Australia's National
Science Agency

Security and privacy in 6G mobile

An exploration of threats and mitigations

H. Suzuki, W. Ni, T. Rakotoarivelo, C. Tapa, S. Camtepe, S. Abuadbba, M. Ding, D. Liu, S. Chau, S. Nepal and G. Walker

30 October 2025

CSIRO Data61

Citation

H. Suzuki, W. Ni, T. Rakotoarivelo, C. Tapa, S. Camtepe, S. Abuadbba, M. Ding, D. Liu, S. Chau, S. Nepal and G. Walker (2025) Security and privacy in 6G mobile. CSIRO, Australia.

Copyright

Important disclaimer

Acknowledgments

This report is an output of a project led by the CSIRO through funding from the Australian Government Department of Home Affairs.

This report does not reflect any Australian Government policy position.

CSIRO would like to thank the Department for its contributions and advice, and the telecommunications industry and universities for participating in workshops. We would also like to thank Monash and Swinburne Universities for their parallel activities in this research area.

Contents

Executive summary

The emergence of sixth generation (6G) mobile networks brings new capabilities in connectivity, sensing, and automation, alongside a more complex security and privacy landscape. This report, developed by CSIRO, outlines key risks and research-led approaches to help industry navigate the transition to 6G securely and responsibly. CSIRO's work is structured around four themes: consumer privacy and security, safe and secure protocols, safe and secure infrastructure software, and secure spectrum management. CSIRO also built a radio frequency test and collaboration platform.

Industry considerations

The transition to 6G presents both opportunities and challenges. By embedding security and privacy into the design and deployment of future networks, and by fostering collaboration across government, academia, and industry, Australia can help shape a resilient and secure digital future. CSIRO's research offers tools, insights, and platforms to support this journey. CSIRO has identified ten areas for industry to consider including exploration, investment, or collaboration.

Consumer privacy and security

1. **Monitoring Integrated Sensing and Communication (ISAC) risk (sensitivity and likelihood) and supporting positive use cases:** As 6G may enable highly accurate location and biometric sensing, privacy risks may increase. Industry could consider monitoring Integrated Sensing and Communication (ISAC) risks, exploring mitigation strategies, and supporting positive applications such as environmental monitoring and urban planning.

Safe and secure protocols

2. **Considering weaknesses in Access and Mobility Function (AMF) and User Plane Function (UPF):** Fuzz testing has proven effective in identifying potential vulnerabilities in 5G protocols (AMF – Next Generation Application Protocol (NGAP) inputs, and UPF – Packet Forwarding Control Protocol (PFCP) messages).
3. **Expanding the use of fuzz testing:** Industry stakeholders may wish to explore fuzz testing in vendor evaluations and development of workflows to strengthen protocol resilience and implementation quality.
4. **Preparing for Post-Quantum Cryptography (PQC):** PQC potentially faces compatibility challenges in legacy systems. Operators might assess capacities of devices and systems to handle bigger PQC keys and ciphertexts, and explore secure digital ID protocols like identity-based Non-Interactive Key Exchange (iNIKE) for latency critical applications and reduced identity-related risks.

Safe and secure infrastructure software

5. **Exploring dynamic threat mitigation frameworks:** Analysis of multiple threat taxonomies and virtualisation risks suggests value in dynamic, AI-enabled threat mitigation systems. Industry may benefit from evaluating their exposure to these risks and considering adaptive security strategies.
6. **Enhancing software supply chain transparency, safety and verifiability:** As reliance on third-party code grows, so do risks of contaminated supply chains. Industry could explore ways to improve transparency, verification, and safety in their software ecosystems, potentially through new vulnerability detection tools.
7. **Leveraging automated standards compliance tools:** Tools using Large Language Models (LLMs) and reverse engineering can compare implementations against standards, assisting with certification and ongoing compliance. Industry might consider integrating such tools into their development and audit processes.
8. **Applying quantified risk frameworks:** Industry could explore the use of objective risk assessment tools for software supply chains and standards compliance to support the prioritisation of threats and alignment of security efforts across diverse infrastructure.

Secure spectrum management

9. **Assessing AI-powered spectrum threats:** Novel jamming, spoofing (sending unauthorised signals) and evasion attacks may degrade spectrum availability. Industry may wish to evaluate their ability to detect such threats and understand their potential impact on service delivery and resilience.

Test platform

10. **Utilising a collaborative science infrastructure:** To enable collaboration and validation of security and privacy science, appropriate infrastructure is required, mimicking real world environments.

1 Introduction

The evolution of mobile communication networks has been marked by significant technological advancements, with each generation introducing new capabilities and presenting new challenges. This report is a high-level overview of the CSIRO 6G Security Research and Development program and the implications of research projects for the Australian industry (telecommunication network operators and vendors and other engaged parties). It draws from detailed work and report produced by CSIRO. The report has four recurring themes:

1. **Consumer privacy and security**: Consumers face challenges in the choice and use of user equipment (UE). This theme explores the risk of devices and seeks to understand the risks exposed in use through Integrated Sensing and Communication (ISAC) techniques.
2. **Safe and secure protocols:** Telecommunications users rely on the safety and security of the telecommunications protocols and services. This theme assesses the suitability of protocols through formal proofs, dynamic testing, and examination of the safety of quantum computing within the infrastructure.
3. **Safe and secure infrastructure software**: Telecommunication infrastructure is increasingly dependent on software supply chains, both inside and outside the sector. These examines the role of standards and compliance for that software and unpacks the risks associated with software-defined infrastructure, combined with the increased prevalence of AI.
4. **Secure spectrum management:** Radio spectrum is a critical enabler for the reliable and secure operation of telecommunications networks. Effective spectrum management ensures that operators can deliver uninterrupted services, maintain high performance, and protect against malicious activities that could degrade network capacity or availability. This theme investigates potential threats—such as interference, jamming, and unauthorised use—that could undermine spectrum integrity and, in turn, jeopardise the network's ability to operate successfully and securely.

Section 2 of this report touches on the research context: internationally and in Australia. Section 3 then explores the security and privacy threats identified by CSIRO in each of the themes. Section 4 elaborates on CSIRO's work to counter or better understand those threats. It includes a test platform built to evaluate Radio Frequency (RF) based threats in a spectrum-safe way and the readiness of open-source telecommunication infrastructure. Section 5 contains specific suggested actions for the industry from the research outcomes and future research, which could heighten the industry's response. Finally, Section 6 provides concluding remarks for the report.

2 Research context

The upcoming International Mobile Telecommunications 2030 standard (IMT-2030) will define the sixth generation (6G) standards, aiming to address the increasing demand for higher data rates, lower latency, and enhanced connectivity, together with improvements in security and privacy. Mobile standards are a combination of agreements between governments under International Telecommunication Union (ITU)cand industry participants who implement these standards under industry bodies such as 3GPP. CSIRO is supporting Australia's contributions to these deliberations. Research is driven by the needs of 6G stakeholders and is an international effort.

6G applications span Unmanned Aerial Vehicle (UAV) mobility, holographic telepresence, autonomous driving, smart grids, industry 5.0, digital twins, intelligent healthcare, and extended reality. Research and development brings new features and applications, simultaneously exposing new threats. Security is an important focus, with research targeting specialised 6G networks, edge intelligence, blockchain, AI security, data privacy, and quantum protection. This section will explore key international research and development impacting the 6G landscape, R&D led by Australian academia, as well as engagement from industry on technology development.

2.1 International context

Major 6G initiatives are underway across North America, Europe, Asia, and the United Kingdom, with governments setting strategic research direction, and industry leading the technological development. Companies like Nokia [1] are advancing AI-driven air interface design, integrated sensing, and new spectrum access through projects like Hexa-X and 6G-ANNA [2]. Ericsson [3] is investing in secure, deterministic networks for industrial automation and leads technical efforts in Hexa-X-II. Samsung [4] is targeting ultra-high data rates, terahertz communications, and intelligent networking through its global research centres and ITU-R leadership. Qualcomm [5] is developing edge-native architectures, Giga-Multiple-Input and Multiple-Output (MIMO), and post-quantum security, while NTT DOCOMO [6] is pioneering sub-THz wireless and distributed MIMO for dense Internet of Things (IoT) environments. InterDigital [7] is focusing on convergence technologies for immersive applications like Extended Reality (XR) and digital twins, supported by multiple Horizon Europe projects.

