for police and rescue personnel. Enriched situational awareness, group communications with high-quality video, large scale IoT, and remote control of vehicles and robots will become available in any location and situation. We analyze cybersecurity in intelligent tactical bubbles, i.e., in autonomous rapidly deployable mobile networks for public safety operations. Machine learning plays major roles in enabling these networks to be rapidly orchestrated for different operations and in securing these networks from emerging threats, but also in enlarging the threat landscape. We explore applicability of different threat and risk analysis methods for mission-critical networked applications. We present the results of a joint risk prioritization study. We survey security solutions and propose a security architecture, which is founded on the current standardization activities for terrestrial and non-terrestrial 6G and leverages the concepts of machine learning-based security to protect mission-critical assets at the edge of the network.

1. Introduction

A tactical bubble is the concept of a rapidly deployable private mobile network [1–5] that supports communications of public security and safety users, such as police, border guards, and rescue personnel. Mission-critical services (MCX) include [6,7], e.g., group-communications with voice, text, and video; surveillance and situational awareness; and remote control of uncrewed land and aerial vehicles, robots, and other devices. Tactical bubbles are needed when sufficient service from fixed mobile network infrastructure is not available, e.g., due to catastrophe, cyber-attack, or a coverage gap. Tactical bubble is a good example of a vertical use case that leverages concepts for the sixth generation (6G) of 3rd Generation Partnership Project (3GPP) specified mobile networks [8–10]. It requires the *distribution* of services and computation from clouds to the edge of a network, *global* coverage via non-terrestrial communications, *increased intelligence* to automate, and ease ad-hoc deployments and operations, as well as *customization* of services to users with strict quality, resilience, and cybersecurity requirements.

Security requirements and solutions related to the concept have been previously discussed from different relevant perspectives. For instance, surveys have been written on the security of 5G and 6G networks [11–14], on the security of tactical and military communications [15–19], on the security of artificial intelligence (AI) solutions [20–23], and on autonomous, policy-based security configurations [24]. However, there is a need to systematically and comprehensively analyze and survey the security implications that arise from the current technology transition in the public safety vertical; to study the integration of 5G/6G, tactical communications, cybersecurity, and edge intelligence. Our analysis helps us clearly understand unique requirements of next-generation tactical communication systems. It also provides input both for standardization parties, for MCX application providers, and for end-users deploying and procuring new systems.

In this paper, we focus on the threats and opportunities arising from emerging edge intelligence, network automation, and satellite-terrestrial network integration. We pioneered the application of a comprehensive set of cybersecurity analysis methods — STRIDE [25], MITRE [26], DREAD [27], CVSS [28], Delphi [29], and X.805 [30] — to explore their feasibility in this new context, to assure the security of mission-critical communication solutions. We contribute by identifying, classifying, and quantifying the most prominent threats and by proposing a conceptual security architecture, which supports an analysis of the requirements for security solutions. We also survey

* Corresponding author.
E-mail address: jani.suomalainen@vtt.fi (J. Suomalainen).

https://doi.org/10.1016/j.future.2024.107500
Received 7 November 2023; Received in revised form 29 May 2024; Accepted 25 August 2024
Available online 26 August 2024

Table 1
Abbreviations.

Abbreviation	Full term(s)
3GPP	Third Generation Partnership Project
5G	Fifth Generation
5GPPP	5G Infrastructure Public Private Partnership
6G	Sixth Generation
AI	Artificial Intelligence
ATLAS	Adversarial Threat Landscape for AI Systems
CI/CD	Continuos Integration / Continuous Delivery
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DoS	Denial of Service
DREAD	Damage, Reproduce, Exploit, Affect, Discover
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
FiGHT	5G Hierarchy of Threats
GSMA	Global System for Mobile Communications
IBN	Intent-based Networking
ICT	Information and Communication Technologies
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IOPS	Isolated Operations for Public Safety
IoT	Internet of Things
IPsec	Internet Protocol Security Architecture
MEC	Multi-access Edge Computing
MCX	Mission Critical Services
ML	Machine Learning
MNO	Mobile Network Operator
NIST	National Institute of Standards and Technology
NFV	Network Function Virtualization
NR	New Radio
NTN	Non-Terrestrial Network
OAuth	Open Authorization
OSS/BSS	Operations Support System / Business Support System
QoS	Quality of Service
RAN	Radio Access Network
SDN	Software Defined Networking
SOC	Security Operation Center
SPARTA	Space Attack Research and Tactic Analysis
STRIDE	Spoof, Tamper, Repudiate, Info disclosure, DoS, Elevate
TCCA	The Critical Communications Association
TETRA	Terrestrial Trunked Radio
TN	Terrestrial Network
UAV	Unmanned Aerial Vehicle
UE	User Equipment
ZSM	Zero-touch network and Service Management

emerging security technologies and highlight and analyze the potential of ML-driven security applications in tactical use cases.

The remainder of the paper is organized as follows. Section 2 describes the background including recent developments in public safety communications, expected advances in 6G, the potential of AI for mission-critical applications, and related cybersecurity studies. Section 3 describes our application of security analysis methodology. In Section 4, we characterize the security threats and present the results of our risk quantification analyses. Section 5 describes the requirements for a conceptual security architecture and security solutions. We discuss the implications of the results and future research opportunities in Section 6 and conclude by summarizing the results in Section 7. The used acronyms are defined in Table 1 for smooth readability.

2. Next-generation public safety communications

2.1. Mission-critical communications

A mission-critical system is a system that is essential for an organization to function and whose failure may lead to serious societal, safety, or business-related consequences. Typical examples of MCX are communication by police and rescue personnel; situational awareness based on various data sources and user interfaces, including extended reality; navigation of uncrewed vehicles; and reactor safety systems. Typical mission-critical requirements for communication networks include ultra-reliability and high-security. Some applications, like video-based surveillance and group communications, have high demands for bandwidth while some applications, like the remote control of vehicles, require very low-latency.

3GPP-based mobile broadband technologies with extensions supporting mission-critical applications [3,6,31] are currently being adopted by public safety users. 4G, 5G, and eventually 6G networks will replace the dedicated public-safety network infrastructures, which were based on narrowband technologies, such as Terrestrial Trunked Radio (TETRA) [32]. This transition is motivated by cost-efficiency and emerging applications, which require increased performance from the network. Standards [33,34] enable operators to differentiate and prioritize quality and security of communication services. The next-generation public safety networks [35,36] will be able to leverage hybrid architecture: commercial mobile operator network infrastructure that is shared with other users and that can be extended with authority-dedicated rapidly deployable networks, i.e., with so called tactical bubbles.

A typical tactical bubble, illustrated in Fig. 1, includes a base station, an antenna for local connectivity, and, optionally, local core network and MCX services on edge computers. Bubbles are typically deployed on transport platforms, like cars, boats, or unmanned aerial vehicles (UAVs). Bubbles may also be connected to remote services in the cloud via terrestrial or non-terrestrial backhaul links. The configuration and coverage of a tactical bubble vary depending on needs, terrain, radio environment, applications, security landscape, and type and amount of local users. The setup can be distributed so that some functions, such as satellite terminal and antenna as well as intelligent services providing enriched situational awareness, arrive, e.g., in a command-and-control vehicle.

2.2. Example scenario - wildfire operations

Wildfire suppression, including firefighting, is an example scenario of a mission-critical operation that reflects the need for tactical bubbles and the communication capabilities they provide. We used the wildfire scenario in the joint risk assessment as the background narrative against which the panelists were asked to reflect their risk scoring.

A wildfire or forest fire is defined as a significant uncontrolled vegetation fire that can be ignited intentionally, accidentally, or naturally and has adverse effects on social, economic, or environmental values. The growing threat of wildfires to people and the environment is caused by several factors, one of which is climate change [37]. Since 2000, wildfires have burned an average of 2.8 million hectares per year in the United States. The figure is more than twice the annual average of the 1990s, 1.3 million hectares [38].

In a wildfire suppression operation, mission-critical wireless communication is an essential tool for managing the operations of firefighters and other first responders, controlling UAVs and other equipment, and creating situational awareness. Reliable and secure communication with sufficient capacity is needed throughout the operation, wherever the operation takes place. Extended coverage and additional capacity may be needed, and for such needs, tactical bubbles are a viable solution. In addition, a fire can damage the existing mobile communication infrastructure, and complementary solutions are needed. An example in the United States is FirstNet's specialized wildfire response team, which is equipped with deployable network solutions, including satellite communications, and is ready to provide communications capacity during wildfires [39].

Firefighting is an integral part of wildfire suppression operations and prioritizing the safety and well-being of firefighters is extremely important. It is critical to minimize harm to firefighters by implementing protective measures, to ensure safe practices in all areas related to firefighting, and in particular to focus on reducing the risk of life-threatening burns, preventing smoke inhalation, especially exposure to carbon monoxide [37]. New technologies based on mission-critical

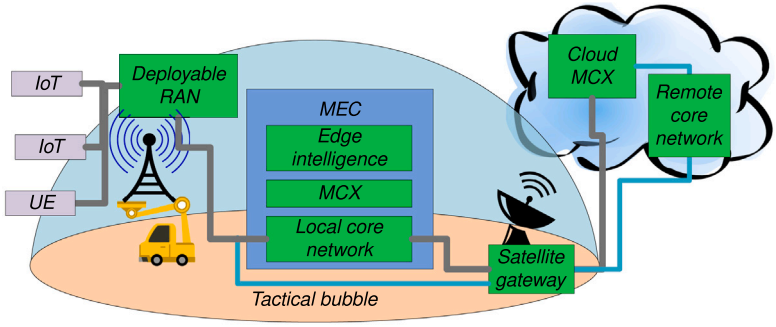

Fig. 1. The concept of intelligent tactical bubble—consists of radio access, core network, and mission-critical (MCX) functions combined with edge intelligence, which supports autonomy of bubble in isolated situations.

wireless communications can be used to improve firefighter safety. With wearable Internet of Things (IoT) technology, field commanders can monitor the health and condition of each firefighter. For example, the system can warn of excessive levels of carbon monoxide, fall down situations, and injuries. If necessary, the field commander can replace the firefighter with another team member and monitor that the replacement has taken place or command others to provide immediate help to a potentially injured colleague [40].

2.3. Mobile network operators' new role

The current networks of mobile network operators (MNOs) can serve as the foundation for next-generation public safety communications by incorporating specific network enhancements to meet the demanding public safety requirements. The network enhancements include coverage extensions and network hardening to improve network resilience, such as measures against cyber security threats, transmission network breaks, and radio site power supply disruptions [41].

The use of MNO networks for public safety communications opens new business opportunities for MNOs. The public safety segment is new for MNOs, although it is usually a small segment compared to the regular customers of MNOs, i.e., consumers and enterprises. An interesting aspect for MNOs is the possibility of having the network enhancement, extended coverage and network hardening at least partly funded by the state as part of a next-generation public safety project. A mobile network with extended coverage and improved resilience is a valuable resource also in the regular mobile service market, and thus can contribute to improved market share and reduced churn. An improved mobile network can also be an asset in other vertical customer segments, such as the smart grid market [36].

This new opportunity also introduces new business risks that jeopardize the MNO's financial goals. The possible consequences of the risks within the public safety market include additional costs, contractual penalties, and lost service revenue. Furthermore, materialized risks could adversely affect the regular operations of MNOs, potentially resulting in decreased market share and revenue [42].

For MNO's public safety business, tactical bubbles are one of the mitigants, which can be used to reduce the consequence of a materialized risk. Tactical bubbles improve the resilience of the service in radio network problems [42].

2.4. Evolution towards 6G-based tactical bubbles

Research on 6G was initiated well before the final release of the 5G standards, release 18, and the standards on 5G advance. The aim is that 6G should be commercially available by 2030, after meeting the important requirements of emerging services that cannot be fulfilled by 5G. The 5G Infrastructure Public Private Partnership (5G PPP) has initiated work on the possible 6G architecture [43]. The building blocks of the architecture are organized in three horizontal layers, and two vertical end-to-end layers covering the three horizontal layers. Fig. 2 presents a modified version of the original high level architecture proposed by the European Commission through the 5G PPP in [43], mainly to highlight the working of the tactical bubble. The horizontal layers include application, network service and infrastructure layers. The vertical layers include security (right-side) and the management and orchestration layers (left-side) spanning the three horizontal layers, showing the relevance to all of these layers. The key disruptive technologies of 6G will emerge in all horizontal and vertical layers.

Tactical 6G networks will require specific applications, services, and network infrastructure components in the three horizontal layers. To demonstrate such needs, consider the example of a geo-fencing application, also listed in the application layer of the high-level architecture Fig. 2. Due to the nature (private non-MNO application) of the application, and its unique requirements (e.g., latency due to ad-hoc mobility of personnel), a private tactical edge node in the network service layer is required. The edge node resides in the user or personnel vicinity, and thus can be mobile. A tactical bubble in the infrastructure layer is depicted in Fig. 2, in which the connectivity is provided by integrated terrestrial-non-terrestrial networks. Similarly, the private cloud infrastructure, either physical or virtual dedicated resources, provides services such as security operation center (SOC) functionality for tactical bubbles. Resources for tactical networks are ensured automatically through AI-based management and orchestration that span all layers. Moreover, robust end-to-end security is provided for all layers leveraging the development in latest technologies [43], such as blockchain, AI, and quantum computing, for all MCX.

