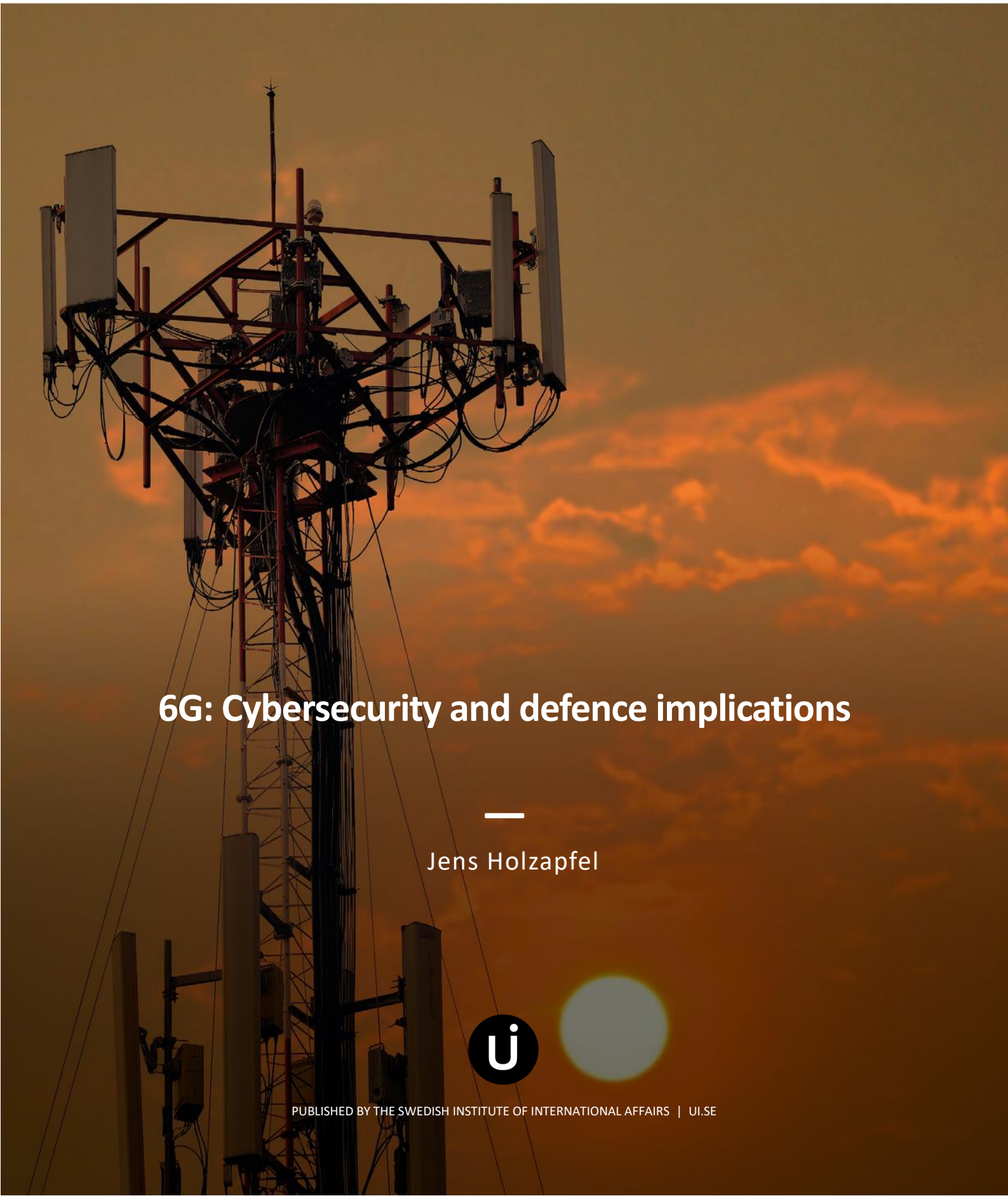
brief

5/2025



6G: Cybersecurity and defence implications

Jens Holzapfel

PUBLISHED BY THE SWEDISH INSTITUTE OF INTERNATIONAL AFFAIRS | UI.SE

Jens Holzapfel

Jens Holzapfel is a cybersecurity and defence expert. Jens has served close to two decades in the Swedish government where he held various managerial and analytical national security roles.