Governments across the globe are investing heavily in 6G research and development, with coordinated national programs and international collaborations. The European Union is funding projects like Hexa-X (I and II) [8] to explore reconfigurable intelligent surfaces, AI-native networks, and integrated sensing. Germany committed to initiatives like 6G NeXt [9], focusing on XR technologies and advanced modulation schemes. In the United States, the Department of Defence's IB5G program [10], the National Science Foundation's (NSF) VINES [11] partnership and the National Institute of Standards and Technology (NIST) [12] are working with academia and industry (Next G Alliance [13]) to advance Open Radio Access Network (O-RAN), zero-trust architectures, and integrated sensing and communication (ISAC). Japan's Beyond 5G Promotion Consortium [14] is developing sub-THz wireless systems and distributed MIMO.

South Korea [15] is investing in 6G research and development, targeting AI and satellite-based communications. The UK [16] has pledged to undertake next-generation telecom research, partnering with Nokia, Ericsson, and Samsung. China [17] leads in scale, with over US$30 billion invested in future telecommunications, including 6G research monitored by the Ministry of Industry and Information Technology. These efforts reflect a globally coordinated push to shape the future of secure, intelligent, and high-performance connectivity by the 2030s.

2.2 Australian academia

CSIRO's 6G research is the main focus of sections 3 and 4. In addition to CSIRO, Monash University, Swinburne University of Technology, University of New South Wales, University of Technology Sydney and the University of Sydney all have active research programs in telecommunications. Alongside the work covered in this report, CSIRO collaborated with Monash [18] to explore secure network slicing, protected federated learning for spectrum sharing, integrity of O-RAN systems and detecting attacks. In collaboration with Swinburne[19], complex, stateful fuzz testing has also been explored.

2.3 Australian industry

The transition to 5G from 4G, with its software defined network, was a significant and challenging shift in the Australian telecommunications landscape. It redefined architecture and internal operating models. Telecommunication companies are eager to engage with the emerging trends for 6G to ensure the transition from 5G to 6G is smoother.

All major Australian telecommunication operators in Australia, their infrastructure vendors, and sector consultants participated in workshops run by the program. At the workshops CSIRO presented its ongoing findings across the four themes and enabled discussion between academia, and these workshop participants. There was a consensus that industry, academia and consultants collaborating on security and privacy will deliver better outcomes across the economy.

3 6G security and privacy risks

This section will explore some of the security and privacy risks and threats associated with new 6G capabilities. The risks are broken down into the four themes: *Consumer privacy and securit*y, *Safe and secure protocols*, *Safe and secure infrastructure software* and *Secure spectrum management*.

3.1 Consumer privacy and security

6G will bring increased connectivity of low-powered devices, personal devices, and autonomous devices. These devices will know more about their surroundings, the work they are doing and the things or people they are monitoring. Each device brings the risk that it may be compromised, and low-cost devices may not have upgrade pathways to counter adversaries as they discover vulnerabilities.

Even normal usage of a secure device poses risks in ISAC. 6G networks will enable significantly more accurate position measurement (at the centimetre scale) by the telecommunication operator or nearby devices, even if they are not in use on the network. The network will sense changes in the radio waves due to movement or changes in the local environment. It may be possible to deduce what a person is doing, saying, what mode of transport they are travelling on, or what their habits are, without decrypting the telecommunication messages themselves. Such accurate sensing could also reveal biometrics, such as a person's gait or their rest frequency.

3.2 Safe and secure protocols

Delivery of 6G applications will require complex ecosystems of organisations and equipment, requiring cooperation between different network providers, application service providers and end-user devices. The protocols and interfaces required to support such integration will introduce additional complexity to the system and could potentially create vulnerabilities.

These vulnerabilities need to be tested, identified and rectified before they are exploited. CSIRO identified three key types of vulnerabilities:

- Design flaws: Can lead to privacy leakage.
- Legacy encryption: Newer computing technologies can allow encryption to be deciphered.
- Implementation flaws: Implementations might be not up to standard or contain bugs. This risk is amplified on low power, budget devices, where cut-down implementations and reduced testing might prevail.

3.3 Safe and secure infrastructure software

CSIRO [20] examined threat and attack taxonomies from multiple agencies, including:

- The European Union agency for Cybersecurity's (ENISA) threat categorisation for 5G [21].
- The US Cybersecurity and Infrastructure Security Agency's (CISA) threat vectors for 5G infrastructure [22].
- MITRE ATT&CK framework adversary "Tactics, Techniques and Procedures" [23].
- Open Software Supply Chain Attack Reference (OSC&R) framework for supply chain attacks [24].

CSIRO determined that software attacks will be critical to the security of 6G infrastructure. 6G network infrastructure is expected to use increasing amounts of software-based functionality to provide flexibility and reduce the dependency on specialised hardware. This is applicable to all parts of the network operator's infrastructure – the Radio Access Network (RAN), Core Network (CN), and Multi-access Edge Computing (MEC) resources.

The primary software-based technologies in 5G/6G networks include:

- Software-defined networks (SDN) – the management and control logic of the forwarding plane (which determines what to do with incoming packets) extracted from hardware devices and placed in software-based solutions.
- Network function virtualisation (NFV) – networks comprise virtual network functions such as firewalls, load balancers, and intrusion detection.
- Network slicing – multiple logical and virtual networks over a shared physical network.
- Multi-access edge computing – cloud computing technologies are extended to the network's edge, close to where services are produced or requested.

At the same time, the increased adoption of AI or Machine Learning (ML) creates new threat opportunities and new tools for malicious actors. These subsequent sections outline the risks of softwarisation, increased use of AI/ML, adoption of new standards and adversarial use of AI/ML.

3.3.1 Softwarisation, AI/ML weaknesses, AI/ML adversarial use

Network virtualisation and softwarisation of the radio and core network in 5G/6G systems bring both traditional and new security threats. They can be difficult to detect and mitigate due to the intricate nature of the systems that are designed for scalability, resource optimisation and automated orchestration of network functions and services. A list of high-risk threats can be found in Appendix A.1.

3GPP's Release 18 for 5G [25] touched on opportunities for AI/ML to improve management of Next Generation Radio Access Networks (NG-RAN) in energy saving, load balancing and mobility optimisation. However, AI/ML also introduce vulnerabilities in training and testing and through compromised AI/ML development tools. A list of threats during training and from development tools can be found in Appendix A.2.

Finally, AI/ML empowers adversaries as much as it empowers networks. It can be used to automate the launching of attacks and adapt them to the environment it finds. The potential impacts of such attacks can be found in Appendix A.3.

3.3.2 Implementation of new complex standards

The standards landscape is complex and includes standards from several organisations. These organisations include ITU, 3GPP and GSMA. Different organisations develop standards focussed on distinct aspects of the overall system. These differences are driven by separate stakeholder groups – for example, ITU has official government representatives focusing on the regulatory aspects, whereas 3GPP and GSMA are industry-led focusing on the technical details.

This diversity of direction and potential incomplete interoperability between standards described in text documents can amplify challenges. Five categories of potential issues were identified:

- Limitations of the standard specifications because security requirements were not addressed by proposed protocols.
- Timeliness of standardisation and their agility in response to changing threat landscape.
- Ambiguities or vagueness in the standard specifications that may allow for different interpretations and implementations
- Gaps between standards and implementation, where not all requirements have been implemented in compliance with the specification
- Implementation-level vulnerabilities where the implementation is compliant with the specification but creates vulnerabilities an attacker could exploit

The risks arising from gaps in standards and implementation include leakage of information, unavailability of services and spoofing of information.

3.4 Secure spectrum management

Radio spectrum use sits at the heart of mobile telecommunications. Since 5G, telecommunication operators have been able to optimise their allocated spectrum. 6G may see even more dynamic spectrum use. AI/ML can help spectrum management be more autonomous but, as described in section 3.3.1, its use provides new threat vectors for malicious actors to interfere with that autonomy and new tools to automate attacks.

Of interest are the following attacks that rob a telecommunication operator of useful spectrum:

- Jamming detection can be improved with AI/ML but adversaries can also use AI/ML to deliver mobile attacks, changing in power and timing. Attacks are designed to elusively degrade spectrum rather than remove it entirely.
- Adversaries can use AI/ML to create illicit spoofing messages between each other that are so close to gaussian noise that operators will need to use AI/ML to detect the nefarious messages.
- Sophisticated adversaries could use AI to corrupt AI based channel estimation in RANs. By synthesising a noisy channel estimating ping, they could trick the autonomous estimator to think a channel is too noisy, thereby reducing usable spectrum, degrading beamforming accuracy, lowering throughput, increasing latency, and negatively affecting overall quality of service.