Future cellular networks, mainly 6G networks, will provide the necessary technologies for improving the overall end-to-end connectivity needs of tactical bubbles. For example, the outdoor precision in current (5G) networks is around 10 m, whereas in 6G it should be in the range of a meter [44]. This will improve geo-fencing applications, mainly in emergency situations where tactical bubbles are deployed. Similarly, 5G covers nearly 5% of sea and provides 20% land coverage. In 6G the coverage of both must increase, which is very important for the tactical networks, since tactical bubble must not have such limitations to be deployed anywhere at sea and on land. This will require the integration of satellite-based connectivity beyond 5G. Furthermore, the use of AI has been used in 5G mostly in a non-systemic manner necessitating the need of 6G-native AI. For dynamic deployment and autonomous service provisioning, the use of AI will be inevitable for tactical bubbles, as discussed in the next sub-section 2.5. 6G will be pivotal to fulfill the specific needs of tactical bubbles compared to 5G, as highlighted in Table 2. Therefore, these needs will be covered by the 6G standards in a secure manner, as discussed in [45,46].

Typically, there are no personnel or administrators available to configure network or security in tactical networks that are operational. Furthermore, connectivity to remote command centers or SOC may not be available. Consequently, rapidly deployable networks benefit if the network and security is easily and rapidly configurable during the

Table 2
Evolution from 5G to 6G w.r.t. the requirements of tactical or mission-critical applications.

Requirement	5G	6G	Explanation relevant to tactical or mission-critical applications
Performance			
Data rate	1 Gbps	1 Tbps	Required by MCX like 3D mapping, 3D video surveillance & immersive tele-presence.
End-to-end latency	5 ms	<1 ms	Ultra-low latency will benefit, e.g., driverless vehicles and collaborative robots.
Processing delay	100 ns	10 ns	Faster processing for video surveillance through far edge.
Positioning accuracy	>5 m	<1 m	Immersive tele-presence to provide remote aid and assistance
Reliability	99.999%	99.99999%	Availability is extremely important in all mission-critical communications.
Frequency bands (GHz)	<6 & >24.25	and 95 to 3 000	Lower bands, e.g., 450 MHz, for coverage, higher for capacity or jamming tolerance.
Relevant New Technologies			
AI	Few applications	6G-native AI	Dynamic security parameter adjustment, application and network configurations.
Blockchain	No support	Use in security	Enabling use of non-trusted civilian services and infrastructures.
NTN integration	Partial	Fully integrated	Locations where terrestrial networks cannot be deployed, e.g., sea and rural areas.
Tactical access	Small & macro cells, IOPS	Small, temporary, moving cells	Basestations in UAVs, cars, or boats in critical & geographically isolated locations.

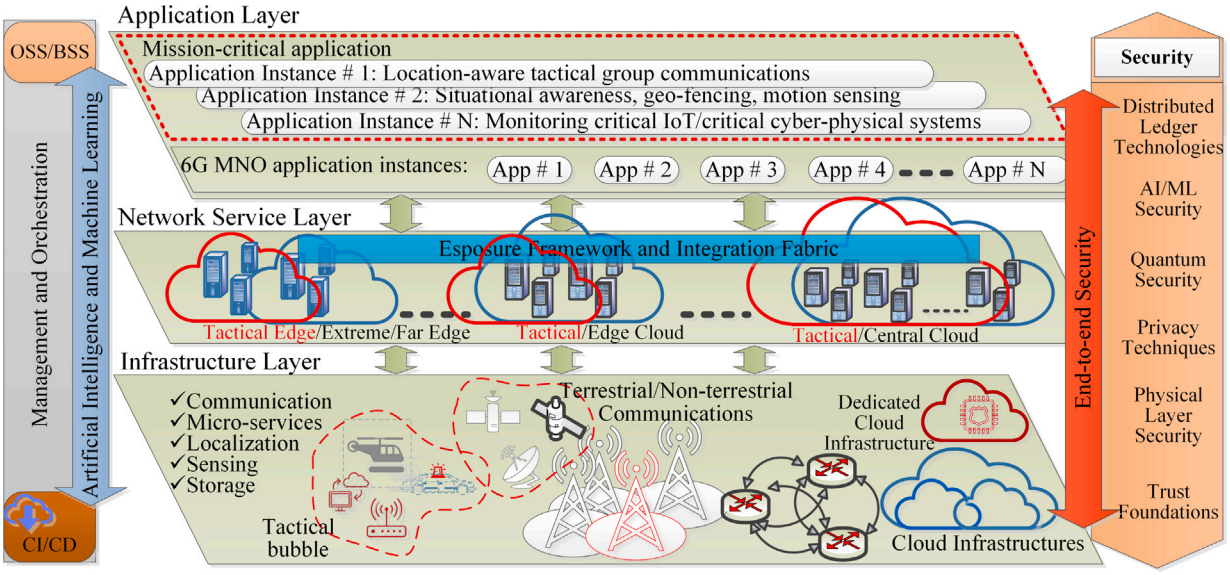

Fig. 2. 6G architecture where security technologies cover all the main layers including the infrastructure, network services and applications. The figure highlights a generic 6G architecture from 5G-PPP [43] that has been extended with networking and security concepts relevant for mission-critical communications.

deployment and if the networks is as autonomous and self-configurable as possible. Enablers for rapid configuration and autonomy include, e.g., software-defined networking (SDN), network function virtualization (NFV), machine learning (ML), as well as intent-based networking (IBN)s. These technologies are being standardized during the 5G development, and will continue with different levels of evolution in the 6G standards [44].

2.5. The role of AI

The increasing complexity and traffic volumes and diversity of UEs in communications networks has necessitated the use of AI and ML in all aspects of networks, ranging from the network infrastructure to architectures, and applications [47]. Recently, the potential use cases for AI and ML in the context of telecommunications networks have been categorized by ETSI [48] into four areas: infrastructure, networks, services, as well as assurance and security. *Assurance and security* use cases leverage ML to fight threats and previously unseen attacks in various layers, as well as manage complexity of fine-grained security policies [49]. These security use cases are further discussed in Section 5.3.

Infrastructure and *network* related cases include, e.g., load balancing and resource deployment based on estimated needs. For tactical bubble-based infrastructure, AI might be used when determining optimal configurations and locations for deployments. Management, deployment, and the migration of network functions can also be based on need and load estimates or anticipated problems. For radio networks, ML might be applied, e.g., to adapt transmission power or to control frequency switching as a reaction to detected jamming. Configuration of public safety networks could also benefit from IBN [50,51]. With natural language processing in IBN, configuration interfaces would be more easily available for non-technical authority users. Intent-based configuration would also facilitate resiliency as the system could configure itself to provide the intended services even when the network sees dynamic changes.

Service specific use cases include, e.g., orchestration — i.e., deployment and configuration — of mission-critical applications to optimize performance or user experience. For instance, ML can play a role in prioritizing information, in alerting or enriching situational awareness by recognizing events or objects (like crowd running or sound of a falling tree) from video or audio streams [52], in voice recognition to support human-machine interfaces [53], in autonomous vehicles [54], and in analyzing open and closed source intelligence [55] to identify requirements or to forecast needs for public safety operations and communication services.

2.6. Related work on cybersecurity

An overview of service requirements in public-safety mission-critical communications through the 5G new radio (NR) is presented in [56].

The article identifies important technical challenges in mission critical networks and explains how 5G NR can provide limitless connectivity, group communications, prioritizing mission-critical traffic, and ensure accurate positioning for first responders. However, security is only briefly discussed concerning the aspects of access control and admission control for prioritizing the traffic.

A survey on security of public protection and disaster relief communications utilizing 4G and 5G is presented in [57]. The main focus of the work is, however, the transition from earlier approaches, such as TETRA, to cellular networks, such as 4G and 5G. The main requirement mentioned in the article is the preferential access of safety personnel to network services and systems, which is provided by the multimedia priority services in 4G and also in 5G, but with some extensions related to Quality of Service (QoS), as defined by the 3GPP. The article further compares how the security of mission critical communications has been improved in the areas of confidentiality, integrity, authentication and non-repudiation, and reliability. However, the article is limited to discussing existing approaches for security in public safety related communications, without providing an in-depth analysis of the potential security challenges.

A survey on public safety communications on commercial and tactical 5G networks is presented in [18]. The article explores security architectures and enablers for prioritized public safety communication in 5G networks. Security threats and corresponding security enablers are analyzed in tactical access and core networks, commercial infrastructure and mission-critical applications are discussed. Focus is laid on solutions for enhanced access control for constrained devices and security of satellite-based backhaul networks. We complement these, our previous, efforts with a more extensive security analysis methodology, with a systematic threat analysis and by focusing to autonomous and AI-driven security features.

An analysis of security of communications networks in critical environments, such as military deployments is carried out in [58]. From the security point of view, the article is mainly focused on IP communications and does not delve into existing (5G) or future wireless networks such as 6G. Similarly, techniques for device-to-device communications for national security and public communications have been proposed in [59]. Moreover, a secure wireless communication system for mission critical communications has been proposed in [60]. The techniques mainly secure privacy in infrastructure-less or ad hoc UAV communications. Malicious receivers of traffic are prevented through jamming packets to prevent revealing network information. Security analyses of 6G use cases, which are relevant also for the public safety vertical, include the work in [61] that studies the security of 6G based telepresence and virtual reality applications. They identified potential threat agents and threats, which were categorized using the STRIDE model.

There are several studies that explore the security of 3GPP communication networks for tactical and public safety use cases include [32, 62–64]. However, these are older studies based on previous technologies such as 4G [63,64], TETRA [32], and the APCO project 25 [62] published in 2011. In contrast to all these previous studies, our work focuses on emerging technologies of 6G, edge intelligence, and ML-based cyber defence, which will be crucial for tactical networks. We dig deep into a practically deployable tactical network and critically analyze it from the security perspective with various security threat and analysis models to draw important conclusions and research directions for future work. Below, we discuss the security analysis methodology.

3. Security analysis methodology

This sections describes the methods that were used and adapted to explore our use cases. We applied several existing approaches and taxonomies that helped us to capture vulnerabilities, threats, attack vectors, and requirements and to make the analysis as representative as possible. We also wanted to understand the potential of different approaches. The aim is not to list every threat variation in detail but to gain a complete high-level view of the security requirements for architecture, implementations and operations, and then focus on a few topics that characterize our cases and emerging technologies. The applied analysis methods — the security metrics — are listed in Fig. 3. The figure highlights a risk bow-tie framework [65] and illustrates our methods related to the reasons of risk in the left and to the consequences of risk in the right.

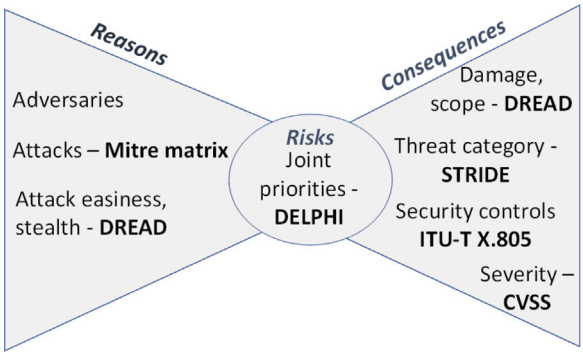

Fig. 3. Applied methods.

The applied methods have been previously used only in limited manner in the context of mobile networks or critical communication systems. STRIDE is widely applied approach and its applications include 5G slicing [66] and 5G public safety networks [67]. DREAD has been previously applied for mobile health systems [68]. CVSS has been applied in the context of industrial IoT protocols [69]. The Delphi method has been applied for researching risk factors in mobile business [70] and for finding QoS requirements for mobile applications [71]. The X.805 architecture has been used when analyzing 5G security [72] but not in the context of public safety vertical. The MITRE matrices have been defined for many context but our approach was the first that created a new synthesis for tactical networks and also utilized the approach to classify ML-solutions.

3.1. Joint risk identification and prioritization with Delphi

The Delphi method [39] aims to support decision making based on reaching a consensus between experts. Delphi describes a group communication process using rounds of anonymous questionnaires. The method was applied within a panel that consisted 11 members from the AI-NET-ANTILLAS project consortium and that represented expertise in network technology, cybersecurity, and business for mission-critical communications.

We applied the Delphi method first to identify and then to evaluate and prioritize security risks in three rounds. The first round was organized as a hybrid event and the last two as online rounds. The results were collected using Questback, which is a web-based online service for user queries. The *threat identification* round collected threats by asking the selected experts to consider what could go wrong in the wildfire operation, which was elaborated in Section 2.2. The collected threats were processed and consolidated after the collection. The *risk scoring* round collected scores for the identified threats. The *scoring consensus* round enabled the experts to revise their scores. The last survey was identical to the survey in the second round, but included earlier answers as well as panel's average scores from previous round. For the selected risks, four questions were asked:

1. How discoverable (detectable by the victim) is the attack?
2. How easy is it for the attacker to perform/execute the attack?
3. What is the impact (in the victim's perspective) of the attack/threat event?