This UI Brief is based on research within the Europe program, made possible through financial support provided by The Swedish Ministry of Foreign Affairs. The views and opinions expressed in the report are those of the author.

Language review: Andrew Mash
Cover photo: TT NYHETSBYRÅN

Introduction

This paper examines the cybersecurity and defence dimensions of sixth-generation (6G) networks. It highlights the importance of security in mobile networks and explores key technological features of 6G that might introduce new threat vectors. To illustrate these risks, this UI Brief analyses 6G security implications through the lens of the Hexa-X-II use case families to show how adversaries might exploit vulnerabilities in domains such as immersive experiences or collaborative robotics. Finally, it emphasises how 6G's enhanced connectivity and data-sharing capabilities could enhance European defence forces by enabling more effective intelligence gathering, strategic coordination and tactical precision on future battlefields.

Mobile Networks and Cybersecurity

Mobile networks form the backbone of today's digital societies, not only providing voice and messaging services, but also facilitating critical functions such as financial transactions, public safety communications and industrial controls. Because these networks transport high-value data and support essential infrastructure, from energy and finance to emergency response, they are prime targets for cyberattacks that seek to steal information, disrupt services or conduct prolonged surveillance.

A noteworthy example of a cyberattack on mobile networks is *Operation Softcell*, which was discovered in 2019. This was a sophisticated campaign attributed to a Chinese state-sponsored group that targeted multiple telecommunications operators worldwide for subscriber data and other sensitive information.[1] Another is the Vodafone Greece hack of 2004–2005, in which vulnerabilities in Ericsson's infrastructure were exploited to enable illicit wiretapping of government officials and other high-profile individuals.[2] More recently, the Chinese threat actor known as *Liminal Panda* used social engineering and technical intrusion techniques to penetrate telecom operators' internal IT networks, allowing real-time monitoring and data exfiltration over extended periods.[3]

Despite the emergence of newer standards, legacy protocols from earlier generations remain in use for inter-carrier communication and within-network cores. For instance, SS7, which was designed in the 1970s and developed on a trust-based architecture that lacks robust authentication, still underpins signalling among telecom providers. This makes intercepting calls or

[1] Cybereason Intelligence (2019). *Operation Softcell: A Worldwide Campaign Against Telecoms.* [Online]. https://www.cybereason.com/blog/research/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

[2] V. Prevelakis, D. Spinellis (2007). "The Athens Affair" [Online]. https://spectrum.ieee.org/the-athens-affair

[3] Crowdstrike Blog (2024). *Unveiling LIMINAL PANDA: A Closer Look at China's Cyber Threats to the Telecom Sector.* [Online]. https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/

rerouting traffic possible if an attacker can access an SS7 node.[4] In addition, Diameter, which was introduced to enhance SS7 for 4G and 5G, remains susceptible to misconfigurations and weak authentication, allowing attackers to inject rogue signalling messages.[5] Similarly, the *GPRS Tunnelling Protocol*, used in 3G and 4G, as well as parts of 5G, provides insufficient authentication in the control plane, which makes session hijacking and IP spoofing feasible. The *Session Initiation Protocol*, relied on for 5G voice services, can also be compromised if not secured with robust encryption and session authentication. In highly interconnected telecom environments, a breach in one operator's infrastructure can quickly spread through cross-carrier trust relationships.

Attackers might also aim to disrupt entire mobile networks, as evidenced by the late 2023 attack on the Ukrainian telecom operator Kyivstar,[6] which left customers without services for several days. Fortunately, the incident did not affect communications for the Ukrainian armed forces or cause physical damage. However, in scenarios where mobile networks support mission-critical functions, security failures can have severe real-world repercussions.