4 CSIRO research and development solutions

CSIRO's program of work sought to solve some of the risks identified and contribute to making future networks secure by design. It also sought to increase the awareness of Australian industry (through workshops) and academia (through collaborative activities). The program has developed test platforms to support ongoing analysis and solution development for ever evolving threats.

4.1 Consumer privacy and security

As telecommunication networks evolve, they increasingly collect precise location and biometric data through high-frequency signals and integrated sensing. While this enables valuable services, it also raises serious privacy concerns. This section explores CSIRO's research into safeguarding personal data, including techniques to anonymise movement patterns, assess the threat of mmWave eavesdropping, and assess risks from widespread device connectivity, potentially triggered by future off-the-shelf 6G system solutions.

4.1.1 Location and biometrics

The telecommunication sector may collect accurate location data as part of its normal operation. This is part of a general field called ISAC. With consent, this data could be anonymised and used to contract value added services. Telecommunication providers may need solutions to safely share such data with enough utility to provide profitable value, while ensuring privacy is not compromised. Service providers could include direct retailers, city planners, or health professionals.

CSIRO [26] explored privacy-preserving mechanisms that balance the trade-off between data utility and user privacy. Two main strategies were investigated: differential privacy, which introduces carefully calibrated noise to data aggregates to obscure individual patterns while maintaining usability, and Markov chain modelling, which synthesizes trajectories to mask real movement paths (see Appendix B). These methods were tested using large datasets of vehicle trajectories (in two separate large cities), demonstrating their potential to protect privacy while supporting location-based services.

Trajectory data is particularly challenging as it is vulnerable to inference attacks, where the multiple trajectories for an individual can allow identification of home or work locations, habits (e.g. gym visits, medical appointments etc), or family members. This set of data can make it easier to re-identify the individual. For example, if a dataset shows a trajectory that starts at a residential area every morning at 7:30 AM and ends at a specific office building, an attacker might cross-reference this with public LinkedIn profiles to identify the person.

The research showed combining differential privacy with Markov modelling can enhance privacy protection, however it still requires careful calibration to avoid re-identification risks. A web-based demonstrator was developed to visualise and explore the impact of different calibration settings. Figure 1 shows the tool with the original and synthetic trajectories.

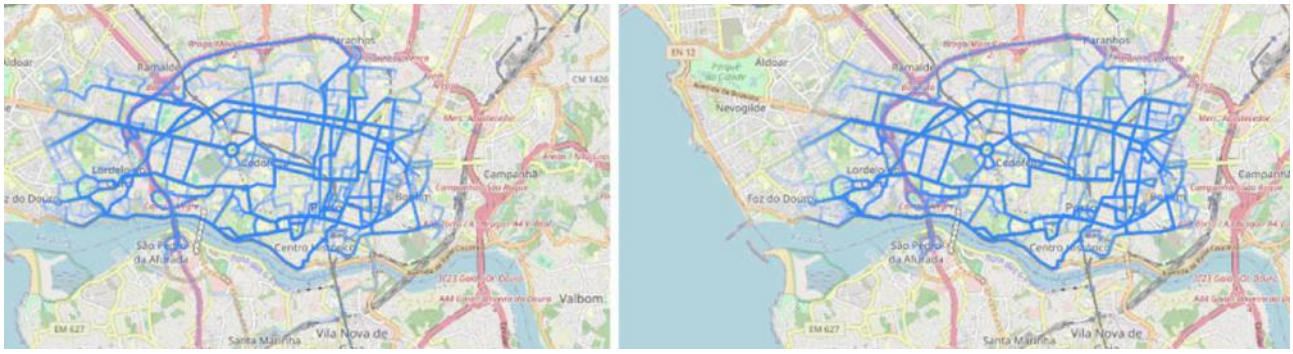

Figure 1 Synthetic trajectories (left) are statistically similar to the original trajectories (right).

4.1.2 Eavesdropping

When we speak on the phone our voice carries to all surfaces around us causing them to vibrate. mmWaves can measure these vibrations. The waves could come from a device used in the conversation or a third-party device measuring what is going on around it. CSIRO [27] used a mmWave radar device to determine if they could recover what was said from surface vibrations. An AI model was trained to translate the vibrations into the same text that was spoken as in Figure 2. The AI tool was able to understand spoken numbers with error rates of 16.8% and identify individual speakers with error rates of 5.9% [28]. Spoken words have proven more difficult for the AI tool to decipher, with error rates from 95% to 60% depending on the model. Even at 60% there is still a significant risk of leakage of sensitive information if participants are having a confidential conversation.

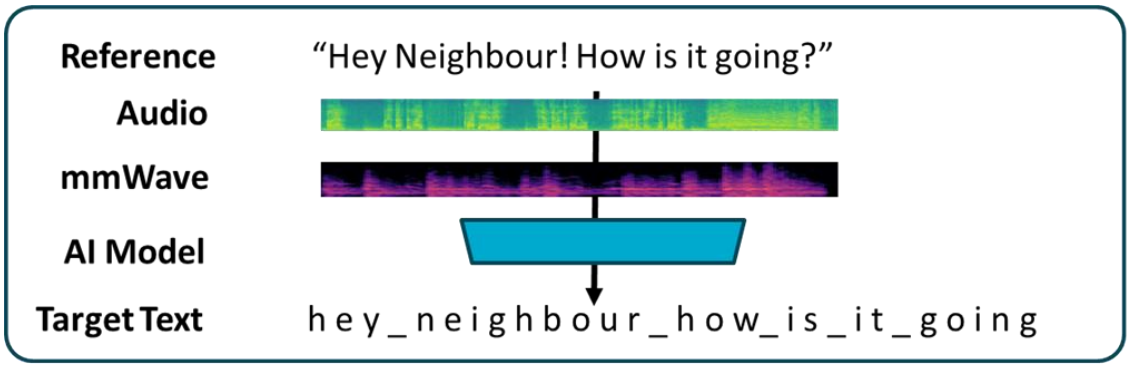

Figure 2 Ideal eavesdropping process

CSIRO used a mmWave radar pointed directly at a speaker producing audio. However, with refinement, it is expected to work on surfaces at a longer range. In the midst of large amounts of telecommunication mmWave traffic, a mmWave eavesdropping radar may be hard to detect. When considering audio security, new threats such as eavesdropping, need to be assessed.

4.1.3 Risk assessment

6G is being designed to enable many devices to interact with a person, business, or a geographically dispersed enterprise such as a farm. There is an increased risk of information leakage from these numerous devices that may not be understood and managed by someone deploying off-the-shelf multi-device solutions.

CSIRO [29] has developed a qualitative risk assessment framework based on Australian Standard AS ISO 31000:2018 Risk management guidelines. This risk framework considers events, consequences, and likelihoods associated with 6G device deployments through a series of templates and worksheets with questions specifically related to technology impact, covering topics of:

- privacy of an individual
- business sensitivity
- device and system integrity.

The CSIRO risk assessment framework provides a systematic basis for the development of future device risk management software when device risk information is available.

4.2 Safe and secure protocols

This section highlights cutting-edge research conducted by CSIRO to address vulnerabilities in protocol design, cryptographic resilience, and protocol implementations. Formal verification of authentication protocols, integration of post-quantum cryptography and fuzz testing, demonstrate Australia's growing capability to secure next-generation networks.

4.2.1 Protocol design – proving design flaws

Telecommunication security and privacy protocols are built around international standards and a consensus-based framework amongst countries and industry participants. These protocols are ideally secure by design, meaning they have security and privacy as intrinsic features. There are formal (mathematical) ways to prove a level of security and privacy. However, if Australia does not invest in the capacity to do this, then it must rely on the assurances of other countries.

CSIRO [26] has taken a step towards developing a sovereign capacity in the formal verification of protocol security by applying the SAPIC+ [30] suite of tools to a new quantum safe transport layer security protocol (KEM-TLS) and 5G authentication protocol (5G-AKA). SAPIC+ is a platform incorporating multiple tools such as Tamarin, Proverif, GSVerif and DeepSec. The application of formal proof with these tools demands specialised expertise. CSIRO was able to successfully apply SAPIC+ to test KEM-TLS and 5G-AKA.

5G-AKA is used to authenticate a user to its home network (HN) via the serving network (SN) so they can utilise mobile communication. The test on 5G-AKA found it met its stated goals but embedded a privacy risk: the user’s identity may be disclosed to the SN when the SN only needs to know that the HN authentication was successful. If Australia can maintain domestic expertise in using these formal tools, it can verify which parts of standards are secure by design.