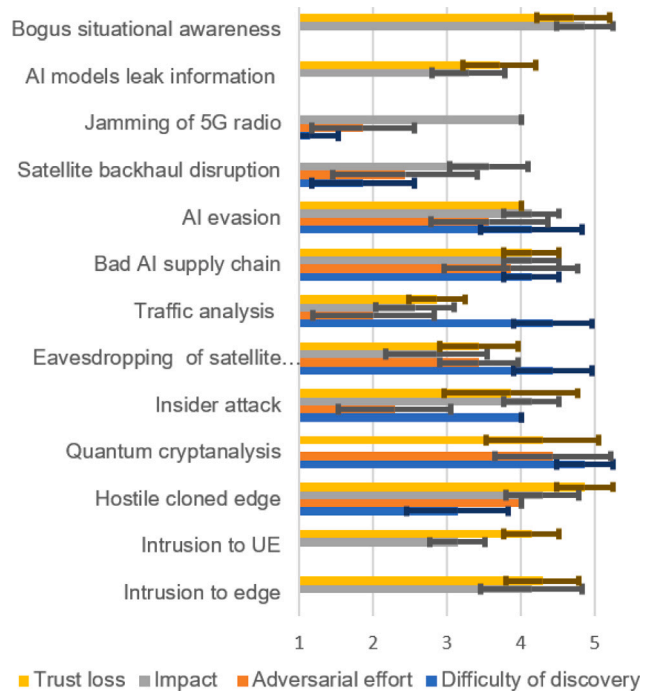

Fig. 4. Risk valuation examples from the Delphi process. The bars highlight average scores for identified threats. The achieved consensus was measured using standard deviation and is illustrated with the dark lines at the right ends of the bars: the higher the consensus, the shorter the line.

4. What kind of an effect does the attack/threat event have for the authority organization's trust towards the system?

The results shown in Fig. 4 are based on the replies given in the final round. We used a five-level ranging from one *very easy* to five *very difficult* for scoring the first two questions and a slightly adapted version ranging from *no effect/impact* to *critical effect/impact* for scoring the two latter questions. The achieved consensus was measured using standard deviation, which is a measure of how dispersed the data is in relation to the mean. We ended the survey after three rounds, which is sufficient for evaluating the diversity of opinions though it did not yet achieve complete consensus.

One reason for the use of the expert group was to increase the objectivity of the threat analysis and to remove the bias that a single security analyst may introduce to the results. Our application of the method and the process are elaborated in more detail in [73].

3.2. Threat and risk metrics

To quantify the threats and risks in each threat scenario that was identified in joint analysis, we applied three existing security analysis methods. These security metrics, which have been commonly applied in computer systems, include STRIDE for threat identification, DREAD for risk assessment, and Common Vulnerability Scoring System (CVSS) for vulnerability severity assessment. The first two where originally developed by Microsoft [25] for assuring the security of operating systems and services, while the last is an open industry standard for computer system vulnerabilities. STRIDE (from the words Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) defines six categories for classifying threats based on adversarial goal. For each identified threat, we subjectively evaluated which STRIDE categories reflect the adversarial objectives best. Our categorizations are presented in Table 4. DREAD [27] (coming from Damage, Reproducibility, Exploitability, Affected users, Discoverability) assess each threat in five categories with values from 0 to 10. Table 3 provides our definitions for the DREAD metrics to be used when assessing risks in public safety communications and in the tactical bubble use case and Table 4 provides our metric assessments for the identified threat scenarios.

CVSS [28] aims to systematically analyze the severity of a given vulnerability with metrics that fall into three groups. Base metrics (attack vector, complexity, privileges, required user interaction, scope) are time independent and irrelevant to the target environment. Temporal metrics (confidentiality requirement, integrity requirement, availability requirement, code maturity, remediation level) are time dependent but irrelevant to the target environment. Environment metrics (confidentiality, integrity, and availability requirements, are relevant to the target environment. For each identified threat scenario, we calculated the base metric value, which illustrates the criticality of the vulnerability with a scale from 0 to 10. We used CVSS version 3.1 where values were defined using a CVSS calculator from NIST [74]. The applied CVSS vectors for each threat scenario have been published through the GitHub repository [75].

3.3. Attack matrices for taxonomy of autonomous defenses

A MITRE Attack Matrix [76] is a commonly utilized security analysis framework/attack database. It is a collection of adversarial tactics and techniques, as well as corresponding mitigations. It is a useful tool in understanding the next steps of an ongoing attack and it can help in planning an appropriate defense strategy. MITRE has developed attack matrices for enterprises, industrial control systems (ICS), and mobile devices. Furthermore, there exists matrix variations for AI systems, i.e., the Adversarial Threat Landscape for Artificial-intelligence Systems (ATLAS) matrix [77]; for 5G networks, i.e., the 5G Hierarchy of Threats (FiGHT) matrix [78]; and for satellite systems, i.e., the Space Attack Research and Tactic Analysis (SPARTA) matrix [79]. Seminal research efforts to adapt attack matrices for mobile networks also include the work by Rao et al. [80].

We looked at attack techniques, tactics, and mitigations in enterprise, ICS, mobile, ATLAS, FiGHT, and SPARTA matrices and selected the ones that were applicable and typical for tactical networks. Our novel tactical communications specific attack matrix is presented in Table 6. We utilized the adapted matrix also as a way to classify security functions. Particularly, our matrix highlights AI-based solutions and enablers that can be used to increase intelligence and autonomy of security controls.

3.4. Security dimensions according to X.805

The International Telecommunication Union provides security recommendations through a security architecture for systems that provide end-to-end communications [30]. The security dimensions are briefly outlined below.

- ***Access Control*** dimension protects the network from unauthorized use of the network resources. Only authorized persons and devices can have access to network components, information, services, applications, and information flows. Furthermore, role-based access control can be provided to different entities based on the authorization provided.
- ***Authentication*** dimension confirms the identities of communicating entities. Verification of identities and protection against masquerading or illegally using identities is performed in the authentication dimension.
- ***Non-Repudiation*** dimension enables binding actions with the corresponding users of data or network resources through procedures of making proofs, etc. It ensures the availability of evidence to proof that an action has been performed by a particular actor or user.

Table 3
Metrics for quantifying risks in tactical bubbles and mission-critical applications. The metrics have been categorized using the DREAD model.

Category	Description	Scale examples
Damage	When exploited, how much damage will be caused?	0 = Nothing 3 = Temporary unavailability of a small asset (e.g., device). Small deprecation of trust towards the root cause provider. 5 = Permanent unavailability of a small asset (e.g., device). Medium-size temporary deprecation of trust. 6 = Temporary unavailability of a large local asset (e.g., bubble, local MC service). Large temporary deprecation of trust. 7 = Temporary unavailability of a large national asset (e.g., all bubble, remote MC services). Major impact on trust. 10 = Complete system destruction or compromise. Permanent lost of trust towards root cause/vulnerability source.
Reproducibility	How reliably can the vulnerability be exploited?	0 = Very hard or impossible 5 = One or two steps required; existing COTS can be utilized. Attack possible after operational human error. 9 = Adversaries within proximity can trivially exploit. Vulnerability is tied to implementation and requires time to patch. 10 = Any adversary can trivially and reliably exploit. Vulnerability is tied to architecture and hard to address.
Exploitability	How difficult is the vulnerability to exploit?	0 = Even with direct knowledge of the vulnerability we do not see a viable path for exploitation 3 = Advanced techniques and custom tool are required. Only exploitable for authenticated users. 5 = Exploit is available, understood, and usable with only moderate skill by authenticated users 7 = Exploit is available, understood, and usable by non-authenticated users 10 = Trivial, e.g., exploitable by non-authenticated users and does not require specialized expertise
Affected users	How many users will be affected?	3 = Single device/data source 4 = Single authority user 5 = Every local authority user in the tactical bubble 7 = Authority users in several bubbles 10 = Society's capability to perform operations prevented. Large scale impact to civilians, e.g., leakage of health records
Discoverability	How easy is it to discover the threat?	0 = Impossible to detect 1 = Requires access to source code/system memory analysis 2 = Causes some network traffic (e.g., command & control) but it may be hidden 7 = Attack signatures are publicly known and detectable 10 = Trivial, e.g., the attack results physical disappearance or destruction of equipment

- ***Data Confidentiality*** dimension protects information from unauthorized disclosure.
- ***Communication Security*** dimension ensures that the data flow occurs only between the authorized entities and the information is not diverted to or intercepted by unintended end-points.
- ***Data Integrity*** dimension ensures the correctness and accuracy of the data.
- ***Availability*** dimension ensures the availability of network resources to all authorized users and that no denial of resources such as information, communication links, services or applications occur for authorized users. The availability dimension also ensures resilience and disaster recovery solutions.
- ***Privacy*** dimension provides protection of information during communications and from observations of network behaviors, events, and activities. Personal activity protection is provided in the privacy dimension.

The X.805 model has been previously used to analyze the security requirements for 5G security architecture. Arfaou et al. [72] extended the eight X.805 categories with more — audit, trust and assurance, and compliance — to identify life cycle and trustworthiness-related security controls for 5G security architecture. We use the security dimensions of X.805 to analyze the security requirements of tactical 6G networks, outline potential threats, and discuss possible solutions to threats in view of the requirements. In the following sections, these dimensions will be referred to during the analysis of threats and solutions, and to draw conclusions for further research.

4. Cybersecurity threats

This section identifies current and emerging security threats in tactical bubbles. The section aims to capture threats that are characterizing for our use cases. The section starts by highlighting the adversaries and their motivations. Then the threats are handled in three main categories: (a) disruption of tactical operations related to threats against availability and integrity in the network, (b) risks related to information assets addresses confidentiality in the network, and, (c) threats in emerging application areas. A detailed categorization and quantification of identified threat and risk levels is presented in Table 4.

4.1. Adversaries

There are no publicly available statistics on attacks against public safety networks nor on adversaries. However, we are able to speculate on the potential threat agent categories and their motives.

Criminals may hijack individual bubbles for financial benefits. Ransomware and hijacking of devices into a botnetwork provide limited advantages as lifetimes of single bubbles are short and new clean bubbles can be easily deployed. Criminal motivation may increase, if the bubbles should give access to long-term secrets or assets that can be sold. Also, denial-of-service attacks may provide some blackmail opportunities, particularly if the blackmailers can demonstrate persistent capabilities. There are also factors limiting criminal's interest. First, criminals are typically humans who may have some ethics. Attacking public rescue/healthcare operations is not good for the reputation of the adversary and may also demotivate individuals working for criminal organization. Second, due to their lifetime and protection, tactical bubbles are not visible and detectable for adversaries, at least not for long consecutive periods of time.

Random hackers and individuals may be motivated by a revenge against authorities or just by the challenge. However, private networks are niche targets, as there is a limited amount of open information or ready adversarial tools available. For tactical networks there are even less customized adversarial resources easily available.

Insiders have best view of tactical bubbles, and they understand the processes and technology. Whether as tactical bubble is the best target for revenge actions is unclear, insiders with grudge might get better revenge by targeting long-term organizational data.

National agencies, terrorists – public safety and security communications may be a valid target for advanced adversaries as a part of hybrid attacks or warfare. Disabling the communications of public authorities is the cyber part of a hybrid operation, which involves also physical operations and where the objective may be to distract authorities or to prevent their operations. These actors have lots of resources and are able to launch advanced persistent threats.

Collateral damage - attacks targeting some other domain may spread to tactical bubbles, e.g., due to use of same components etc. However, the nicheness of MCX, short lifetimes, (periodic) isolation from the network, and restricted visibility will also limit collateral damage.

Table 4
Analysis metrics for risks in tactical bubbles.

Threat scenario	Objectives	Risk					Vulnerability score	Joint prioritization (Delphi)			
	STRIDE	D	R	E	A	D	CVSS base	Stealth	Efforts	Impact	Trust
Disruption of Tactical Operations											
Spoofed or prevented situational awareness	STRD	5	8	2	5	2	6.8	–	–	4.86	4.71
Denial-of-service	D	3	9	8	5	8	7.5	1.86	2.43	3.57	-
Compromised authentication infrastructure	STRDE	8	2	2	5	2	8.0	–	–	4.14	4.14
Credential stealing from a device	STRE	4	3	2	5	4	6.6	–	–	4.14	4.14
Attacks against support systems	SD	4	5	5	4	5	7.1	–	–	–	-
Vulnerabilities due to bubble federation	ID	5	5	5	4	5	6.3	–	–	–	-
Misconfigurations & insider attacks	TIDE	7	2	2	7	2	6.5	4.00	2.29	4.14	3.86
Persistent threats via AI poisoning	TID	7	2	1	7	1	5.5	4.14	3.86	4.14	4.14
Avoiding threat detection via ML evasion	SD	7	2	1	7	1	4.4	4.14	3.57	4.14	4.00
Sensitive Information Assets											
Information theft from the cloud	I	9	2	2	9	3	4.4	–	–	4.00	4.00
Information theft from the edge	I	7	2	2	7	3	4.4	–	–	4.00	4.00
Information theft from UE	I	3	5	5	3	3	4.4	–	–	3.14	4.14
Failing E2E secrecy & eavesdropping at RAN	STRI	8	2	1	6	1	3.7	3.86	3.14	4.14	4.14
RAN leaking operational information	I	3	5	3	5	2	3.7	4.43	2.00	2.57	2.86
AI models leaking organizational secrets	I	5	2	5	5	1	2.2	–	–	3.29	3.71
Unmanned Vehicle and IoT Challenges											
Malware infected devices	ID	5	3	3	5	5	7.5	3.00	3.14	3.14	–
Denied positioning	D	3	7	7	5	7	6.2	1.19	1.17	3.57	–
Impaired control latency	D	3	7	7	5	7	6.2	1.14	1.86	4.00	–
Device capture by hijacking control	TIDE	5	2	2	3	8	5.9	2.42	3.14	4.14	4.00
Massive IoT signaling	D	4	4	4	5	7	4.3	–	–	3.57	–

4.2. Disruption of tactical operations

Depending on the deployment options, tactical bubbles host various assets that are threatened. At minimum, the tactical access bubble hosts RAN-specific software and hardware functions and related information. Each function has its own credentials and certificates enabling it to authenticate clients and to connect other services. As the radio access network is connected to remote core and MCX services the tactical bubble also typically hosts IP Security Architecture (IPsec) keys enabling protection of backhaul communications. Further, devices and user equipment (UE) in the tactical bubble have their own credentials for the network and MCX and may also have application specific secrets.