Security in 6G: Emerging Challenges and Strengthening Measures

The shift to sixth-generation networks opens up unprecedented possibilities for global connectivity and advanced data analytics, as well as extensive use cases across various sectors.[7] Compared to 4G, which primarily relies on more centralised, core-focused architectures, and 5G, which has introduced features such as network slicing and multi-access edge computing (MEC) to distribute processing more efficiently, 6G goes even further. It is expected to move a substantial proportion of computation and data handling to the network edge, thereby enabling vast numbers of endpoints such as wearables, sensors, autonomous robots and holographic interfaces. In parallel, 6G's ultra-high bandwidth and sub-millisecond latencies may offer real-time control and monitoring capabilities that surpass 5G, fuelling exponential growth in the "Internet of Things" (IoT).[8]

[4] GSMA (2018). "SS7 Vulnerabilities and Attack Exposure Report". [Online] https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2018/07/SS7_Vulnerability_2017_A4.ENG_.0003.03.pdf

[5] GSMA (2018). "Diameter Vulnerabilities and Exposure Report". [Online] https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2018/09/Diameter-2018-eng.pdf

[6] D. Antoniuk (2024). "Russian hackers infiltrated Ukrainian telecom giant months before cyberattack". [Online] https://therecord.media/russians-infiltrated-kyivstar-months-before

[7] Ericsson (2023). "Ericsson 6G Security White Paper". [Online]. https://www.ericsson.com/en/6g/6g-security; Nokia (2023), "*Nokia Bell Labs 6G Vision.*" [Online]. https://www.nokia.com/networks/research/6g/

[8] Ericsson (2023). "Ericsson 6G Security White Paper". [Online]. https://www.ericsson.com/en/6g/6g-security; Nokia (2023), "*Nokia Bell Labs 6G Vision.*" [Online]. https://www.nokia.com/networks/research/6g/

Expanded attack surface

These advances expand the range of possible applications but also broaden the attack surface. Whereas 5G supports tens of billions of IoT devices, 6G's ultra-high bandwidth and sub-millisecond latencies could facilitate hundreds of billions or even trillions of endpoints. This leap would enable use cases that demand more throughput and real-time control, but also amplify security challenges. Each additional device could serve as an attack vector or entry point. Adversaries could thereby exploit seemingly benign IoT devices to infiltrate networks or harvest private data, and the deeper convergence of digital, physical and biological domains – for instance, via brain-computer interfaces or biomedical sensors – introduces novel attack vectors.[36] A compromised virtual system might allow perpetrators to commandeer physical operations or sabotage data analytics in mission-critical functions.

Furthermore, 6G applications could be mission- or life-critical, which emphasises the importance of ultra-low latency and robust reliability. Autonomous vehicles, energy grids and robotic surgery systems are environments where even minor security lapses could trigger severe disruption or endanger public safety. The accelerating role of artificial intelligence (AI) further compounds these risks. While AI can rapidly detect anomalies and automate threat responses, it can also be weaponised to create advanced malware, conduct espionage or compromise machine-learning models. Quantum computing adds another dimension. Although still nascent, quantum machines could eventually break classical cryptographic algorithms, which underscores the need for quantum-safe encryption.

Physical Layer Considerations

Beyond these architectural shifts, the 6G physical layer is expected to employ higher-frequency millimetre-wave and terahertz bands to achieve ultra-fast data rates and minimal latency.[9] Although their short propagation distances could curb large-scale interception, they could enable localised eavesdropping and precision jamming by attackers in close physical proximity. The dense infrastructure needed for comprehensive high-frequency coverage – which requires more base stations – adds additional physical points of attack. While directional beamforming improves confidentiality, it depends on secure management of beam control and signalling.[10] If these processes were compromised, attackers would be able to intercept or manipulate high-frequency transmissions.

Privacy, Trust and Edge Data Handling

In 6G, large-scale AI computations and mission-critical logic might reside at or near the network edge, dramatically reducing

[9] Ericsson (2023). "A Primer on 6G Networking". Ericsson White Paper. [Online]. https://www.ericsson.com/en/6g/6g-networking-primer