4.2.2 Post Quantum Cryptography – upgrading legacy encryption

Quantum computing poses a serious threat to public-key cryptographic schemes (e.g., Subscription Concealed Identifier (SUCI), Elliptic Curve Diffie-Hellman (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA), Rivest-Shamie-Adleman (RSA)) currently deployed in 5G networks. Although powerful quantum computers have not been developed, the harvest-now-decrypt-later attack is a concern for long-lived sensitive data.

To address the security threats from quantum computers, NIST [31] has recently standardised several Post Quantum Cryptography (PQC) algorithms. However, due to the distinctive features of new PQC algorithms (e.g., longer ciphertexts and keys), the transition to PQC in 5G networks is not a simple drop-in replacement. CSIRO [32] investigated the PQC transition and the performance impact of PQC algorithms. They found three cryptographic protocols to test on CSIRO's 5G test platform (mini-PT, refer to section 4.5.1):

- **SUCI:** In roaming applications, identity is confirmed with the HN before secure communication on the SN proceeds. OAIBOX [33] did not implement pre-quantum SUCI and the buffers were too short for some of the longer keys in PQC. End to end checking of commercial 5G implementation could be improved by checking buffer requirements.
- **Base station to CN:** IP Security (IPSec) is based on Internet Key Exchange v2 (IKEv2). CSIRO used an open source implementation of IPSec called StrongSwan [34], extended the implementation to include PQC and, with some challenges, incorporated the new module in mini-PT.
- **Communication inside the CN:** CN employs Transport Layer Security (TLS), in most cases, HTTPS. The team used an Open Quant Safe (OQS) Provider [35] library integrated with OpenSSL to upgrade the mini-PT. PQC suffered only a 4% loss of throughput and a negligible increase in latency.

These findings suggest the transition to PQC and 6G will need careful planning and public engagement.

To further reduce latency, CSIRO developed an identity-based Non-Interactive Key Exchange (iNIKE) to secure communication within the 5G CN. With NIKE, a network function can send encrypted messages to another entity without the need to exchange key establishment messages. In CSIRO's implementation of iNIKE for mini-PT, the Network Repository Function (NRF) is used to distribute identity-based secret values for all network functions at the time of their registration. Note that an identity-based secret value for a network function is only distributed once. On mini-PT, the iNIKE reduced latency by a small amount, which requires more work to properly quantify.

In addition to mitigating 5GCN latency, iNIKE offers potential applications across broader 5G/6G use cases. For example, by using phone numbers as identities, iNIKE can authenticate data exchanged between two phones, such as voice or message packets, which may help prevent caller ID spoofing scams.

4.2.3 Fuzz testing – finding implementation flaws

Fuzz testing, or fuzzing, is an automated software testing technique that feeds invalid, unexpected, or random data into a program to uncover coding errors and security vulnerabilities. This approach aims to trigger software faults such as crashes, buffer overflows, memory leaks, or

other erratic behaviours, thereby exposing potential security risks. Fuzz testing is a powerful tool for ensuring software robustness and security by pushing software beyond its conventional operational boundaries and closely monitoring its reactions for signs of malfunction.

CSIRO [36] conducted comprehensive fuzz testing on key 5G core network protocols, including Next Generation Application Protocol (NGAP, N2 interface), GPRS Tunnelling Protocol - User Plane (GTP-U, N3 interface), and Packet Forwarding Control Protocol (PFCP, N4 interface). The objective of this was to assess the robustness, security, and protocol conformance of the OpenAirInterface (OAI)-based 5G system under malformed and adversarial packet injection scenarios.

The fuzzing experiments revealed several high-risk vulnerabilities in the Access and Mobility Management Function (AMF)'s handling of NGAP messages, including system crashes triggered by invalid procedure codes and memory exhaustion caused by repeated NG Setup Requests with modified identifiers. These findings demonstrate critical gaps in input validation and memory management within the AMF entity. In contrast, fuzz testing of the GTP-U protocol showed that the User Plane Function (UPF) demonstrated robust packet validation and rejected corrupted user-plane messages without service disruption. For PFCP, the UPF revealed mixed resilience: while structural validation of some critical fields was correctly enforced, logical inconsistencies, such as accepting duplicate or malformed session rules, indicated insufficient semantic checks, especially in session modification procedures.

CSIRO's fuzzing results point to key areas for improving 5G core network resilience. Operators could consider integrating fuzz testing into vendor evaluations and deploying safeguards around AMF to handle malformed NGAP messages. Vendors are encouraged to strengthen input validation and memory management in AMF and improve PFCP handling in UPF. Incorporating fuzzing into development workflows and supporting coordinated vulnerability disclosure can further enhance ecosystem-wide security.

The team also explored the use of LLMs to generate protocol-aware fuzz testing cases to uncover potential protocol vulnerabilities, laying the groundwork for future intelligent fuzzing practices. A dedicated dataset for fine-tuning an LLM-empowered fuzzer has been constructed, and model selection was incorporated into the fuzz testing methodology.

4.3 Safe and secure infrastructure software

Software based infrastructure is likely to be more prevalent under 6G as it provides greater flexibility and service options. This section highlights CSIRO research into software robustness, virtualisation security, AI-driven vulnerability detection, and automation of standards compliance.

4.3.1 AI/ML based security solutions

AI and ML are being used to improve the security of modern telecommunication infrastructure. These technologies help detect and stop different types of cyberattacks in systems like SDN and NFV. For example, they can spot unusual behaviour or known attack patterns using classical, deep-learning, or reinforcement-learning models. This helps protect against threats like denial-of-service attacks, malware, and eavesdropping. However, there are still challenges, such as not

having enough data to train the systems, the risk of attackers tricking the AI, rapidly evolving 5G/6G software and the difficulty in understanding AI decision making.

CSIRO [37] performed a detailed analysis of AI/ML solutions in attack detection, countermeasures, effectiveness, utilisation, and their integration and limitations. CSIRO then went on to construct and test a specific AI/ML solution, examining code vulnerabilities in 5G C/C++ network infrastructure software, called VulnGuard [38]. This tool takes a suite of downloadable LLMs and fine-tunes them on a database of known vulnerabilities in C/C++. CSIRO then applied these fine-tuned LLMs to open-source network infrastructure code. The ability to download the models and apply them locally allows testing on proprietary code and testing within the development cycle.

Results of the different models are shown in Table 1. All downloadable models showed high precision in discovering real vulnerabilities. However, they generally only found half of the known vulnerabilities in the code [39] [40] [41] [42]. This means they cannot be relied on alone for finding vulnerabilities but are a useful tool for testers to supplement traditional vulnerability identification techniques

The public ChatGPT model was also run as a comparison. ChatGPT found more vulnerabilities, but it also found more issues that were not genuine vulnerabilities. Therefore, using ChatGPT may find more vulnerabilities overall, but would increase time wasted investigating false vulnerabilities. Combining the results from all the local LLMs (Committee of experts – if any thought the code vulnerable, it was vulnerable) improved recall (to 56%) with very little loss of precision.

Table 1 Results for vulnerability discovery

MODEL	ACCURACY	PRECISION	RECALL	F1-SCORE
ChatGPT	53.40%	51.42%	73.46%	60.50%
Committee-of-experts	76.50%	93.22%	56.12%	70.06%
BERT_base	65.00%	93.75%	30.61%	46.96%
DistilBERT_base	65.00%	91.17%	31.63%	47.32%
CodeBERTa_small	64.50%	96.55%	28.57%	44.09%
GPT2_small	65.50%	93.93%	31.63%	47.32%
CodeT5_small	71.00%	93.47%	43.87%	59.72%

4.3.2 Virtualisation side channel defence

New security challenges are emerging because 6G networks will increasingly rely on software-based functions and virtualisation to enhance flexibility and reduce hardware dependency. CSIRO's research explored these vulnerabilities [43], focusing on a scenario known as "network slicing," where users are allocated their own virtual network resources. This setup is ideal for private networks, such as those used by mining companies, which require control without owning physical infrastructure. However, CSIRO demonstrated that a network slice owner could use machine learning on performance data from shared hardware to infer sensitive information about other users. This highlights the potential for privacy breaches even in isolated virtual environments.