The availability of MCX (group push-to-talk, situational awareness, remote control) is critical for the operation to succeed. Availability-related attacks may happen in radio, network, or application layers and prevent the connectivity or use of a particular service or damage the service level so that real-time applications become unfeasible. For instance, low video quality or delayed voice services will deny group communications. Denial-of-service attacks may be performed in different layers and domains. Disruption may be instigated by:

- Outsiders in proximity may jam radio signals [81–83]). To maximize coverage, tactical bubbles often use lower radio frequencies. For instance, 450 MHz can be the preferred frequency in search and rescue operations where users are dispersed over a large area. However, lower frequencies offer lower bandwidth and hence are more vulnerable to jamming. 5G and 6G networks can utilize bands higher than 30 GHz where jammers need high power levels for successful attacks, but that would also affect the coverage of the tactical bubble.
- Authorized but misbehaving user equipment (UE) in a tactical bubble may attack, e.g., against vulnerable QoS functions and interfaces, network control points, IoT gateways, and the IoT platform. Tactical operations may be disrupted also by tampered situational awareness, i.e., by missing information or by misinformation by compromised sensors. Such UEs can cause privacy exposures, and compromise data confidentiality and integrity.
- Remote adversaries, e.g., from the Internet may target open interfaces of the bubble, firewall, backhauls, or remote services. Attacks can be brute force or specific attacks utilizing known but unpatched vulnerabilities. The result can be a lack of availability, unauthorized access, and privacy leakage.

Service orchestration of functions to provide end-to-end services may introduce several vulnerabilities due to complexity and involvement of various actors. Human errors has been the root cause in more than 20% of security incidents in telecommunications and around 90% of lost user hours were due to them [84]. Vulnerabilities caused by end-users circumventing security have been recognized also in existing public safety networks [62]. Security challenges arise when a tactical bubble federates with other networks of authorities or private networks belonging to third-parties. Authorities may utilize federating access networks or edge computing platforms to achieve coverage or capacity for their MCX but federation expands the threat surface and forces the bubble to trust external actors.

Operations can also be disrupted through different auxiliary security and non-security related systems, like authentication infrastructure, electricity, navigation of vehicles carrying equipment, or database providing spectrum data. For instance, attack vectors enabling device masquerading or cloning by an adversary creating credentials include leakage of secrets from the authentication infrastructure in different phases of the life-cycle. Signing keys for asymmetric secrets may leak during provisioning or in the factory, shared secrets may leak from the server-side functions, and credentials may be stolen from UEs.

Cybersecurity for connectivity solutions that are based on integrated satellite-terrestrial networks inherits threats and challenges from the mobile networks, from satellite networks, and from application domains. In addition, the integration of these domains will introduce totally new challenges. We analyzed cybersecurity implications arising from the satellite-terrestrial network integration in [46,85].

4.3. Disclosure of sensitive information

Public safety networks and UEs store and transmit sensitive societal, organizational, and operational data. Leaking of health and police record information can have significant impact on civilians trust in the authorities. IoT sensors, UAVs, and cameras collect information that can be critical from the privacy perspective. Further, the situational awareness that is based on this information is critical both regarding

confidentiality and integrity. Remote control and safety of vehicles and actuators depends on control data coming through network. Further, devices itself may be valuable and lost and destroyed.

An analysis of potential data categories in a public safety use case has been done by NIST [86]. The NIST analysis also covered risk assessments according to FIPS 199 [87], which associates security objectives (confidentiality, integrity, availability) and impact assessments (low, moderate, high effect on organizational operations) with data categories. The analysis focused on a specific scenario (explosion at a chemical plant), it covers only a subset of the potential information types in four categories: operations, situational awareness, sensor, and public source data.

4.4. Disruption of uncrewed vehicles and IoT

New applications, data collection gadgets, such as UAVs, body cameras and IoT sensors, and the remote control of vehicles and robots can improve the efficiency and safety of public safety operations. However, IoT devices can be vulnerable to attacks and provide an attack vector to the infrastructure. The heterogeneity of IoT devices' computing and communication capabilities must be considered during the procurement phase. Security solutions for many IoT products are manufacturer specific and not standard-compatible. The lack of common security architecture for the heterogeneous IoT landscape is one reason why some devices may be unprotected and consequently should be accepted for operational use only in limited and controlled roles with zero-trust. Massive numbers of simultaneously communicating devices may exhaust resources with signaling spikes and, limited resources of tactical networks e.g., a satellite link can become a bottle neck.

5. Security solutions

The security architecture is a combination of models, methods, protocols, services, and principles that secure mission-critical assets from cyber threats. This section describes requirements for the security architecture and surveys existing and emerging security solutions (concepts, enablers, and technologies) and highlights how they relate and contribute to tactical bubbles.

5.1. Baseline security architecture

The baseline security architecture provides the first line of defenses to protect tactical communications. The architecture consists of elements and procedures in the network and application layer as well as security and hardening for devices—from UE and IoT to network components.

A European Commission study on the architectural perspectives of 6G [43] outlines key new trends that existed in 5G, but will develop beyond the state-of-the-art 5G solutions. These include AI- and computation-pervasiveness, programmability beyond control and data plane, integration of the concepts of cloudification and softwarization beyond the core network, and continuum orchestration post 5G. The architectural principles that guide the design of the architecture, henceforth, are (i) exposure of capabilities, (ii) AI for full automation, (iii) flexibility to different topologies, (iv) scalability, (v) resilience and reliability, (vi) exposed interfaces are service-based, (vii) separation of concerns of network functions, and (viii) network simplification in comparison to previous generations. Most of these principles require a reinvigorated approach to security of users, the infrastructures, and generic or use-case-specific architectures deployed on heterogeneous infrastructures.

3GPP is clear on the fact the coverage in future networks will be provided by a combination of terrestrial and non-terrestrial networks [88]. The security architecture of 5G networks is mainly focused on terrestrial networks, which have its own kind of requirements as studied in [89]. The security of non-terrestrial networks, on the other hand, have own and very distinct requirements, as elaborated in [46]. In principle, the security architecture for tactical communications must be capable to provide end-to-end security for a rapidly deployed network. Such networks may operate on an ad-hoc basis, thus necessitating security of all randomly joining and leaving nodes. Such nodes must be properly authenticated and authorized first. 3GPP provides access control based on subscriber identifiers and authentication and key agreement procedures. Mission-critical application may deploy own authentication and communication protection solutions for end-to-end security as well as support authorization that can be based, e.g., on organizational or operational policies or on clearance levels.

Existing cryptographic technologies already provide enough security to ensure data confidentiality. However, efficient key distribution in situations where integrated non-terrestrial networks (NTNs) are used, and developing lightweight encryption techniques for MCX will be important in the future. The availability of network resources is the most important dimension that is mostly threatened by denial-of-service (DoS) or distributed DoS (DDoS) types of attacks. Due to resource limitations in such networks, mounting variants of DoS attacks will be comparatively easy. However, multiple connectivity options, such as integrated cellular and satellite connectivity, and redundancy in localized resources can provide the necessary security. Non-repudiation requires third-party identity systems to be integrated with the tactical bubble. Software-based USIM does pave the way towards achieving this goal; however, it will bring security challenges related to software systems, necessitating further research in software/remote attestation.

Services in the tactical networks can be deployed as virtualized functions whose configuration and management, i.e., the orchestration, is automated as much as possible. Security requirements for virtualized solutions are being standardized by ETSI and include trust and platform security issues [90,91], automated orchestration, zero-touch network and service management (ZSM), and deployment of security functions [92–95], security management and monitoring [96].

Different standardization parties and governments define specific security requirements for systems, network and user equipment, and applications, when they are used by public safety authorities. Table 5 lists standardization efforts relevant in different areas of the security architecture, emphasizing also security enablers we expected to emerge through 6G. For instance, ISO [97], NIST [98,99], and ENISA [100,101] have defined security guidance for the use of IoT devices and AI based systems. Guidelines have also emerged for developing trustworthy solutions for specific mission-critical application areas, including UAV and neural network relevant concepts for design assurance from European Union Aviation Safety Agency [102], interoperability for MCX from the Critical Communication Association [7,103], as well as various standards for different industrial control/cyber–physical systems, surveyed, e.g., in [104]. Countries have own requirements for security auditing of information and cloud systems used by authorities, e.g., KATAKRI [105] in Finland, and NIST 800-53 [106] in US. Similarly, specific devices have own common criteria profiles that must be met before devices are being accepted for use. Increased security for devices can be based, e.g., on hardware security elements, specified by Trusted Computing Group (TCG) or security assurance and certification processes and framework for network equipment from GSMA [107] and 3GPP [108]. Further, regulation that apply to AI and telecommunication networks and their security and privacy, e.g., European Union's electronic communications code and AI acts, are in many extend relevant also for public safety networks.

5.2. 3GPP security architecture

3GPP is specifying several standards that are relevant for the security architecture of tactical networks. An overview of the architecture is presented in Fig. 5. The starting point is the security architecture and procedures specification [109], which is illustrated in the figure in the gray boxes. 3GPP extensions of network standards supporting

Table 5
Standards and ongoing work for the security architecture.

Domain	Baseline standards
Network	
Access network	3GPP Security Architecture [109], eSIM, IOPS [3], 6G→post quantum cryptography, physical layer security, new decentralized subscription models
Backhaul and core	3GPP Security [109]/IETF: IPsec, HTTPS, OAuth
Non-terrestrial	6G→new protocols for NTN; integrated TN-NTN security
Application security	3GPP MCX [110]: OpenID, TLS; TCCA interoperability [103]; ENISA [100] & NIST [98]: IoT
Automation and intelligence	
Security automation	ETSI ZSM [93] & ENI [48], OASIS [111], 3GPP: AI support [112], 6G→native AI
AI trustworthiness	ISO [97], NIST [99], ENISA [101], EASA CoDANN [102]
Infrastructure and devices	
Virtualization	ETSI NFV [95]
Security assurance	Common Criteria profiles; TCG: security hardware; 3GPP [108] & GSMA [107]: certification framework
System security	NIST 800-53 [106]; KATAKRI [105]

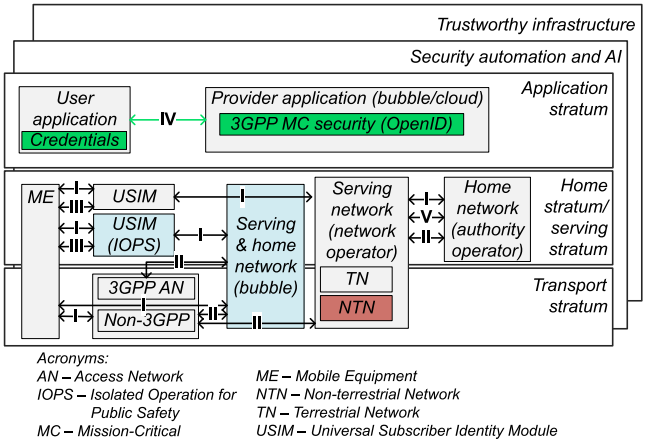

Fig. 5. Security architecture - illustrating tactical network domains. The architecture model merges concepts from the 3GPP security architecture (gray), Isolated Operation for Public Safety users (IOPS, blue), Mission-Critical Services (MCX, green), and Non-Terrestrial Network (NTN, red) specifications and highlights the importance of (non-3GPP) secure infrastructure and intelligent security as own layers, which impact each domain.

tactical use cases — isolated operations for public safety (IOPS) [3,6] and edge security [113–115] — are highlighted in light blue. Work on NTN integration [116,117] is illustrated in red. Security specifications — the MC security framework [6,110] — supporting interoperability of MC applications are highlighted in green. Security technologies outside the focus of 3GPP include secure infrastructure and intelligent security, which are highlighted in the figure in their own layers.

The 3GPP security architecture has the following main domains, which are each impacted by the tactical network use case:

- **Network access security (I)** comprises the set of security features that enable UE to securely authenticate and access network services. The domain includes security of 3GPP and non-3GPP access technologies, and delivery of security context from serving network to the UE. In the context of tactical networks, IOPS specifications provide means for users to connect to private networks with isolated network specific subscriber identities.
- **Network domain security (II)** is composed of security features that enable network nodes to securely exchange signaling and user plane data. NTN communication introduces challenges as it makes backhaul communication more easily interceptable from wider geographical location than tactical bubble. Satellite-specific security controls and adaptation of both network domain security and application domain security for NTN is required.
- **User domain security (III)** consists of security features that enable secure user access to UE. Mobile terminals and devices used by public safety organizations are typically hardened and certified for the authority users with security clearances.
- **Application domain security (IV)** includes security features that enable applications, both in user and provider domains, to securely exchange messages. The MC security framework [110,118] outlines the use of established security solutions — OpenID Connect and Transmission Layer Security — for identity management and end-to-end protection.
- **Service Based Architecture domain security (V)** is composed of security features for the registration, discovery, and authorization of network elements, as well as security for service-based interfaces. Isolated deployment of tactical network, necessitate core services and security capability to be deployed to local bubbles and secured appropriately.
- **Visibility and configurability of security (VI)** includes different security features that inform users whether security features are in operation or not. As highlighted by past incidents [62], security features should not be made optional for public safety end-users.