[10] Nokia (2023). "Integrated Sensing and Communication in 6G". Nokia White Paper. [Online]. https://www.nokia.com/networks/research/6g/integrated-sensing

round-trip times to the core. Although this approach will improve performance and real-time responsiveness, it also distributes resources across many smaller edge nodes, heightening the risk of local compromise.[11] Moving more data processing to the network edge reduces the amount of sensitive information traversing the core, mitigating the fallout if the core is breached. However, it also shifts a larger security burden to the local nodes that handle and aggregate user data. If adversaries were to compromise an edge node, they could intercept data or disrupt critical services without necessarily breaking through the central core. As wearables, immersive interfaces and autonomous systems proliferate, the total volume of user-specific data is likely to escalate, heightening the importance of robust end-to-end encryption, data minimisation and purpose limitation.[12] Zero-trust architectures reduce reliance on historical trust relationships by requiring continuous authentication at both the device and the network levels.[13] Meanwhile, edge-based processing can limit large-scale data aggregation but demands stronger local cryptography, secure key management and rapid patching cycles.

Security-by-Design and Defence Strategies

In the light of these heightened challenges, 6G research and standardisation initiatives must incorporate security principles from the outset. Zero-trust frameworks require ongoing validation of devices and users, discarding the implicit trust assumptions of earlier mobile generations. Post-quantum cryptographic protocols, which protect against emerging quantum threats, are being integrated early into 6G design.[14] AI-driven threat detection enables real-time oversight across distributed architectures,[15] while micro-segmentation and software-defined networking empower 6G infrastructures to contain compromised endpoints.[16]

Supply chain security also looms large. Rigorous product testing, secure manufacturing, cryptographically signed over-the-air updates and verified hardware provenance work to ensure the integrity of critical components. Lightweight blockchains

[11] Ericsson (2023). "Ericsson 6G Security White Paper". [Online]. https://www.ericsson.com/en/6g/6g-security; Nokia (2023), "*Nokia Bell Labs 6G Vision.*" [Online]. https://www.nokia.com/networks/research/6g/

[12] P. Porambage et al (2021). "The Roadmap to 6G Security and Privacy". IEEE Open Journal of the Communications Society. [Online]. https://ieeexplore.ieee.org/document/9426946

[13] Ericsson (2023). "Ericsson 6G Security White Paper". [Online]. https://www.ericsson.com/en/6g/6g-security; Nokia (2023), "*Nokia Bell Labs 6G Vision.*" [Online]. https://www.nokia.com/networks/research/6g/. P. Porambage et al (2021). "The Roadmap to 6G Security and Privacy". IEEE Open Journal of the Communications Society. [Online]. https://ieeexplore.ieee.org/document/9426946

[14] ETSI (2024). Quantum-safe network architecture for next-generation systems (ETSI White Paper No. 45). [Online]. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp45_ETSI_technology_radar.pdf

[15] P. Porambage et al (2021). "The Roadmap to 6G Security and Privacy". IEEE Open Journal of the Communications Society. [Online]. https://ieeexplore.ieee.org/document/9426946

[16] Ericsson (2023). "A Primer on 6G Networking. Ericsson White Paper." [Online]. https://www.ericsson.com/en/6g/6g-networking-primer

or other distributed ledger technologies (DLTs) can secure device credentials and communications using tamper-resistant logs.[17] Combined with robust on-device cryptography and hardware roots of trust, these measures reduce the dangers posed by physical intrusion or rogue IoT devices. Together, they can reinforce network integrity and protect user privacy, thereby bolstering confidence in the future of 6G.

Ultimately, 6G security must contend with the tension between a dramatically expanded IoT environment that potentially means hundreds of billions or trillions of connected devices and fortified defences. If global stakeholders adopt security-by-design methods that incorporate post-quantum encryption, zero-trust models, AI-enabled threat intelligence and robust supply-chain oversight, 6G can deliver the ultra-high bandwidth and low latency demanded by mission-critical scenarios.[18] Achieving these ambitious goals will require steps to ensure that new network capabilities rest on firm governance and rigorous technical safeguards that allow innovation to flourish without endangering safety or privacy. At the policy level, the importance has been recognised of researching and developing 6G with security in mind from the outset, such as in the joint declaration by the US, Sweden, Finland and others.[19]