Researchers went on to develop a side-channel attack defence system [44], as shown in Figure 3, to reduce the chance of sensitive information being learnt from shared memory and cache resources. A logging module logs activity from O-RAN and core network functions, and a Deep Reinforcement Learning (DRL) module is then trained to identify safe data events containing non-sensitive information. A simulated user agent uses those safe events to inject additional "safe" messages into the network. With enough safe messages in the network, sensitive data is flushed out of the cache. To reduce performance loss, a threshold was set where the central logging agent determines sufficient sensitive information is in the shared cache to render it safe. The current experimental threshold is about 30%. This system was tested on the mini-PT test platform (see Section 4.5.1).

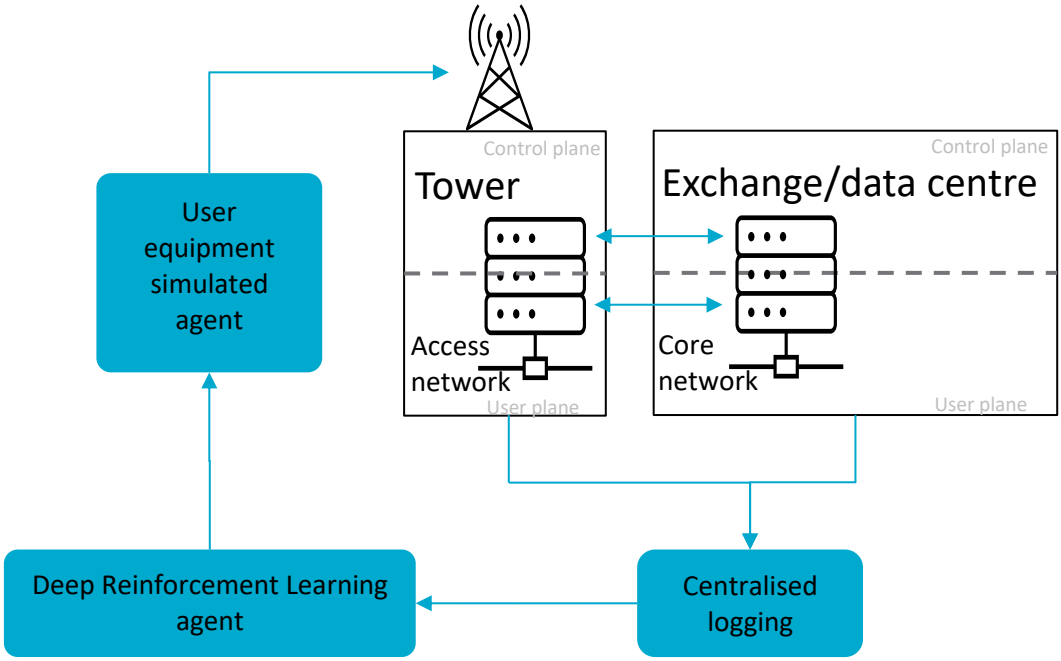

Figure 3 Virtualisation side-channel attack defence system

4.3.3 Standards as a service

Standards form the fundamental building blocks of reliable, interoperable telecommunications infrastructure. However, standards are produced by multiple organisations, often as PDF documents. Standards as a Service (StaaS) makes standards digitally accessible in a machine-readable format. Traditionally this involves formal modelling of standards, then generating the PDF artifact [45]. However recent advances in text processing using LLMs make extracting formal representations from text feasible.

CSIRO [46] used Llama3 LLM to extract message structures and field extents from telecommunication standards documents for compliance checking and risk assessment. LLM analysis of standards informs guidelines for LLM-friendly standards writing.

A compliance checking tool, CompCheck [47], was developed to compare implementations with the newly processed standards. As the source code for implementations is generally not available, information needs to be extracted from executable firmware for comparison to the specifications.

The first step is reverse engineering using general-purpose tools such as IDAPro[1], Binary Ninja[2] and Ghidra[3], followed by using specialised tools designed for analysis of source code for communications protocol message structures. The message structures from standards and implementations are compared in terms of detailed syntax and the semantic logic implementation to understand the gap between standards and implementations.

The tool also looks for cryptographic function signatures in the reverse-engineered code. The functions are identified with two methods: semantic analysis (text from function names or debug messages is matched to cryptography) and pattern recognition (constants and code sequences used in cryptography). The identified functions are then compared against the approved list from NIST [48]. Finally, an LLM was used to synthesise the findings into human-readable reports. This tool will be further tested and could be made available to potential collaborators such as regulatory bodies, certifiers, security professionals, and product developers.

Tools such as CompCheck work best within a systematic framework for security compliance. CSIRO developed a six-layer framework [49] which could help enhance security compliance across the entire organisation. The framework covers:

1. Foundational legislation
2. Specific regulations
3. Mandated frameworks and standards
4. Global best practices
5. Vendor/Operation compliance activities
6. Regulatory bodies.

4.3.4 Risk and supply chain threat assessment

The risks arising from gaps between standards and implementation include leakage of information, unavailability of services and spoofing of information. There are many standards and frameworks for management of these risks, including ISO 31000 [50], 27005 [51] and 31010 [52] standards, NIST frameworks (e.g., NIST RMF [53]) and telecoms-specific guidance in ITU-T X.1055 [54]. The key elements of risk management, regardless of the framework used, include analysis of the threats, development of scenarios specific to the context where the standard is used, and modelling of the threat impact. These are used for risk prioritisation and to determine any required mitigations.

Standards gap detection, as described in the previous section, could be used to identify threats. The impacts of threats could be supported with guidelines but are context dependent. CSIRO [55] has developed a quantitative threat assessment tool that evaluates the likelihood and impact of threats to determine a threat risk.

[1] https://hex-rays.com/ida-pro

[2] https://binary.ninja/

[3] https://github.com/NationalSecurityAgency/ghidra

Figure 4 shows the proposed risk management framework with phase 1 covering gap identification, phase 2 the likelihood and impact analysis and phase 3 the risk-based management plan.

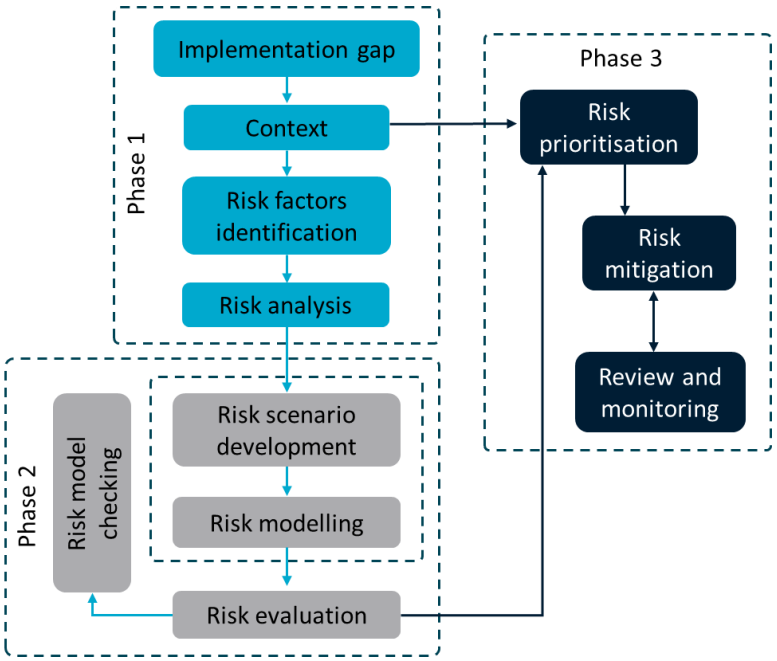

Figure 4 CSIRO Implementation risk frameworks: standards implementation gap

CSIRO has also extended its work on vulnerability analysis in software supply chains to develop a quantitative risk assessment tool for supply chains. The Software Analysis Framework for Evaluating Risk (SAFER) [56] assesses individual software for risk. It quantitatively and dynamically combines developer risk (code dependencies, specifications, and programming language), publisher risk and user-based risk into a final score (Figure 5).