The tactical bubble and the served UE must follow the security standard set by the 3GPP since it provides the baseline security. However, there will be additional requirements based on the criticality and deployment infrastructure of the tactical bubble. For example, it is highly likely that a tactical bubble may be connected through a combination of terrestrial and non-terrestrial networks working in unison. Therefore, there will be additional security requirements needed by the deployed infrastructure. One such security feature, for instance, is meant to mitigate binding down attacks, as discussed in [109]. Since tactical bubbles will be deployed in critical or even hostile environments, there is a possibility of binding down attacks by making the UE or the network entities believe that a particular security feature is not supported, which in fact will not be true. Security feature of UEs and the tactical bubble must be verified before deployment to avoid such attacks. Similarly, binding to the network (serving network) can also be carried out prior to deployment to avoid pitfalls in the actual environment. In the case of non-terrestrial networks, the most challenging part is the key agreement procedures required for authentication. Therefore, the keying procedure should also be carried out beforehand to avoid security risks.

Lack of mandatory end-to-end encryption was a major vulnerability in the previous generations of public safety communications [62]. Similar vulnerabilities exist also in the 3GPP standards [119]. Consequently, IPsec protection for tunneled communication between core and base stations is considered mandatory. Furthermore, the challenge of fake base stations, which could have been a major security concern for tactical networks, that persisted in the previous generations, have also been averted in 5G [89], and thus, will no longer pose a major threat. Moreover, the latest technological developments, such as SDN and NFV, further strengthen the network security landscape [120]. In summary, 5G improves the overall security of communications networks on a general level compared to the previous generations, however, new security procedures must be investigated and adapted for emerging technological concepts, as discussed below.

Table 6
Potential attack tactics and techniques, against tactical bubbles, as well as mitigations, including examples of autonomous ML-based security solutions.

Attack tactics & techniques	Mitigations & references on 5G/6G applicable intelligent defenses
Reconnaissance	
Gather victim information	Counter-reconnaissance: automating cyber threat intelligence sharing [55,124,125]; intelligent honeypots [126]
Active scanning	Monitoring, moving target defenses [127–129]
Eavesdropping (passive)	Radio and end-to-end encryption; detecting eavesdroppers with visual or radio frequency surveillance [130,131]
Resource development	
Digital certificates	Protecting credentials in user and network equipment; Automated management of certificate life cycles
Exploits, vulnerabilities	Hardening; Finding vulnerabilities using automated scanners [132] or threats using large language models [73,133]
Compromise infrastructure	Intrusion detection [134–136], response orchestration [137], and automated playbook recommendations [138,139]
Poison training data	Control access to data sources and data sets; sanitize training data
Upload malware	Internet scan for pre-compromise identification; virus detection for post-compromise
ML model access	Control access to ML models
Obtain capabilities (UE)	End-point security and physical guarding for user equipment and IoT devices
Initial access	
Exploit public-facing app	Hardened firewalls; authorize core service access; ML for constructing [140] or verifying [141] access policies
External remote services	Hardening; strong authentication; monitoring; automated partitioning for networks [142]
Transient cyber asset	Audit; testing; and certification of connected UE and IoT; access control; antivirus; segmentation
Valid accounts	Audits; user-behavior [143] or user-intent based access control [144] to support principle of least privileges
Trusted relationship	Segmentation and account management; audits and monitoring
Supply chain compromise	Patch management; vulnerability monitoring; code review
Wireless compromise	RAN & end-to-end security
Execution	
Flooding	Filter network traffic; monitor traffic & sensor health; ML approaches for DDoS detection [145]
Jamming	Monitoring, e.g., ML for multi-input/multi-output antennas [146]
Exploit code flaws	Software testing, updates, and source control; least privilege
Malicious code	Fingerprint and behavior based anti-malware; function log monitoring; intrusion detection [147–150]
Disable/bypass encryption	Monitoring system configuration, security posture, and anomalies
Network flow manipulation	Security SDN routers and controllers as well as control communication; log monitoring and correlance analysis
gNodeB manipulation	End-point security; physical security
Persistence & defense evasion	
Modify program	Audits; malware, anomaly, and intrusion detection for edge [151]; detecting covert control channels [152]
Backdoor ML model	Protect and sanitize training data; validate model
Obfuscated control	Network traffic monitoring; ML-based covert channel detection [152]
Masquerading	UE integrity verification and behavior monitoring; Radio fingerprinting [153] revealing captured credentials on rogue UEs
Evade ML model	Model hardening; ensemble methods; multi-modal sensors; adversarial input detection; tracking isolation tied behavior
Collection	
Data from local system	Intrusion detection for edge services and UE; data loss prevention; confidential computing
Adversary-in-the-middle	End-to-end security; network and host (core services at edge) intrusion prevention
Wireless sniffing	Radio and end-to-end security; minimized signal propagation
Impact	
Deception	Managing trustworthiness of situational data; least privilege principle for critical information
Loss of availability	Redundant capacity; ML for resource allocation [154]
Loss of productivity	Loadbalancing; backups; traffic filtering; security-driven prioritization [155]; intent-driven security [156,157]
Theft of operational information	Data loss prevention; access control; encryption
ML intellectual property theft	Control access to models; encrypt sensitive information; minimize information in models
System misuse	Monitor use of system

5.3. Adaptive ML-driven security

The baseline security architecture can be extended with adaptive threat detection and prevention capabilities. In Table 6, we survey potential intelligent ML-based security applications and classify them using the attack matrix, which we defined for tactical bubbles. Here, we also discuss the potential role of ML for applications of cyber defense [121–123] and its challenges in the tactical communication context. For tactical bubbles, ML-based security intelligence serves as a mean to capture different threat indicators and thus autonomously orchestrate of security responses.

Reconnaissance and *resource development* are adversarial tactics, which occur before actual attacks and which are also considered first in the table. Reconnaissance can be prevented with by detecting spying activities in the proximity of bubbles and by detecting data breaches and leakage from other systems of public safety authorities. For instance, ML algorithms can be used to analyze network traffic patterns to detect active reconnaissance attempts such as port scanning and enumeration. Anti-reconnaissance outside cyber-domain include visual and radio surveillance to detect potential eavesdroppers on the ground or in the air. For instance, radio frequency fingerprinting of UAV control communication [131] can be used to detect aerial eavesdroppers. Authorities may also initiate counter-reconnaissance activities, i.e., collecting and automatically processing cyber threat intelligence from various open and closed sources [55,133]. Active information sharing enables authorities to be aware of relevant new threats and to update tactical networks continuously. ML can assist in the identification and categorization of vulnerable software and systems by analyzing security advisories, patch notes, and vulnerability databases. This information can then be used to prioritize patching and mitigate the risk posed by vulnerable resources. Intelligent vulnerability scanners [132] can identify weak components and alert the defenders to develop or deploy fixes.

Initial access is denied from outsiders using access controls, physical guarding, and firewalls. As a secondary line of defence, ML-based anomaly detection can identify and block suspicious access attempts in network traffic and thus reduce the success rate of initial access tactics. Access control management can be automated [140–142] to limit the number of users and available resources. For tactical bubbles, it is crucial that there is the capability to authenticate and authorize

all the users and devices that are or later arrive to the operation site. However, at the same time the database containing authorization information should be as small as possible to minimize the risk of leaking organizational data.

The execution of attacks — running malicious code or performing network intrusions — can be mitigated with machine learning models that detect known malicious signatures or anomalies from communication payloads, stored data, or traffic patterns. Tactical bubbles provide specific advantages when detecting and reacting towards anomalous behavior: the approved user applications can be allowlisted. Consequently, when compared to commercial mobile networks, user traffic patterns are more homogeneous and typically also user and traffic amounts are more moderate. As a result, anomalies can be identified with higher certainty and autonomously quarantined. Also, fewer resources are needed, as analysis efforts can focus on fewer traffic types. Nevertheless, as tactical bubbles are deployed in different operations with different users and in differing conditions, it is difficult to build a comprehensive model from the typical or normal user behavior. Each tactical bubble can be characterized as an anomaly itself. Consequently, models must focus on the features that remain constant or are otherwise independent of context where the bubble is deployed. Further, as data flows in individual bubbles may be small and operation-specific, the big data, which is needed by AI to learn, must be collected from various bubbles and other sources and, then, the aggregated big data must be filtered from bubble-specific details.

The mamming of radio channels can be detected and neutralized by physical or cyber means. Machine learning has been considered [146] useful in detecting jamming and also for making communication robust against jamming. But due to the required lengthy training, anti-jamming applications, which adapt dynamically to jammers actions, may not be feasible in temporary tactical bubbles. There are also various research options, e.g., on defenses based on directional antennas and multiple-input/multiple-output technology though they may require antenna hardware, which may not be available for every tactical bubble.

Persistence, command and control, defense evasion tactics can be mitigated with ML algorithms that identify abnormal system behaviors and thus enable the detection of persistent malware and rootkits. Behavior analysis can enhance evasion detection, making it more challenging for attackers to bypass traditional signature-based defenses. An adversary may try to exploit situations where a tactical bubble is disconnected from a remote SOC and, hence, malicious behavior may become visible only when the remote connectivity becomes unavailable. Consequently, behavior differences between connected mode and isolated mode should be closely monitored. The increasing use of ML will increase the importance of data integrity in ML. New solutions, both platform and algorithmic, and research is needed to ensure trustworthiness and robustness of ML against poisoned data sets and evasion attacks.

Collection and leakage of operation or privacy-critical data is primary prevented by cryptography and access control. Machine learning can assist in detecting suspicious data exfiltration attempts or abnormal file access patterns, contributing to the mitigation of data collection tactics. In tactical bubbles, the main concern is the leakage of long term secrets and, hence, both the minimization of critical data stored in bubbles and protection of the edge platform, are essential.

For those applications where data is collected from local bubbles and then shared to a central database, federated learning [158], differentiated privacy [159], and blockchain-based techniques [160] can be viable solutions. However, the privacy problem in general public safety communications is a reverse to the privacy problem in typical federated learning cases: instead of worrying about the privacy of the locally collected data, we need to worry about the confidentiality of the data coming from central repositories or from other bubbles. Hence, the development of AI models that are distributed and stored in bubbles must be done with care so that the models itself do not contain critical information that could be reverse-engineered if leaked.

Leakage of operational information through wireless communication due to traffic analysis, fingerprinting, or weaknesses in 3GPP protocols [161,162], cannot be completely prevented. However, it can mitigated with optimized coverage, by detecting eavesdropping devices, and via the effective use of pseudonymized temporary identifiers.

The impact of the attacks can be detected and limited with different intelligent defense strategies. By analyzing system behavior and user activity, machine learning can contribute to the early detection and mitigation of data destruction, tampering, or encryption caused by attacks. Solutions for adapting the network enable autonomous mitigation of availability related threats. For instance, security-driven prioritization [155] is a concept that was proposed for tactical networks. The concept enables mission-critical applications to adapt QoS level and bandwidth given for users based on user's attested security posture and monitored behavior.

Intent-driven security extends the IBN concepts to meet cybersecurity-related intentions and requirements. IBN inherits the security advantages that software-defined networks introduce, including the ability for centralized control over routing infrastructure, but also introduce new capabilities for automation: presenting security policies and requirements as intentions whose exact implementation is then the responsibility of a machine. For instance, Ooi et al. [157,163] proposed SecurityWeaver system to annotate network service requirements with security-related demands and to automatically create secure network designs. They described security intents with help of MITRE attack matrix based knowledge base: to identify relevant adversarial tactics and recognize appropriate countermeasures into designs. Chowdhary et al. [156] proposed a framework for administrators to express security policies at the abstract application plane level. They also proposed an unified format for intent policies to facilitate multi-domain cooperation.

6. Discussion

6.1. Applicability of analysis methods

Mission-critical systems have some characterizing requirements including *time criticality* (quickly aging of operational information vs. organizational information with mid-term life-time vs. privacy-critical societal with very long life-time), *space dependency* (most threats apply only within bubble, i.e., within the coverage area of a private network), and *latency and reliability criticality*. Threat analysis methods were originally designed for different fields or for generic ICT cyber challenges and hence do not emphasize these characteristics. Nevertheless, all the tested methods were successfully applied for our use cases.

The DREAD method covers five dimensions that relate to the likelihood and impact of the risk. However, mission-critical cases have some of their own priorities and characteristics and it would be valuable to look also these dimensions separately to gain more accurate analysis. Firstly, DREAD does not have a category that would cover the impact time. In mission-critical use, there is a difference whether (a) the adversary impacts ad hoc operations or gains access to temporary identifying information, or whether (b) the adversary gains access to long-term organizational secrets or databases containing critical information on citizens. This can be addressed on the damage-dimension but its own category would benefit in these use cases where there are clearly short-lived and long-lived secrets and assets. Other categories that DREAD misses is the categorization where the damage is, e.g., whether impact is on organizational, operational, or societal assets (though this is quite related to affected users dimension and secondarily related to the damage category). Trust is also one dimension that is missing and highly relevant for critical communication business. Similarly, the basic CVSS does not provide granularity to consider the criticality of assets, e.g., life-time or sensitivity of data.

Our attack matrix for tactical bubbles, composed from several MITRE variants, provides a flexible way to identify and classify the characterizing security issues and solutions. On the other hand, STRIDE and X.805 models provide very high-level categorizations to which the identified relevant threats and security controls are not distributed evenly. However, they provide indications where the main challenges are and what type of security objectives are essential; availability and information disclosure are relevant in almost every identified threat scenario. In the tactical use cases, non-repudiation and privacy controls have fewer identified needs but nevertheless applications requiring these features may emerge.