Emerging 6G Use Case Families and Associated Cybersecurity Threats

The Hexa-X-II project envisages that 6G will be a transformative technology delivering superior connectivity, integrated sensing and advanced intelligence across broad application areas. Six principal use case families have been identified: Immersive Experience, Collaborative Robots, Physical Awareness, Digital Twins, Fully Connected World and Trusted Environment.[20] Although each family enables unique capabilities from hyper-realistic extended reality to real-time robotic collaboration, they also introduce vulnerabilities that raise critical cybersecurity and resilience concerns. It should be emphasised that many of these threats are already relevant to 5G networks, as noted in the EU coordinated risk assessment for 5G.[21]

[17] Nokia (2023), "*Nokia Bell Labs 6G Vision.*" [Online]. https://www.nokia.com/networks/research/6g/. P.Porambage et al (2021). "The Roadmap to 6G Security and Privacy". IEEE Open Journal of the Communications Society. [Online]. https://ieeexplore.ieee.org/document/9426946

[18] Ericsson (2023). "Ericsson 6G Security White Paper". [Online]. https://www.ericsson.com/en/6g/6g-security; Nokia (2023), "*Nokia Bell Labs 6G Vision.*" [Online]. https://www.nokia.com/networks/research/6g/. P.Porambage et al (2021). "The Roadmap to 6G Security and Privacy". IEEE Open Journal of the Communications Society. [Online]. https://ieeexplore.ieee.org/document/9426946

[19] U.S. Embassy & Consulates in Canada (2024). "Joint Statement Endorsing Principles for G6". [Online]. https://ca.usembassy.gov/principles-for-6g/ (Removed from the White House and State Department Websites post-inauguration)

[20] Hexa-X-II (2023). Deliverable D1.2 – 6G Use Cases and Requirements. [Online]. https://hexa-x-ii.eu/wp-content/uploads/2024/01/Hexa-X-II_D1.2.pdf

[21] European Commission (2019). EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks. [Online]. https://digital-strategy.ec.europa.eu/en/news/eu-member-

However, 6G could broaden the scope of impacts by connecting more segments of society at higher speeds.

Immersive Experience

It is anticipated that 6G technologies will be able to support ultra-low latency, high-throughput applications such as extended reality (XR), holographic telepresence and immersive education or healthcare. By merging physical and virtual realms, 6G applications will enable complex simulations and real-time interactions with holographic interfaces.

However, these immersive platforms face risks such as content manipulation, privacy invasion and service disruption. Malicious actors could inject fabricated visuals or audio to confuse or mislead users. They could also exploit vulnerabilities in high-bandwidth data streams and sensor fusion to access biometric or other sensitive user data. Moreover, denial-of-service attacks targeting latency-critical environments could compromise the reliability and continuity of immersive experiences.

Collaborative Robots

By leveraging 6G, swarms of robots or drones will be able to communicate with minimal latency and near-perfect reliability. This will assist factory automation, warehouse management and operations in hazardous environments. Multiple robots will be able to coordinate autonomously using distributed AI models and consistent connectivity.

Attackers might intercept command-and-control links to seize operational control, potentially enabling sabotage or physical harm if they alter robot movements. AI-driven decisions could also be corrupted by feeding in malicious data inputs, resulting in dangerous outcomes. Furthermore, network jamming or overloading could cause collisions or workflow bottlenecks, negating the reliability 6G aims to deliver.

Physical Awareness

Cutting-edge 6G deployments will integrate communication and sensing, allowing the network itself to function as a sensor. By leveraging precise positioning and environment mapping, 6G could offer real-time situational awareness for autonomous vehicles, and public safety and smart infrastructure.

However, these sensing features can be manipulated. Attackers could spoof sensor inputs to conceal an object or distort its location, effectively deceiving applications reliant on accurate detection. Heightened sensing capabilities also raise privacy concerns if advanced location data is misused for unauthorised surveillance. Finally, targeted interference could blind significant portions of a 6G network, enabling stealth intrusions or theft.

Digital Twins

Digital twins are real-time virtual counterparts of physical systems – be they manufacturing lines, logistics networks or

states-publish-report-eu-wide-coordinated-risk-assessment-5g-networks-security

entire cities. They rely on continuous data exchange, large-scale analytics and AI/ML algorithms for tasks such as predictive maintenance and scenario-based planning. The merging of physical and virtual layers through 6G connectivity makes rapid feedback loops and sophisticated simulations achievable.