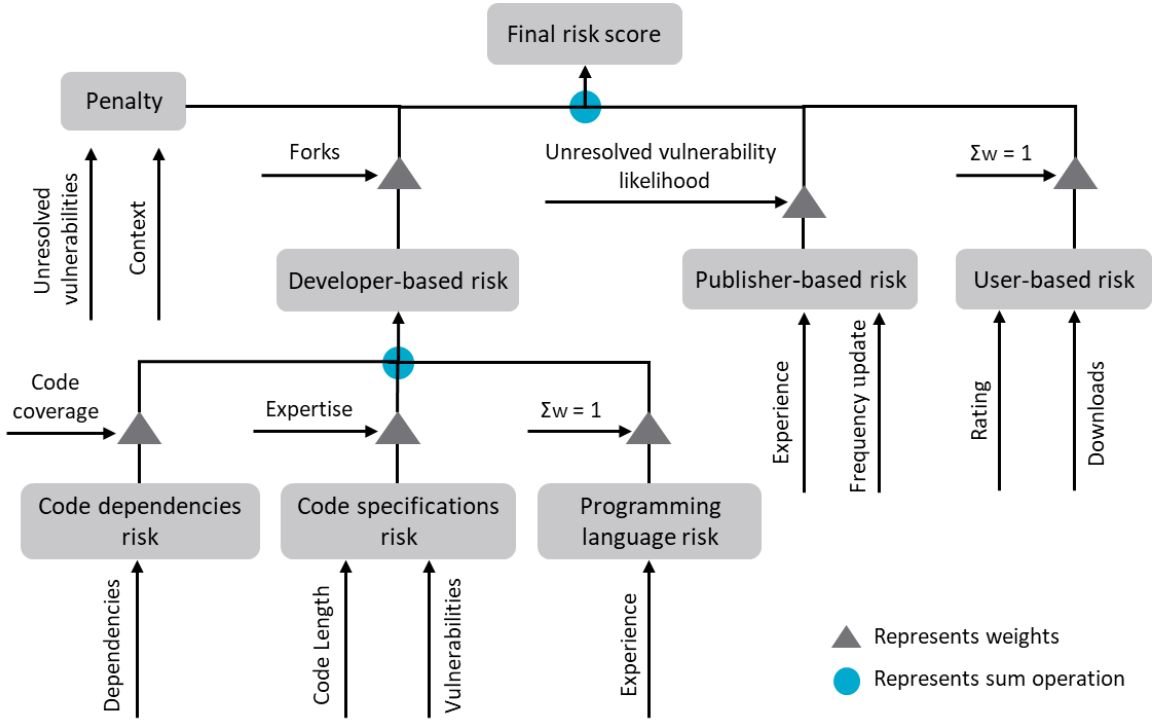

Figure 5 SAFER software supply chains

4.4 Secure spectrum management

Radio spectrum is a precious and limited resource. Attacks that compete for the resource or cause the telecommunication operator to use the resource inefficiently will mean less spectrum is available for productive use. CSIRO has considered jamming, spoofing and corrupted AI channel estimation as potential threats to the spectrum.

4.4.1 Jamming

In 6G's highly interconnected environment, uncrewed aerial vehicles (UAVs) might be configured as mobile platforms for 5G/6G jamming. These mobile devices are harder to detect than stationary jamming devices. The ability to detect, classify, and locate jamming signals becomes essential for preserving network integrity. Real-time detection ensures reliable communication. Classification enables targeted mitigation strategies, and accurate localisation of jammers supports swift countermeasures.

CSIRO [27] evaluated existing techniques for identifying the location of jammers through triangulation of signals from radio towers or friendly mobile access points on UAVs. A constant jamming signal is relatively easy to find in clear conditions. Using a pretrained AI ResNet18 model, accuracy increased with the number of towers available (from 10% error with 3 towers to 1% with five towers), indicating an advantage with rapidly deployable UAV access points. However, accuracy decreased in congested and noisy environments.

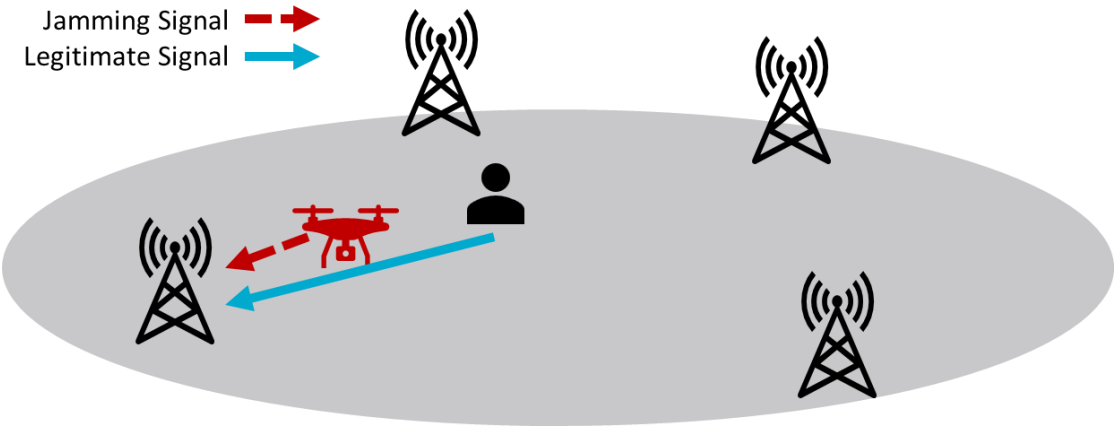

Figure 6 UAV-based jamming

A more sophisticated jamming with AI-enabled smart power hopping (frequently adjusting power levels and hopping patterns) was then tested. Such an attack is well-suited to a UAV with low power consumption and maximum disruption, designed to break up rather than block communication. Bayesian optimisation was employed to determine the most effective modulation patterns for adversaries. Location accuracy fell dramatically and became worse as more towers were fooled by the power hopping.

4.4.2 Spoofing

CSIRO [27] examined a spoofing scenario where adversaries rob network operators of usable spectrum by using it to communicate amongst themselves with a signal mimicking environment noise after standard receiver processing (e.g., low-pass filtering). Not only do they restrict operators' use of spectrum, but they may also use that operator's spectrum for malicious activity. Modern wireless systems use wideband modulations, such as Quadrature Phase-Shift Keying (QPSK), 16-Quadrature Amplitude Modulation (16-QAM), or Orthogonal Frequency-Division Multiplexing (OFDM), to achieve high data rates and efficient spectrum utilisation. CSIRO explored a threat where QPSK is used by adversaries.

A traditional, supervised AI detector was trained on a data set of normal (noise) data to represent current typical detection systems. A QPSK attack dataset was generated under fixed Signal to Noise Ratio (SNR) conditions (0, 1, 3, 30 dB) and may not reflect all real-world effects such as multipath fading or mixed modulation attacks. The detector was unable to distinguish filtered QPSK from environmental noise.

A state-of-the-art AI time-series transformer model was also created and fine-tuned on Gaussian noise. This model was designed to determine if the signal was Gaussian and was able to detect spoofing signals with a 0.96-0.99 F1 score (average of precision and recall) across all SNRs. While the method is computationally efficient and robust to noise, its real-world effectiveness will depend on how it manages channel variability, adaptive thresholds, and potential adversarial countermeasures.

4.4.3 AI threats to channel estimation

6G networks will require complex network management, resource allocation, and scheduling to meet the expected performance requirements in terms of speed, latency and density of devices. This will require rapid real-time analysis of the environmental and contextual characteristics such as phase shift, Doppler effect, path loss and noise. The analysis allows tuning of signal processing to optimise performance. AI is a promising way to solve these problems, with 6G networks expected to have AI embedded in the network management and control functions to enable autonomous network management through automated analysis and decision making.

With the increasing use of AI, new threats emerge. CSIRO [27] explored the potential for adversaries to impact AI channel estimator inputs (signal alignment, power level, phase, and amplitude), and produce incorrect channel estimates that can degrade beamforming, disrupt resource allocation, increase latency, reduce throughput, and compromise overall network reliability. For real-world application, an adversary would need either access to the RAN platform or to inject different radio signals at the time of channel estimation. Researchers used DeepMIMO [57] data to simulate an environment for channel estimation. This data simulates complex real-world environments and is often used to train channel estimation models.

Channel estimation models BiLSTM, LSTM_GRU, CNN, and MLP were tested in this environment. CSIRO found that BiLSTM and LSTM_GRU were resilient to channel estimation attacks, whilst CNN and MLP performed poorly. CSIRO proceeded to build a more sophisticated attack model (AdvPilotNet), which demonstrated strong effectiveness and generalizability across different channel estimation models, with an attack success rate of 80%.

4.5 Test platform

CSIRO has developed a test platform to test open source RAN and CN software with simulated or commercial UE. It is designed for early-stage fault detection and experimentation in emerging technologies, as open-source implementations precede many commercial offerings in the 6G era. A CSIRO trusted platform could facilitate telecommunication operators, vendors, and researchers exploring 6G capabilities such as AI-native networks, reconfigurable surfaces, and quantum-safe communications.