Our risk assessments for tactical bubbles are qualitative as we made the analysis for emerging technologies for which we have no numerical data on the value of assets nor probability information based on real incident statistics. However, we minimize subjectivity from the valuations by clearly defining the metrics for quantifying the risks and by trying to achieve a consensus on the risk levels within a group of experts. The Delphi method originates outside the cyber-world but it is feasible also for analyzing cyberthreats. It cannot be used when trying to capture complete lists of threats but it can be used as an auxiliary method, in addition to literature and threat databases, to identify, and most importantly, to prioritize use case-specific threats. The main advantage of the Delphi is that it makes results one step more objective.

6.2. Future research

Various security controls listed in Section 5 have potential in the context of tactical bubbles. However, the value and feasibility of many of those solutions for our use case has never been fully evaluated or piloted. Consequently, there is a need for prototypes and trials to gain practical experience. Our use case emphasizes some characteristics that are not typical in AI-based security applications. These characteristics and their potential for future research and prototyping activities are listed in Table 7.

In this article, we presented many security metrics for evaluating the security of tactical networks as well as various security controls. Future research is needed to define and apply metrics for intelligence-based security controls. First, there is a need for better understanding on the security and robustness of ML solutions. In tactical use cases, we need, in particular, assurances that the models that are deployed to bubbles do not contain critical information and could leak information to adversaries and that the models cannot be misused or evaded by the adversaries. Second, we need trust metrics and prototype solutions for platform security and confidential computing. There is a need to precisely understand their advantages and shortcomings. Can confidential computing enable public safety authorities to use communication and computing services within any private mobile network that is operated by civilians?

Security based on AI is a constant battlefield: while the defenders capabilities to detect and mitigate threats evolve, so do adversaries' capabilities to evade detection and cause impact through alternative means. When comparing the tactical communications context to general ICT world, the defenders have few advantages over attackers. First, the systems are closed and attackers have limited knowledge on AI models that the authorities use. Second, the faster the attacks the better the changes being undetected are. However, a big worry in tactical communications are the slow attacks, i.e., advanced persistent threats where the time from initial access to exploitation may take years while a hidden threat is waiting a conflict. During this time, the defenders' capabilities will evolve, increasing the likelihood of catching hidden threats. Potential strategies for slowing down adversarial evolution should be researched. For instance, the customization and increase confidentiality protection of ML models would make it even more difficult for adversaries to learn means to evade detection.

Table 7
Essential security related characteristics of edge intelligence in tactical networks and needs for future research.

Small data	Data collected within a single bubble is small and homogeneous as the number of users and allowed applications are small. Consequently, most anomalies/signs of unrecognized applications are true positive alarms that can be used to trigger aggressive autonomous defenses. Applicability of (autonomous) response strategies in different situations requires future piloting and user studies. Simulated attacks and synthetic data needs to be created to enable teaching in situations where real adversarial data is not available.
Heterogeneous bubbles	Data produced by different bubble instances is different in many aspects as the operations, users, applications, behaviors are different. Large datasets, for learning, can be created from characteristics that remain the same between bubbles, e.g., the behavior of particular applications like IoT.
Leaking bubbles	As the security capabilities of individual bubbles are smaller than capabilities in cloud services, care must be given over what data and models can be shared with bubbles and how this distributed information is protected. Trusted and confidential computing concepts provide an interesting research area in this direction. On the other hand, privacy must be considered for data that is collected from bubbles and federated learning provides one approach for this.
Federated security intelligence	AI-based defenses in a hybrid architecture means that each individual bubble must maintain a sufficient local detection and response capability. How to manage synchronization between local and remote security functions is an open question. Similarly, more research is needed to understand federation capabilities between authorities' bubbles and private civilian networks.
Evolving evasion and detection	ML-based reactive security needs to be constantly developed to respond to new and emerging threats. Adversaries capabilities to evade threat detection evolves and research is needed to understand how defenders can slow down this development and, e.g., keep the ML-models unexplainable for attackers.
Autonomous	In isolated bubbles, the level of autonomy must be high as there are no on-site human security analysts or administrators and as public safety authorities in the field have limited time and skills for configuration. Consequently, security functions that can be deployed to the tactical bubbles are limited to those with zero or minimal configuration efforts. Research is needed to develop and trial such autonomous security intelligence.

The survey provided in this paper is complemented by several practical trials and technology specific analyses that we have made or are currently working on. These efforts include field trials with tactical bubbles [5], with tactical satellite backhauls [164], and with tactical SOCs and dynamic prioritization concept [155]; orchestration of 5G, SOC, and MCX to cloud, edge, and trusted execution environments [165]; as well as security analysis of intent-based networking paradigm [166].

7. Conclusion

We provided a security requirement analysis for an important 6G vertical: for tactical communications of public safety users. The analysis includes a survey of cybersecurity threats and solutions for rapidly deployable mission-critical public safety networks, i.e., for tactical bubbles. We focused to the anticipated features arising from 6G standards and edge intelligence. The main security implications arising from NTN, AI, and the edge include added complexity and an extended

threat surface but also new capabilities and the flexibility to increase resilience and defense against advanced adversaries.

We also assessed and applied several cybersecurity analysis methods: we used them as a classifying foundation for our survey, analyzed their feasibility for mission-critical networks, identified gaps in them, and proposed extensions. Particularly, attack matrices provided us systematic means to identify potential attack vectors, but it served also as a taxonomy that supported our survey over intelligent security solutions. The risk prioritization study based on the Delphi method serves as an example of how to achieve objective cyber-risk assessments for emerging concepts, where real quantitative risk information is unavailable. Security metrics based on STRIDE, DREAD, and CVSS were demonstrated as applicable, with a bearable amount of work for the domain of mobile networks where they were not initially planned.

The foundation of tactical network cybersecurity relies on traditional cyber defenses: on authentication and access control, on cryptographic solutions, on physical security, and on the minimization of information stored in the edge and on the use of high-secure private cloud services for critical assets. Nevertheless, some assets must be brought to the edge and exposed to adversaries in proximity. Intelligent cyber defenses and confidential computing paradigms provide a promising additional layers of defense, which should demonstrated and trialed in the future.

CRediT authorship contribution statement

Jani Suomalainen: Writing – review & editing, Writing – original draft, Project administration, Methodology, Conceptualization. **Ijaz Ahmad:** Writing – original draft. **Annette Shajan:** Writing – original draft. **Tapio Savunen:** Writing – original draft.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Tapio Savunen reports financial support was provided by Airbus. Jani Suomalainen reports financial support was provided by Business Finland. Ijaz Ahmad reports financial support was provided by Business Finland. Annette Shajan reports was provided by Business Finland. Tapio Savunen reports financial support was provided by Business Finland. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work was supported by the AI-NET-ANTILLAS project, funded by Business Finland. The authors are grateful for the consortium members, who participated to the work of the cyber threat analysis task force and/or to the joint risk assessment panel.

References

[1] J. Evans, G. Minden, K. Shanmugan, G. Prescott, V. Frost, B. Ewy, R. Sanchez, C. Sparks, K. Malinimohan, J. Roberts, R. Plumb, D. Petr, The rapidly deployable radio network, IEEE J. Sel. Areas Commun. 17 (4) (1999) 689–703.

[2] K. Miranda, A. Molinaro, T. Razafindralambo, A survey on rapidly deployable solutions for post-disaster networks, IEEE Commun. Mag. 54 (4) (2016) 117–123.

[3] 3GPP, Isolated evolved universal terrestrial radio access network (E-UTRAN) operation for public safety. TS 22.346. Release 13, 2014.

[4] J. Hallio, R. Ekman, J. Kalliovaara, T. Lakner, J. Auranen, A. Arajärvi, T. Jokela, J. Paavola, H. Kokkinen, T. Savunen, et al., Rapidly deployable network system for critical communications in remote locations, in: 2019 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting, BMSB, IEEE, 2019, pp. 1–5.

[5] M. Heikkilä, P. Koskela, J. Suomalainen, K. Lähetkangas, T. Kippola, P. Eteläaho, J. Erkkilä, A. Pouttu, Field trial with tactical bubbles for mission critical communications, Trans. Emerg. Telecommun. Technol. 33 (1) (2022) e4385.

[6] 3GPP, Mission critical services support in the isolated operation for public safety (IOPS) mode of operation. TS 23.180. Release 17, 2019.

[7] The Critical Communications Association, Mission critical broadband applications, TCCA white paper, 2022.

[8] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G.K. Karagiannidis, P. Fan, 6G wireless networks: Vision, requirements, architecture, and key technologies, IEEE Veh. Technol. Mag. 14 (3) (2019) 28–41.

[9] M.Z. Chowdhury, M. Shahjalal, S. Ahmed, Y.M. Jang, 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions, IEEE Open J. Commun. Soc. 1 (2020) 957–975.

[10] L.-H. Shen, K.-T. Feng, L. Hanzo, Five facets of 6G: Research challenges and opportunities, ACM Comput. Surv. 55 (11) (2023) 1–39.

[11] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, Overview of 5G security challenges and solutions, IEEE Commun. Stand. Mag. 2 (1) (2018) 36–43.

[12] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, A. Rezaki, Security and trust in the 6G era, IEEE Access 9 (2021) 142314–142327.

[13] P. Porambage, G. Gür, D.P.M. Osorio, M. Liyanage, A. Gurtov, M. Ylianttila, The roadmap to 6G security and privacy, IEEE Open J. Commun. Soc. 2 (2021) 1094–1122.

[14] P. Ranaweera, A.D. Jurcut, M. Liyanage, Survey on multi-access edge computing security and privacy, IEEE Commun. Surv. Tutor. 23 (2) (2021) 1078–1124.

[15] J.L. Burbank, P.F. Chimento, B.K. Haberman, W.T. Kasch, Key challenges of military tactical networking and the elusive promise of MANET technology, IEEE Commun. Mag. 44 (11) (2006) 39–45.

[16] J.G. Ponsam, R. Srinivasan, A survey on MANET security challenges, attacks and its countermeasures, Int. J. Emerg. Trends Technol. Comput. Sci. (IJETTCS) 3 (1) (2014) 274–279.

[17] M. Ďulík, M. Ďulík, Cyber security challenges in future military battlefield information networks, Adv. Mil. Technol. 14 (2) (2019) 263–277.

[18] J. Suomalainen, J. Julku, M. Vehkaperä, H. Posti, Securing public safety communications on commercial and tactical 5G networks: A survey and future research directions, IEEE Open J. Commun. Soc. 2 (2021) 1590–1615.

[19] L. Bastos, G. Capela, A. Koprulu, G. Elzinga, Potential of 5G technologies for military application, in: 2021 International Conference on Military Communication and Information Systems, ICMCIS, IEEE, 2021, pp. 1–8.

[20] M. Barreno, B. Nelson, R. Sears, A.D. Joseph, J.D. Tygar, Can machine learning be secure? in: Proc. 2006 ACM Symposium on Information, Computer and Communications Security, ASIACS'06, ACM, New York, NY, USA, ISBN: 1-59593-272-0, 2006, pp. 16–25.

[21] N. Papernot, P. McDaniel, A. Sinha, M.P. Wellman, SoK: Security and privacy in machine learning, in: Proc. 2018 IEEE European Symposium on Security and Privacy, EuroS&P, IEEE, 2018, pp. 399–414.

[22] J.-h. Li, Cyber security meets artificial intelligence: a survey, Front. Inf. Technol. Electron. Eng. 19 (12) (2018) 1462–1474.

[23] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mämmelä, I. Ahmad, Machine learning threatens 5G security, IEEE Access 8 (2020) 190822–190842.

[24] D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza, Automation for network security configuration: state of the art and research trends, ACM Comput. Surv. (2023).

[25] A. Shostack, Experiences threat modeling at microsoft, in: Proceedings of the Workshop on Modeling Security (MODSEC08) Held As Part of the 2008 International Conference on Model Driven Engineering Languages and Systems, MODELS, 2008.

[26] B.E. Strom, A. Applebaum, D.P. Miller, K.C. Nickels, A.G. Pennington, C.B. Thomas, Mitre att&ck: Design and philosophy, in: Technical Report, The MITRE Corporation, 2018.

[27] OpenStack, Security/OSSA-metrics, 2014, Online: https://wiki.openstack.org/wiki/Security/OSSA-Metrics.

[28] FIRST, Common vulnerability scoring system v3.1. Specification document, 2019.

[29] B.B. Brown, Delphi Process: A Methodology Used for the Elicitation of Opinions of Experts, Rand Corporation Santa Monica, CA, 1968.

[30] ITU-T, X.805: Security architecture for systems providing end-to-end communications, 2003, Available online at www.itu.int/rec/T-REC-X.805-200310-I/en.

[31] J. Oueis, V. Conan, D. Lavaux, R. Stanica, F. Valois, Overview of LTE isolated E-UTRAN operation for public safety, IEEE Commun. Stand. Mag. 1 (2) (2017) 98–105.

[32] C.D. Barca, et al., Information security in digital trunking systems, Database Syst. J. 8 (1) (2017) 40–48.

[33] 3GPP, Policy and charging control framework for the 5G system (5GS). TS 23.503. Release 17, 2021.

[34] G.P. Gomez, J.M. Batalla, Y. Miche, S. Holtmanns, C.X. Mavromoustakis, G. Mastorakis, N. Haider, Security policies definition and enforcement utilizing policy control function framework in 5G, Comput. Commun. 172 (2021) 226–237.