Cybercriminals could undermine digital twins by altering key metrics or software parameters, producing misleading analytics or interrupting synchronized processes. The wealth of operational data fuelling digital twins makes industrial espionage a significant concern, as attackers could glean insights into proprietary methods or intellectual property. In addition, ransomware attacks targeting real-time data might coerce operators to make payments to avoid crippling both physical assets and virtual models.

Fully Connected World

A core ambition for 6G is to deliver seamless, global connectivity through terrestrial, aerial and space-based networks. Users and devices would enjoy an extremely fast, dependable service anywhere, laying the foundation for essential functions across transport, healthcare and education. Such broad coverage also supports massive machine-type communications in industrial and consumer sectors.

At the same time, a truly worldwide network greatly magnifies the attack surface. Compromising satellites or critical ground stations could cause widespread outages, while adversaries might launch cross-border cyberattacks that are difficult to trace and mitigate. Distributed denial-of-service attacks could ripple across these multi-layered infrastructures, disrupting key services on multiple continents.

Trusted Environment

In the Hexa-X-II vision, robust security, privacy and trust are foundational to the 6G era. It is anticipated that zero-trust models, advanced encryption and distributed ledger technologies (DLTs) will provide seamless authentication for users, devices and data streams. AI-driven anomaly detection and threat intelligence will help networks adapt to evolving attack vectors.

Nonetheless, sophisticated defences spur equally refined attacks. Forged digital identities or compromised cryptographic credentials can grant unauthorized access to sensitive systems, undermining the trust model at the core of 6G. Attackers could also compromise the training data of AI-based defences or use stealthy evasion techniques. Insider threats remain a persistent concern, as even the strongest perimeter can be undone by a malicious actor with legitimate access.

The Impact of 6G on Defence and National Security

Although 6G, like 5G, is primarily designed for civilian environments, it will undoubtedly underpin future military functions. Mobile networks have already proved crucial in the 5G era and are viewed by NATO as a disruptive technology with battlefield implications. Mobile network equipment manufacturers such as Ericsson and Nokia

offer defence-specific 5G solutions.[22] The resilience of Ukraine's mobile communications infrastructure during Russia's 2022 invasion underscores how indispensable commercial mobile networks can be in modern warfare. Despite predictions of swift destruction, Ukrainian operators continued to provide coverage even in contested areas. This resilience has significantly aided both military coordination and civilian communication, demonstrating how mobile infrastructure can help to maintain connectivity under extreme duress.

6G is poised to play a pivotal role in national security, military operations and broader geopolitical affairs. Within NATO, the Science & Technology Organisation (STO) has established exploratory teams to investigate next-generation communication systems, focused on 6G technologies that offer secure, resilient and high-capacity data exchange.[23] Moreover, the 6G Test Centre at the University of Oulu, Finland, has been selected as a test centre of NATO's Defence Innovation Accelerator for the North Atlantic.[24]

The European Union's Hexa-X flagship project similarly explores 6G solutions, addressing not just civilian but also potential defence applications such as integrated sensing and AI-driven network management.[25] Concurrently, the European Defence Fund (EDF) is backing research that could adopt 6G in battlefield communications.

In the United States, the Department of Defense has identified future generations of mobile commercial networks ("FutureG") as one of 14 critical technologies, and has launched several initiatives to coordinate efforts across diverse service branches to evaluate and deploy advanced wireless technologies, including early 6G prototypes. Pilot programmes at military installations integrate edge computing and AI analytics into 5G/6G testbeds to provide real-time awareness, spectrum sharing and interference mitigation. Meanwhile, the Defense Advanced Research Projects Agency (DARPA) is investigating high-frequency spectrum exploitation, which is central to prospective 6G architectures.[26] Collectively, these transatlantic and domestic initiatives

[22] NATO Allied Command Transformation (2024). "5G Technology: Nokia meets with NATO Allied Command Transformation to Discuss Military Applications". [Online] https://www.act.nato.int/article/nokia-meets-act/; Ericsson (2024). "Ericsson 5G for Defense". [Online] https://www.ericsson.com/en/industries/defense