The platform is composed of physical twins (PT) [58] (physical RF components) and digital twins (DT) [59] (simulated RF components). Physical twins operate at smaller scales and in controlled RF environments to limit radio leakage so as not to interfere with licensed spectrum. Digital twins can simulate a large, complex, and speculative RF space such as a future cityscape. They offer scalable, secure environments for interoperability testing, performance benchmarking, and early-stage deployment validation.

4.5.1 Mini-PT

A Mini-PT is a compact, narrowband (40 MHz) 5G testbed enabling basic end-to-end connectivity with a single user equipment (UE). It uses OAI software [60] across three workstations (CN, RAN, UE) and Ettus Research SDRs [61]. Radio signals are transmitted via shielded RF cables to prevent spectrum interference, allowing safe indoor testing (Figure 7). This platform is easy to use for simple testing.

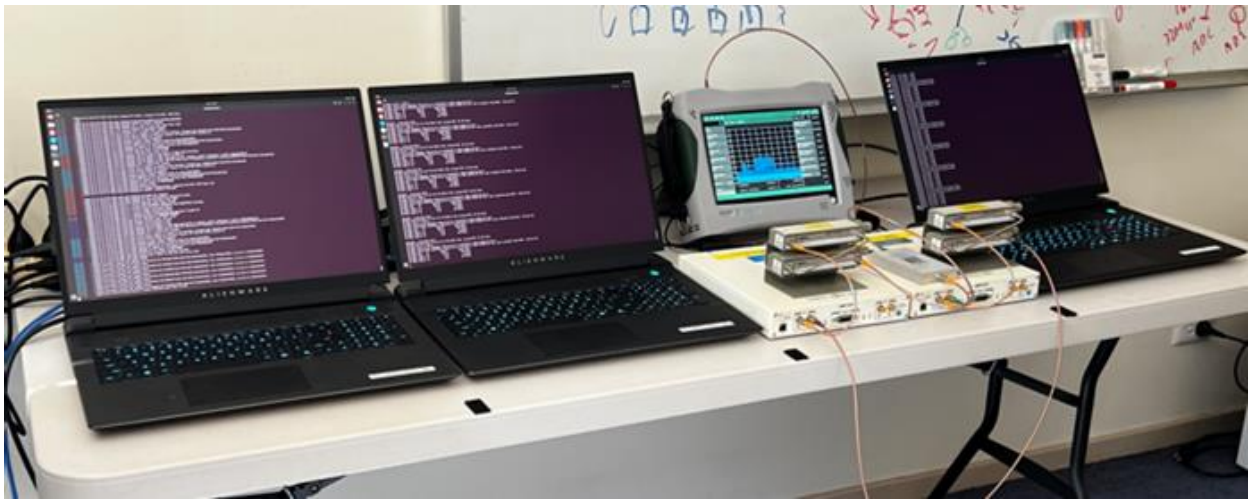

Figure 7 Mini PT equipment

Source: CSIRO

4.5.2 Full-PT

Full-PT was designed to test systems under a multiuser environment. It allows testing of radio networks where users may interfere with each other, or where significant loads change operating conditions. It incorporated a wideband (100 MHz) testbed supporting multi-device scenarios.

Two configurations are in use:

- **NVIDIA ARC-OTA-based Full-PT:** Built on NVIDIA's Aerial RAN CoLab platform [62], featuring GH200 Grace Hopper superchips, Viavi timing gateways, and Benetel O-RUs. This is currently being integrated and tested.
- **OAIBOX-based Full-PT:** A fully operational Open RAN system from Ablesmart [33], including O-RAN Centralised Unit (O-CU), O-RAN Distributed Unit (O-DU), O-RAN Radio Unit (O-RU) (LITEON), and commercial of the shelf UEs. RF shielding cubes and a shielded room mitigate emissions, enabling over-the-air testing without regulatory conflict (Figure 8).

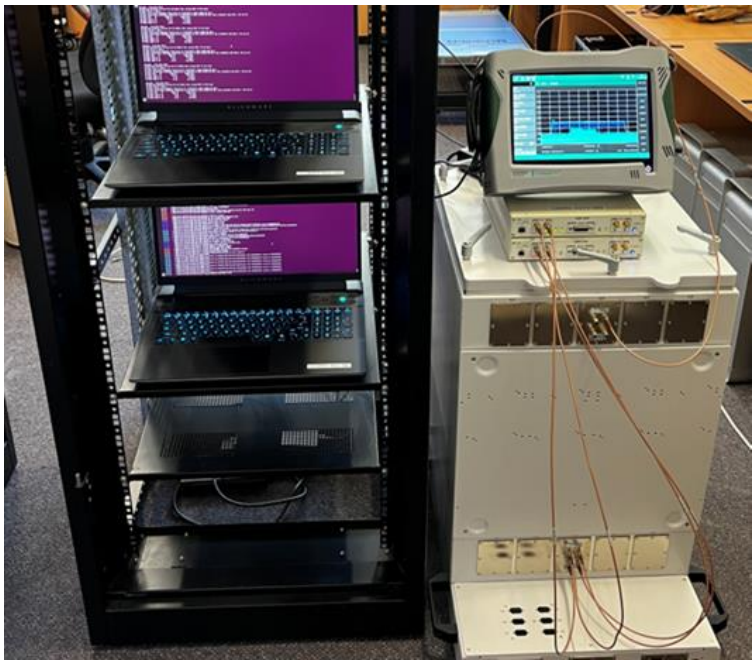

Figure 8 Full-PT equipment with shielded UE box

Source: CSIRO

4.5.3 Digital Twin (DT)

The DT simulates complex radio environments using a cluster-based architecture and diverse software tools:

- **MATLAB:** Antenna Toolbox (ray tracing), 5G Toolbox (3GPP-compliant simulation), and 6G Exploration Library (THz, RIS). [63]
- **NVIDIA Tools:** Aerial Omniverse (GPU-accelerated ray tracing), Sionna (differentiable link/system-level simulation).
- **Open Source Platforms:** Aether (5G core + O-RAN RAN) [64], 5G-LENA (NS-3 simulation) [65], Neo4J (graph-based network topology modelling) [66].

These tools enable "what-if" analyses, waveform testing, and dynamic topology simulations, supporting both academic research and industry prototyping.

5 Industry considerations and future research

CSIRO has extracted a set of key considerations for industry from its research, and to help ensure future telecommunications networks are secure by design. These are described below in each of the four thematic areas. Alongside the considerations are areas of research that CSIRO believes will support industry as they engage with the issues in emerging 6G telecommunications systems.

5.1 Consumer privacy and security

Consideration 1: Monitor ISAC risk (sensitivity of the data and the likelihood of extracting information from it), identify mitigations, support valuable uses.

The most relevant consumer privacy and security challenges are around ISAC, which has the potential to introduce sensitive information leakage for both individuals and businesses. Telecommunication operators should understand the risk, in terms of the data sensitivity and the likelihood of extracting information from it and identify activities to control the risk.

While recent 5G applications have highlighted the value-added capabilities of ISAC, such as flood monitoring [67], (albeit with coarser 5m-wide resolution), given the 5G limitations, further studies are required to develop and evaluate actionable strategies to control risks when substantially finer resolution will be available with 6G technologies. Specifically, adequate balance needs to be achieved between the usefulness of data shared with service providers (e.g. SME providing value-added product from the data), and the sensitivity of the collected ISAC data.

5.2 Safe and secure protocols

Consideration 2: Network infrastructure vendors consider AMF and UPF weaknesses and add fuzz testing to their release processes.

Transitioning to a new standard inherently introduces new risks in design and implementation. CSIRO's fuzz testing of existing 5G protocols found potential weaknesses (section 4.2.3) in NGAP input handling in AMF and in the UPF handling of PFCP messages. CSIRO encourages vendors and operators to identify if their implementations have similar weaknesses.

Consideration 3: Network operators consider diversifying their evaluation of vendor products by including fuzz testing (in-house, certified vendor testing or third-party testing).

If the weaknesses above were found in an established protocol (5G) through fuzz testing, then it is likely that fuzz testing might find new weaknesses in emerging 6G protocols. Therefore, CSIRO encourages network operators to place greater emphasis on fuzz testing as part of vendor evaluation, and to include fuzz testing as part of their pre-release testing regime.

Consideration 4: Network operators check buffer size compatibility with PQC and consider better secure digital ID protocols such as iNIKE.

PQC requirements from NIST will emerge at a similar timeframe to 6G. While 6G implementations may accommodate the longer messages required in PQC, legacy 4G and 5G networks may not. CSIRO encourages network operators to evaluate whether devices on their network, RAN and CN, have sufficient buffer capacity to avoid buffer overflow problems, and their overall risk for transition to PQC, when the existing RSA algorithms become unsupported in 2035. Operators could also consider the utility of CSIRO's new iNIKE protocol for SIM cards to establish secure digital IDs and reduce scams.