[35] M. Höyhtyä, K. Lähetkangas, J. Suomalainen, M. Hoppari, K. Kujanpää, K.T. Ngo, T. Kippola, M. Heikkilä, H. Posti, J. Mäki, et al., Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and qos control, IEEE Access 6 (2018) 73572–73582.

[36] T. Savunen, H. Hämmäinen, K. Kilkki, P. Kekolahti, The role of mobile network operators in next-generation public safety services, Telecommun. Policy 47 (3) (2023) 102489.

[37] A. Sullivan, E. Baker, T. Kurvits, A. Popescu, A.K. Paulson, A. Cardinal Christianson, A. Tulloch, B. Bilbao, C. Mathison, C. Robinson, et al., Spreading Like Wildfire: The Rising Threat of Extraordinary Landscape Fires, United Nations Environment Programme, 2022.

[38] Congressional Research Service, Wildfire statistics, report IF 10244, 2023.

[39] F. Scalera, When wildfires spark, FirstNet wildfire response team is ready. AT&T blog, 2022.

[40] Airbus, What 5G could mean for mission-critical users — right now? Whitepaper, 2023.

[41] M. Peltola, H. Hämmäinen, Effect of population density and network availability on deployment of broadband PPDR mobile network service, Digit. Policy Regul. Gov. 20 (1) (2018) 78–96.

[42] T. Savunen, P. Kekolahti, P. Mähönen, H. Hämmäinen, K. Kilkki, Mobile network operators' business risks in next-generation public safety services, in: Proceedings of the 32nd European Conference of the International Telecommunications Society, ITS, 2023.

[43] 5G-PPP, The 6G Architecture Landscape: European Perspective. White Paper, European Commission, 2023.

[44] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, J.S. Thompson, E.G. Larsson, M.D. Renzo, W. Tong, P. Zhu, X. Shen, H.V. Poor, L. Hanzo, On the road to 6G: Visions, requirements, key technologies, and testbeds, IEEE Commun. Surv. Tutor. 25 (2) (2023) 905–974.

[45] D. Zhou, M. Sheng, J. Li, Z. Han, Aerospace integrated networks innovation for empowering 6G: A survey and future challenges, IEEE Commun. Surv. Tutor. 25 (2) (2023) 975–1019.

[46] I. Ahmad, J. Suomalainen, P. Porambage, A. Gurtov, J. Huusko, M. Höyhtyä, Security of satellite-terrestrial communications: Challenges and potential solutions, IEEE Access 10 (2022) 96038–96052.

[47] I. Ahmad, S. Shahabuddin, H. Malik, E. Harjula, T. Leppänen, L. Lovén, A. Anttonen, A.H. Sodhro, M. Mahtab Alam, M. Juntti, A. Ylä-Jääski, T. Sauter, A. Gurtov, M. Ylianttila, J. Riekki, Machine learning meets communication networks: Current trends and future challenges, IEEE Access 8 (2020) 223418–223460.

[48] ETSI, Experiential networked intelligence (ENI); ENI use cases; standard ETSI GR ENI 001, 2011.

[49] C.E. Landwehr, Cybersecurity and artificial intelligence: From fixing the plumbing to smart water, IEEE Secur. Priv. 6 (5) (2008) 3–4.

[50] Y. Wei, M. Peng, Y. Liu, Intent-based networks for 6G: Insights and challenges, Digit. Commun. Netw. 6 (3) (2020) 270–280.

[51] E. Zeydan, Y. Turk, Recent advances in intent-based networking: A survey, in: 2020 IEEE 91st Vehicular Technology Conference, VTC2020-Spring, IEEE, 2020, pp. 1–5.

[52] K.C. Apostolakis, N. Dimitriou, G. Margetis, S. Ntoa, D. Tzovaras, C. Stephanidis, DARLENE–Improving situational awareness of European law enforcement agents through a combination of augmented reality and artificial intelligence solutions, Open Research Europe 1 (87) (2022) 87.

[53] N.D. Huynh, M.R. Bouadjenek, I. Razzak, K. Lee, C. Arora, A. Hassani, A. Zaslavsky, Adversarial attacks on speech recognition systems for mission-critical applications: A survey, 2022, arXiv:2202.10594.

[54] Y. Ma, Z. Wang, H. Yang, L. Yang, Artificial intelligence applications in the development of autonomous vehicles: A survey, IEEE/CAA J. Autom. Sin. 7 (2) (2020) 315–329.

[55] J.R.G. Evangelista, R.J. Sassi, M. Romero, D. Napolitano, Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence, J. Appl. Secur. Res. 16 (3) (2021) 345–369.

[56] J. Li, K.K. Nagalapur, E. Stare, S. Dwivedi, S.A. Ashraf, P.-E. Eriksson, U. Engström, W.-H. Lee, T. Lohmar, 5G new radio for public safety mission critical communications, IEEE Commun. Stand. Mag. 6 (4) (2022) 48–55.

[57] F. Neto, J. Granjal, V. Pereira, A survey on security approaches on PPDR systems toward 5G and beyond, IEEE Access 10 (2022) 117118–117140.

[58] S. Roy, M.J. Nene, Analysis and recommendations for network and communication security for mission critical infrastructure, in: 2016 3rd International Conference on Advanced Computing and Communication Systems, Vol. 01, ICACCS, 2016, pp. 1–8.

[59] G. Fodor, S. Parkvall, S. Sorrentino, P. Wallentin, Q. Lu, N. Brahmi, Device-to-device communications for national security and public safety, IEEE Access 2 (2014) 1510–1520.

[60] J.H. Sarker, A.M. Nahhas, A secure wireless mission critical networking system for unmanned aerial vehicle communications, Telecommun. Syst. 69 (2018) 237–251.

[61] Z. Laaroussi, E.U. Soykan, M. Liljenstam, U. Gülen, L. Karaçay, E. Tomur, On the security of 6G use cases: Threat analysis of'all-senses meeting', in: 2022 IEEE 19th Annual Consumer Communications & Networking Conference, CCNC, IEEE, 2022, pp. 1–6.

[62] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, M. Blaze, Why (Special agent) johnny (Still) can't encrypt: A security analysis of the APCO project 25 two-way radio system, in: USENIX Security Symposium, Vol. 2011, 2011, pp. 8–12.

[63] A.R. McGee, M. Coutière, M.E. Palamara, Public safety network security considerations, Bell Labs Tech. J. 17 (3) (2012) 79–86.

[64] H. Ghafghazi, A. El Mougy, H.T. Mouftah, C. Adams, Security and privacy in LTE-based public safety network, in: Wireless Public Safety Networks 2, Elsevier, 2016, pp. 317–364.

[65] B. Sheehan, F. Murphy, A.N. Kia, R. Kiely, A quantitative bow-tie cyber risk classification and assessment framework, J. Risk Res. 24 (12) (2021) 1619–1638.

[66] D. Sattar, A.H. Vasoukolaei, P. Crysdale, A. Matrawy, A stride threat model for 5g core slicing, in: 2021 IEEE 4th 5G World Forum, 5GWF, IEEE, 2021, pp. 247–252.

[67] J. Suomalainen, J. Julku, M. Vehkaperä, H. Posti, Securing public safety communications on commercial and tactical 5g networks: A survey and future research directions, IEEE Open J. Commun. Soc. 2 (2021) 1590–1615.

[68] M. Cagnazzo, M. Hertlein, T. Holz, N. Pohlmann, Threat modeling for mobile health systems, in: 2018 IEEE Wireless Communications and Networking Conference Workshops, WCNCW, IEEE, 2018, pp. 314–319.

[69] S. Figueroa-Lorenzo, J. Añorga, S. Arrizabalaga, A survey of iIoT protocols: A measure of vulnerability risk analysis based on CVSS, ACM Comput. Surv. 53 (2) (2020) 1–53.

[70] F.M. Chen, Y.Q. Liu, Research on the risk factors of mobile business: based on the sorting delphi method, Int. J. Eng. Res. Afr. 21 (2016) 215–230.

[71] M.A. Almaiah, F. Hajjej, A. Lutfi, A. Al-Khasawneh, T. Alkhdour, O. Almomani, R. Shehab, A conceptual framework for determining quality requirements for mobile learning applications using delphi method, Electronics 11 (5) (2022) 788.

[72] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P.K. Nakarmi, M. Näslund, P. O'Hanlon, et al., A security architecture for 5G networks, IEEE Access 6 (2018) 22466–22479.

[73] N. Papakonstantinou, D.L.V. Bossuyt, B. Hale, R. Arlitt, J. Salonen, J. Suomalainen, CyberRiskDELPHI: Towards objective cyber risk assessment for complex systems, in: International Design Engineering Technical Conferences / Computers and Information in Engineering Conference, IDETC/CIE2023, 2023.

[74] NIST, Common vulnerability scoring system calculator. CVSS version 3.1, 2023, Available online at.

[75] GitHub, CVSS vectors, 2023, Available online at https://github.com/SuomalainenJani/antillas_cvss/wiki/CVSS-vectors.

[76] MITRE, ATT&CK®, 2023, Available online at https://attack.mitre.org/.

[77] MITRE, ATLAS, 2023, Available online at https://atlas.mitre.org/.

[78] MITRE, FiGHT. Version 1.0.1, 2023, Available online at https://fight.mitre.org/.

[79] Aerospace, SPARTA: Space attack research and tactic analysis, 2023, Available online at.

[80] S.P. Rao, H.-Y. Chen, T. Aura, Threat modeling framework for mobile communication systems, Comput. Secur. 125 (2023) 103047.

[81] M. Lichtman, R. Rao, V. Marojevic, J. Reed, R.P. Jover, 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation, in: 2018 IEEE International Conference on Communications Workshops, ICC Workshops, IEEE, 2018, pp. 1–6.

[82] K. Vaishnavi, S.D. Khorvi, R. Kishore, S. Gurugopinath, A survey on jamming techniques in physical layer security and anti-jamming strategies for 6G, in: 2021 28th International Conference on Telecommunications, ICT, IEEE, 2021, pp. 174–179.

[83] M.S. Kang, Potential security concerns at the physical layer of 6G cellular systems, in: 2022 13th International Conference on Information and Communication Technology Convergence, ICTC, IEEE, 2022, pp. 981–984.

[84] ENISA, Telecom security incidents 2021, report, 2022.

[85] J. Suomalainen, I. Ahmad, Cybersecurity for machines in satellite-terrestrial networks, in: Integrating Machine-Type-Communication (MTC) and Satellites for IoT: Towards 6G, Wiley-IEEE Press, 2024.

[86] NIST, Identifying and categorizing data types for public safety mobile applications: Workshop report. NISTIR 8135, 2016.

[87] NIST, Standards for security categorization of federal information and information systems, federal information processing standard (FIPS) 199, 2004.

[88] X. Lin, An overview of 5G advanced evolution in 3GPP release 18, IEEE Commun. Stand. Mag. 6 (3) (2022) 77–83.

[89] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, Security for 5G and beyond, IEEE Commun. Surv. Tutor. 21 (4) (2019) 3682–3722.

[90] ETSI, Network functions virtualisation (NFV); NFV security; Security and trust guidance. Standard. ETSI GS NFV-SEC 003, 2014.

[91] ETSI, System architecture specification for execution of sensitive NFV components. Standard. ETSI GS NFV-SEC 012, 2017.

[92] ETSI, Network functions virtualisation (NFV) release 3; Security specification for MANO components and reference points. Standard. ETSI GS NFV-SEC 014, 2018.

[93] ETSI, Zero-touch network and service management (ZSM); General security aspects. Standard. ETSI GSM ZSM 010, 2021.

[94] ETSI, Network functions virtualisation (NFV) release 3; VNF package security specifications. Standard. ETSI GS NFV-SEC 021, 2019.

[95] ETSI, NFV security; Cataloguing security features in management software. Standard. ETSI GS NFV-SEC 002, 2015.

[96] ETSI, Network functions virtualisation (NFV) release 3; Security management and monitoring specification. Standard. ETSI GS NFV-SEC 013, 2017.

[97] International Standardization Organization, Artificial intelligence. Data quality for analytics and machine learning (ML). Part 1: Overview, terminology, and examples. ISO/IEC FDIS 5259-1, 2024.

[98] NIST, IoT device cybersecurity guidance for the federal government: Establishing IoT device cybersecurity requirements. SP 800-213, 2021.

[99] NIST, Artificial intelligence risk management framework (AI RMF 1.0), 2023.

[100] ENISA, Baseline security recommendations for IoT, 2017.

[101] ENISA, Multilayer framework for good cybersecurity practices for AI, 2023.

[102] European Union Aviation Safety Agency, Concepts of design assurance for neural networks (CoDANN), Public report, 2020.

[103] The Critical Communications Association, Security considerations for interconnection of TETRA and mission critical broadband systems, White paper, 2018.

[104] I. Ahmad, F. Rodriguez, T. Kumar, J. Suomalainen, S.K. Jagatheesaperumal, S. Walter, M.Z. ASGHAR, G. Li, N. Papakonstantinou, M. Ylianttila, J. Huusko, T. Sauter, E. Harjula, Communications security in industry X: A survey, IEEE Open J. Commun. Soc. (2024).

[105] Ministry of Foregin Affairs of Finland, Information security auditing tool for authorities - Katakri, 2020.

[106] NIST, Security and privacy controls for information systems and organizations. SP 800-53 Rev. 5, 2020.