[23] NATO Science & Technology Organization (2023). [Online]. https://www.sto.nato.int/Pages/activitieslisting.aspx

[24] University of Oulu, 6G Flaghship (2024). "Empowering the Future of Connectivitiy and Innovation" [Online] https://www.6gflagship.com/6gtc/

[25] Hexa-X (2024). OBjectives.https://hexa-x.eu/objectives/

[26] U.S. Department of Defense (2022). "Three New Projects for DoD's Innovate Beyond 5G program". https://www.defense.gov/News/Releases/Release/Article/3114220/three-new-projects-for-dods-innovate-beyond-5g-program/; U.S. Department of Defense (2022). "DoD Establishes 5G and Future Generation Wireless Cross-Funcational Team ". https://www.defense.gov/News/Releases/Release/Article/2960806/dod-establishes-5g-and-future-generation-wireless-cross-functional-team/

provide a foundation for future 6G cooperation on cybersecurity, spectrum governance and standardisation.

A key area in which 6G will potentially be impactful for defence purposes is Integrated Sensing and Communication (ISAC).[27] Modern warfare is increasingly reliant on rapid information transfer, where minimising the gap between observation and action provides a decisive advantage. Consequently, there is a growing need to exchange real-time data on the battlefield, seamlessly linking systems and units across multiple domains (land, sea, air, space and cyber).[28] In addition to higher data speeds, 6G networks will potentially converge communication and sensing, allowing mobile nodes to operate simultaneously as radars and high-fidelity sensors.[29] In high-intensity conflicts, swarms of small, interconnected devices could furnish real-time intelligence to enhance situational awareness, rapidly identify threats and streamline strategic decision making. Detection of drones, as well as traffic management of large numbers of drones are other examples where ISAC could play a critical role.[30]

As 6G reduces latency and moves AI processing closer to the network edge, more advanced autonomous systems will likely emerge, such as aerial drones and ground robots capable of immediate analytics, target recognition and coordinated manoeuvres. This collaborative autonomy underpins swarming tactics, where numerous unmanned vehicles share intelligence and adapt strategies in real time. Precision targeting also stands to benefit from combining diverse data sources – optical imaging, infrared signatures and radar telemetry – and delivery of accurate intelligence to facilitate coordinated strikes.

Tactical "bubbles", or rapidly deployable private networks for military and disaster-relief scenarios, could similarly leverage 6G's high performance.[31] One direction from which the above-mentioned FutureG-project in the United States is approaching 6G, is with the objective of replacing large numbers of often wired network equipment deployed by US forces with 6G base stations and associated equipment.[32] However, the associated cybersecurity threats remain substantial. In a future 6G battlefield, every node equipped with sensing or

[27] IQT (2025) IQT Explains: Whats to Come with 6G innovation. https://www.youtube.com/watch?v=d2B52iLz8Rc

[28] M. Juntti and J. Pirskanen (2023). "Military Communications in the 6G Era: Finnish Perspective", in 2023 6G Wireless Summit (6GWS), Levi, Finland, Mar. 2023.

[29] Ericsson (2023). "Communications, Sensing, and Services in 6G. Ericsson White Paper." [Online]. https://www.ericsson.com/en/6g/communications-sensing

[30] IQT (2025) IQT Explains: What's to Come with 6G innovation. https://www.youtube.com/watch?v=d2B52iLz8Rc

[31] M. Juntti and J. Pirskanen (2023). "Military Communications in the 6G Era: Finnish Perspective", in 2023 6G Wireless Summit (6GWS), Levi, Finland, Mar. 2023. https://oulurepo.oulu.fi/bitstream/handle/10024/53228/nbnfioulu-202412117206.pdf?sequence=1&isAllowed=y

[32] IQT (2025) IQT Explains: What's to Come with 6G innovation. https://www.youtube.com/watch?v=d2B52iLz8Rc

communication capabilities becomes a potential vulnerability.[33] Jamming, spoofing and cyber intrusions could disrupt or disable vital services. Consequently, layered security involving physical safeguards, robust encryption and AI-driven threat detection will be essential, alongside the capacity to adapt dynamically to evolving adversarial tactics.