[107] GSMA, Network equipment security assurance scheme—Overview. FS.13, 2019.

[108] 3GPP, Security assurance methodology (SCAS) for 3GPP network products, TR 33.916, 2019.

[109] 3GPP, Security Architecture and Procedures for 5G System. TS 33.501. Release 18, 3GPP, 2022.

[110] 3GPP, Security of the mission critical service. TS 33.180. Release 17, 2023.

[111] OASIS Open, CACAO security playbooks version 2.0, specification, 2023.

[112] 3GPP, Study on 5G system support for AI/ML-based services. TR 23.700-80. release 18, 2022.

[113] 3GPP, Study on security aspects of enhancement of support for edge computing in the 5G core (5GC). TR 33.839, 2023.

[114] 3GPP, Security aspects of enhancement of support for enabling edge applications. TS 33.558, 2023.

[115] 3GPP, Study on security enhancement of support for edge computing phase 2. TR 33.739. Release 18, 2023.

[116] X. Lin, S. Rommer, S. Euler, E.A. Yavuz, R.S. Karlsson, 5G from space: An overview of 3GPP non-terrestrial networks, IEEE Commun. Stand. Mag. 5 (4) (2021) 147–153.

[117] M. El Jaafari, N. Chuberre, S. Anjuere, L. Combelles, Introduction to the 3GPP-defined NTN standard: A comprehensive view on the 3GPP work on NTN, Int. J. Satell. Commun. Netw. 41 (3) (2023) 220–238.

[118] 3GPP, Mission critical services (MCS) identity management; Protocol specification. TS 24.482. Release 18, 2023.

[119] S.I. Salim, A Deep Dive into the Packet Reflection Vulnerability Allowing Attackers to Plague Private 5G Networks, TrendMicro, 2023.

[120] I. Ahmad, S. Namal, M. Ylianttila, A. Gurtov, Security in software defined networks: A survey, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2317–2346.

[121] N.N. Abbas, T. Ahmed, S.H.U. Shah, M. Omar, H.W. Park, Investigating the applications of artificial intelligence in cyber security, Scientometrics 121 (2) (2019) 1189–1211.

[122] J. Banerjee, S. Maiti, S. Chakraborty, S. Dutta, A. Chakraborty, J.S. Banerjee, Impact of machine learning in various network security applications, in: 2019 3rd International Conference on Computing Methodologies and Communication, ICCMC, IEEE, 2019, pp. 276–281.

[123] V. Ford, A. Siraj, Applications of machine learning in cyber security, in: 27th International Conference on Computer Applications in Industry and Engineering, vol. 118, IEEE, 2014.

[124] A. Tundis, S. Ruppert, M. Mühlhäuser, On the automated assessment of open-source cyber threat intelligence sources, in: Proceedings of the 20th International Conference on Computational Science–ICCS 2020, Springer, 2020, pp. 453–467.

[125] R. Riesco, V.A. Villagrá, Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (STIX™, SWRL and OWL), Int. J. Inf. Secur. 18 (6) (2019) 715–739.

[126] W.Z.A. Zakaria, M.L.M. Kiah, A review on artificial intelligence techniques for developing intelligent honeypot, in: 2012 8th International Conference on Computing Technology and Information Management, Vol. 2, NCM and ICNIT, IEEE, 2012, pp. 696–701.

[127] J.-H. Cho, D.P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T.J. Moore, D.S. Kim, H. Lim, F.F. Nelson, Toward proactive, adaptive defense: A survey on moving target defense, IEEE Commun. Surv. Tutor. 22 (1) (2020) 709–745.

[128] T.A. Główka, Moving Target Defence Against the Active Reconnaissance, (Master's thesis), Warsaw University of Technology, 2021.

[129] H. Galadima, A. Seeam, V. Ramsurrun, Cyber deception against DDoS attack using moving target defence framework in SDN IOT-EDGE networks, in: 2022 3rd International Conference on Next Generation Computing Applications, NextComp, IEEE, 2022, pp. 1–6.

[130] J. Flórez, J. Ortega, A. Betancourt, A. García, M. Bedoya, J.S. Botero, A review of algorithms, methods, and techniques for detecting UAVs and UAS using audio, radiofrequency, and video applications, Tecnológicas 23 (48) (2020) 262–278.

[131] W. Nie, Z.-C. Han, M. Zhou, L.-B. Xie, Q. Jiang, UAV detection and identification based on WiFi signal and RF fingerprint, IEEE Sens. J. 21 (12) (2021) 13540–13550.

[132] R. Tommy, G. Sundeep, H. Jose, Automatic detection and correction of vulnerabilities using machine learning, in: 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication, CTCEEC, IEEE, 2017, pp. 1062–1065.

[133] V. Jakkal, Microsoft security copilot early access program: Harnessing generative AI to empower security teams. Blog article, 2023.

[134] K. Gai, M. Qiu, L. Tao, Y. Zhu, Intrusion detection techniques for mobile cloud computing in heterogeneous 5G, Secur. Commun. Netw. 9 (16) (2016) 3049–3058.

[135] N. Yadav, S. Pande, A. Khamparia, D. Gupta, Intrusion detection system on IoT with 5G network using deep learning, Wirel. Commun. Mob. Comput. 2022 (2022) 1–13.

[136] N. Hu, Z. Tian, H. Lu, X. Du, M. Guizani, A multiple-kernel clustering based intrusion detection scheme for 5g and IoT networks, Int. J. Mach. Learn. Cybern. (2021) 1–16.

[137] M.A. Rahman, M.S. Hossain, A deep learning assisted software defined security architecture for 6g wireless networks: IIoT perspective, IEEE Wirel. Commun. 29 (2) (2022) 52–59.

[138] F. Jiang, T. Gu, L. Chang, Z. Xu, Case retrieval for network security emergency response based on description logic, in: 8th IFIP TC 12 International Conference, Springer, 2014, pp. 284–293.

[139] I. Kraeva, G. Yakhyaeva, Application of the metric learning for security incident playbook recommendation, in: 2021 IEEE 22nd International Conference of Young Professionals in Electron Devices and Materials, EDM, IEEE, 2021, pp. 475–479.

[140] E. Abramov, D. Mordvin, O. Makarevich, Automated method for constructing of network traffic filtering rules, in: Proceedings of the 3rd International Conference on Security of Information and Networks, 2010, pp. 203–211.

[141] NIST, Machine Learning for Access Control Policy Verification, Report 8360, Technical Report, 2021.

[142] N. Wagner, C.Ş. Şahin, M. Winterrose, J. Riordan, J. Pena, D. Hanson, W.W. Streilein, Towards automated cyber decision support: A case study on network segmentation for security, in: 2016 IEEE Symposium Series on Computational Intelligence, SSCI, IEEE, 2016, pp. 1–10.

[143] L. Argento, A. Margheri, F. Paci, V. Sassone, N. Zannone, Towards adaptive access control, in: Proceedings of the 32nd Annual IFIP WG 11.3 Conference, Springer, 2018, pp. 99–109.

[144] A. Almehmadi, K. El-Khatib, On the possibility of insider threat prevention using intent-based access control (IBAC), IEEE Syst. J. 11 (2) (2015) 373–384.

[145] B.A. Khalaf, S.A. Mostafa, A. Mustapha, M.A. Mohammed, W.M. Abduallah, Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods, IEEE Access 7 (2019) 51691–51713.

[146] Y. Arjoune, S. Faruque, Smart jamming attacks in 5G new radio: A review, in: 2020 10th Annual Computing and Communication Workshop and Conference, CCWC, IEEE, 2020, pp. 1010–1015.

[147] A. Gupta, R.K. Jha, S. Jain, Attack modeling and intrusion detection system for 5G wireless communication network, Int. J. Commun. Syst. 30 (10) (2017) e3237.

[148] A. Alotaibi, A. Barnawi, IDSoft: A federated and softwarized intrusion detection framework for massive internet of things in 6G network, J. King Saud Univ.-Comput. Inf. Sci. (2023) 101575.

[149] H.W. Oleiwi, D.N. Mhawi, H. Al-Raweshidy, A meta-model to predict and detect malicious activities in 6G-structured wireless communication networks, Electronics 12 (3) (2023) 643.

[150] I.T. Aktolga, E.S. Kuru, Y. Sever, P. Angin, AI-driven container security approaches for 5G and beyond: A survey, ITU J. Future Evol. Technol. 4 (2) (2023) 364–386.

[151] H. Sedjelmaci, N. Ansari, Zero trust architecture empowered attack detection framework to secure 6G edge computing, IEEE Netw. (2023).

[152] M.A. Elsadig, A. Gafar, Covert channel detection: machine learning approaches, IEEE Access 10 (2022) 38391–38405.
[153] A. Jagannath, J. Jagannath, P.S.P.V. Kumar, A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges, Comput. Netw. (2022) 109455.
[154] J.-B. Wang, J. Wang, Y. Wu, J.-Y. Wang, H. Zhu, M. Lin, J. Wang, A machine learning framework for resource allocation assisted by cloud computing, IEEE Netw. 32 (2) (2018) 144–151.
[155] J. Suomalainen, J. Julku, A. Heikkinen, S.J. Rantala, A. Yastrebova, Security-driven prioritization for tactical mobile networks, J. Inf. Secur. Appl. 67 (2022) 103198.
[156] A. Chowdhary, A. Sabur, N. Vadnere, D. Huang, Intent-driven security policy management for software-defined systems, IEEE Trans. Netw. Serv. Manag. (2022).
[157] S.E. Ooi, R. Beuran, T. Kuroda, T. Kuwahara, R. Hotchi, N. Fujita, Y. Tan, Intent-driven secure system design: Methodology and implementation, Comput. Secur. 124 (2023) 102955.
[158] Y. Cheng, Y. Liu, T. Chen, Q. Yang, Federated learning for privacy-preserving AI, Commun. ACM 63 (12) (2020) 33–36.
[159] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, Y.-D. Lin, Security and privacy for 6G: A survey on prospective technologies and challenges, IEEE Commun. Surv. Tutor. 23 (4) (2021) 2384–2428.
[160] G. Fragkos, C. Minwalla, J. Plusquellic, E.E. Tsiropoulou, Artificially intelligent electronic money, IEEE Consum. Electron. Mag. 10 (4) (2021) 81–89.
[161] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, J.-P. Seifert, Practical attacks against privacy and availability in 4G/LTE mobile communication systems, in: 23rd Annual Network and Distributed System Security Symposium, NDSS 2016, Internet Society, 2016.
[162] A. Shaik, R. Borgaonkar, S. Park, J.-P. Seifert, New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities, in: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, 2019, pp. 221–231.
[163] S.E. Ooi, R. Beuran, Y. Tan, T. Kuroda, T. Kuwahara, N. Fujita, SecureWeaver: Intent-driven secure system designer, in: Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, 2022, pp. 107–116.
[164] H. Kokkoniemi-Tarkkanen, K. Ahola, J. Suomalainen, M. Höyhtyä, M. Säynevirta, Mission-critical connectivity over OneWeb system in Finland: Architecture and measurements, in: Winter Satellite Workshop, 2024.
[165] J. Suomalainen, K. Ahola, M. Sailio, G. Kiss, G. Megyaszai, R. Asif, P. Jehkonen, J. Rivalan, Tactical orchestration: Network, security, and drone intelligence for mission-critical operations, in: European Conference on Networks and Communications, EuCNC, 2024.
[166] I. Ahmad, J. Malinen, F. Christou, P. Porambage, A. Kirstaedter, J. Suomalainen, Security in intent-based networking: Challenges and solutions, in: IEEE Conference on Standards for Communications and Networking, CSCN 2023, 2023.

Jani Suomalainen is a senior scientist in VTT Technical Research Centre of Finland in Espoo. He received his M.Sc. degree in information technology from Lappeenranta University of Technology, and D.Sc. degree on telecommunications software from Aalto University. Jani is specialized in cyber and network security and has over twenty years of experience on different cybersecurity topics. He has participated to several European and Finnish cooperation projects studying security in 5G/6G networks and in tactical private networks for public safety communications. His research interests include threat modeling, security architectures, and intelligent security solutions.

Dr. **Ijaz Ahmad** is a senior scientist in VTT Technical Research Centre of Finland, and an adjunct professor at the University of Oulu, Finland. He received his M.Sc. and D.Sc. degrees in the field of telecommunications from the University of Oulu, Finland, in 2012, and 2018, respectively. Dr. Ijaz has been a visiting scientist at the Technical University of Vienna, Austria (2019), at Aalto University Finland (2018), and is the recipient of several awards including the Nokia Foundation, Tauno Tönning and Jorma Ollila grant awards, and the VTT research excellence awards in 2021 and 2023. Furthermore, Dr. Ijaz has received two best paper awards at IEEE conferences. His research interests include cybersecurity, security of 5G and 6G.

Annette Shajan is a Master's student pursuing her dual degree across University of Turku, Finland and EURECOM, France majoring in Cybersecurity. She pursued her Bachelor's in Computer Science from Bangalore, India. Her interests lie in offensive security research, threat intelligence, malware analysis and the application of AI with cyber defence. She also has a year of work experience as a full stack developer at JP Morgan Chase.

Tapio Savunen works as director of strategic marketing at Airbus Defence and Space in the Secure Land Communications business. In addition, he is a doctoral student at Aalto University. Tapio graduated from the Helsinki University of Technology with a master's degree in engineering and holds several international patents in the field of mobile communications. He is also involved in several European and Finnish research projects addressing the development of critical communications. His research interests include mobile network operators' new business opportunities in the public safety market.