Needless to say, the United States can rely on resources vastly greater than its European partners and allies when it comes to researching and developing 6G capabilities for defence. On the geopolitical stage, 6G is already a focal point of strategic competition, particularly between the United States and China.[34] The Chinese mobile equipment manufacturer Huawei's products are banned in the US but remain operational elsewhere. From a military perspective, the United States is seeking to understand how to use 6G for worldwide secure communications despite the use of hardware controlled by China.[35] Two of Huawei's competitors, Nokia and Ericsson, are European, and the EU Agency for Cybersecurity (ENISA) emphasises the importance of protecting telecom infrastructure. ENISA has also highlighted the importance of 5G to the EU's technological sovereignty. Whether Europe can leverage this position into 6G defence and resilience policies in the face of Sino-US rivalry, however, remains to be seen. Finland's approach to 6G deployment is perhaps illustrative for Europe's defence community.[36] By fostering partnerships across government agencies, academic institutions, private sector industry and defence stakeholders, Finland has accelerated the adoption of leading-edge network technologies in military contexts. Broader EU collaborations through the EDF, Horizon Europe and unified spectrum policies could further harmonise standards, reinforce cybersecurity and lay the groundwork for a more cohesive transition to 6G platforms.

[33] J. Suomalainen et al (2025). "Cybersecurity for tactical 6G networks: threats, architecture, and Intelligence". Future Generation Computer Systems 162. https://acris.aalto.fi/ws/portalfiles/portal/156572648/1-s2.0-S0167739X24004643-main.pdf

[34] Institute for International and Strategic Studies (2022). "Strategic Settings for 6G: Pathways for China and the US. https://www.iiss.org/sv/research-paper/2022/08/strategic-settings-for-6g-pathways-for-china-and-the-us/

[35] IQT (2025) IQT Explains: Whats to Come with 6G innovation. https://www.youtube.com/watch?v=d2B52iLz8Rc

[36] M. Juntti and J. Pirskanen (2023). "Military Communications in the 6G Era: Finnish Perspective", in 2023 6G Wireless Summit (6GWS), Levi, Finland, Mar. 2023.

Conclusions and Recommendations

To work proactively to mitigate the potential cybersecurity risks associated with 6G, industry, policymakers and suppliers should:

- Embed zero-trust principles throughout 6G network architectures, ensuring continuous authentication of devices and users at every stage—from protocol design to hardware manufacturing;
- Introduce post-quantum cryptography early on to protect data against future quantum decryption threats, especially where adversaries might store encrypted traffic for later exploitation;
- Uphold supply chain integrity through meticulous audits of hardware and software vendors, cryptographically signed updates and transparent manufacturing processes;
- Develop AI-driven security tools to detect anomalies, automate responses and operate effectively at both core and edge nodes, while safeguarding these systems against adversarial manipulation and data poisoning.

For Europe to leverage its position as the home of two major telecom manufacturers, and for strategic and defence autonomy, EU and European NATO member states should:

- Strengthen secure 6G research and development within EU frameworks;
- Foster targeted partnerships among public agencies, research institutions and telecom manufacturers to advance zero-trust battlefield communications, quantum-safe cryptography and AI-based threat intelligence;
- Conduct thorough supply chain audits, enforce stringent procurement policies and align with NATO protocols;
- Expand and leverage testbed activities, validate multi-vendor interoperability, refine security standards and speed technology transfers for defence, under a unified European approach that integrates strong governance, rigorous safeguards and collaborative innovation.

brief

About UI

Established in 1938, the Swedish Institute of International Affairs (UI) is an independent research institute on foreign affairs and international relations. Any views expressed in this publication are those of the author. They should not be interpreted as reflecting the views of the Swedish Institute of International Affairs. All manuscripts are reviewed by at least two other experts in the field.

The Swedish Institute of International Affairs
Visiting Address: Amarilitetsbacken 1, 111 49 Stockholm
Postal Address: Box 3163, 103 63 Stockholm
Phone: +46 8 511 768 00
www.ui.se info@ui.se X: @UISweden