5.3 Safe and secure infrastructure software

Consideration 5: Adopt a dynamic threat mitigation system based on known attack taxonomies and evaluate the current risk of these threats.

ENISA, CISA, MITRE, and OSC have developed threat taxonomies and adversarial frameworks. CSIRO has expanded this to identify threats in softwarisation and AI/ML. Together they represent a comprehensive guide to what is vulnerable and how adversaries exploit those vulnerabilities. For a specific, proven side channel virtualisation attack, CSIRO developed a technique to reduce the risk of information loss. Industry could consider how to integrate these taxonomies into a threat management strategy and assess their vulnerability to a virtualisation side channel attack.

Consideration 6: Assess risk of third-party software and what steps could be taken to ensure transparency, safety, and verifiability of the software stack.

As developers reach for third-party code bases to increase functionality, the risk of contaminated software supply chains increases. The ability to check supply chains for vulnerabilities and verify provenance will reduce software risk. CSIRO has taken some steps to reduce that risk by developing VulnGuard, a software vulnerability checking tool. We suggest the industry consider the risks associated with their software dependencies and the steps they could take to mitigate those risks.

Consideration 7: Network vendors and operators' use of automated standards compliance tools as an additional check for in-house and third-party software compliance.

The new standards in 6G will be implemented using new or revised software implementations. CSIRO has developed some automated compliance tools which use LLMs to analyse standards and reverse engineering to compare data structures and cryptographic functions in the implementation against the standards. This automated certification can occur during both formal certification and use, as standards are revised. Industry could consider such tools supporting automated checking, to reduce inconsistencies and provide an accessible secondary qualification to software guarantees.

Consideration 8: Industry adopts a risk framework with quantified risk vectors to assist with threat prioritisation.

CSIRO has developed a novel framework called Software Analysis Framework for Evaluation of Risk (SAFER), which quantifies software security risk, enabling precise and objective assessments of potential security efforts by eliminating inconsistencies in evaluation. They have also developed a quantified risk evaluation tool for standards compliance. Industry could consider such risk evaluation tools to prioritise the management of threats from the wide variety of sources, including those described in threat taxonomies, code vulnerabilities, and incomplete standards compliance.

5.4 Secure spectrum management

Consideration 9: Industry determines if they can detect AI-powered jamming, spoofing, or evasion attacks, and know the impact it is having on customers.

To disrupt telecommunications in Australia, adversaries do not need to take down entire networks; they could simply degrade the spectrum bandwidth everyone relies on. CSIRO demonstrated the ability to use and detect novel jamming techniques, particularly on mobile platforms that can partially and intermittently remove bandwidth. They could be used to interfere in Australian engagement in national activities such as social events or political involvement. Spoofing was shown to be difficult to detect, because it looks like noise. It removes bandwidth and allows parties to organise themselves for malicious acts, at the network operator’s expense. In addition, adversarial evasion attacks were shown to be highly successful, impacting all downstream tasks such as beamforming and resource allocation, while remaining difficult to detect due to their stealthy nature. Network operators could investigate if they are able to detect if jamming, spoofing, or evasion attacks against channel estimators are occurring and how they would know if these were impacting their network operation.

5.5 Test platform

Consideration 10: Collaborative science to identify and mitigate risks requires accessible testing infrastructure.

Activities in fuzz testing, virtualisation mitigations, and analysis of PQC all used the CSIRO test platform. The platform added robustness to the findings. Industry workshops identified value in greater collaboration between individual companies, and between companies and universities in telecommunications security and privacy. Test platforms can represent a safe common ground.

6 Conclusion

6G is an emerging technology expected to revolutionise communication by meeting the growing demand for higher data rates, lower latency, and improved connectivity of modern and emerging applications. It is expected to become a fundamental technology for future communication, serving as a vital foundation for various critical infrastructure sectors, including transportation, healthcare, finance, and energy. It is essential to adopt a proactive security and privacy-by-design approach for 6G before its rollout. The Department of Home Affairs tasked CSIRO with studying the security and privacy implications of 6G by examining its potential applications, including the impact of other critical technologies like AI and Quantum computing on 6G.

CSIRO conducted extensive research, in collaboration with university partners, and in consultation with industry and government stakeholders. This report has summarised the findings of the research, which was aimed at both industry and government audiences. The findings were organised into four key areas: consumer privacy and security, safe and secure protocols, safe and secure infrastructure software, and secure spectrum management.

As 6G is still in its early stages, the security and privacy research in this study is based on past knowledge and some speculative insights about the future. Once the technology is deployed, it is expected to introduce numerous innovative applications that could significantly impact the security and privacy problems associated with 6G. Key points to guide future research includes, but are not limited to:

- In the context of integrated sensing capability of 6G, how do we keep consumer information safe; both what is communicated, and what can simultaneously be learnt from that communication?
- How do we ensure any future policies and regulations safeguard our national interest while fostering innovation?
- Considering the advancement of AI technology, how do we protect our spectrum from adversaries, including during times of heightened threat actor activity and geopolitical conflict?
- How can we establish the necessary research infrastructure to continuously test, validate, and verify the supply chain for 6G-related technologies? This will help ensure the safe rollout of 6G technology for Australians and the Australian industry.

While security and privacy are facilitated by standards and technological implementations, the settings that are used are inherently local. Continued work is needed to understand the implications of security and privacy in mobile communications for Australia, and to support the development of future telecommunications networks that are secure by design.

Appendix A Software and AI/ML threats

A.1 Softwarisation threats

CSIRO conducted a literature review of network softwarisation and cyber vulnerabilities connected with the telecommunications sector [68]. CSIRO then prioritised those threat-based risks (likelihood and impact). The highest risk softwarisation threats have been identified as:

1. Nefarious activity: Harmful actions by attackers who try to break into or disrupt the network. These actions can include tricking the system, altering how data moves through the network, or secretly watching what is happening. Complex software systems make these hard to spot.
2. Vulnerabilities: Softwarisation increases potential vulnerabilities including flaws in virtual machines, containers, Application Programming Interfaces (APIs), and management tools. These can lead to data theft, service disruption, or unauthorised access. They are difficult to detect as they may be unknown.
3. Weak isolation and management of shared resources: When multiple virtual network functions or services share the same physical or virtual infrastructure without strong separation. If isolation is weak, attackers can exploit one part of the system to access or disrupt others—such as moving between network slices or accessing shared memory or processing resources. This can lead to data leaks, service disruptions, or bypassing of traditional security controls.
4. Eavesdropping, interception, hijacking: These attacks involve unauthorised access to, or manipulation of, network communications. Common techniques include traffic diversion, man-in-the-middle attacks, backdoors, and packet sniffing. Attackers may exploit vulnerabilities in east–west communication channels (between internal systems), use scanners to probe for weaknesses, or hijack sessions to gain control.
5. Orchestrator risks: the orchestrator—responsible for coordinating network functions, resources, and services—becomes a target or point of failure. In complex setups like network slicing, orchestrators often handle mixed workloads and inter-container traffic, which can be insecure or poorly isolated. If compromised, an orchestrator can be used to manipulate configurations, leak sensitive data, or disrupt services across multiple domains.
6. Supply-chain attack: These attacks exploit vulnerabilities introduced during the development, integration, or distribution stages of hardware and software. Malicious actors can insert flaws or malware early in the supply chain, which may go undetected until after deployment. This is particularly dangerous in complex, virtualised environments where components are sourced from diverse vendors. The difficulty in tracing and verifying every element in the supply chain makes detection and mitigation challenging
7. Insecure APIs: APIs are essential for provisioning, managing, monitoring, and orchestrating network functions and services. However, if not properly secured, they can become significant attack vectors. Insecure APIs may expose sensitive data, allow unauthorised access or be exploited to manipulate network configurations.

A.2 AI/ML weaknesses

AI/ML models face various vulnerabilities during training and testing, including [37]:

- Poisoning Attacks – Injecting bad data into AI training to make it behave incorrectly.
- Backdoor Attacks – Secretly adding hidden triggers that make AI act in a specific way when activated.
- Evasion Attacks – Tricking AI systems with cleverly crafted inputs to fool their decisions.
- Inference Attacks – Extracting private or sensitive information from AI models.
- Prompt Injection – Feeding misleading instructions to AI (like chatbots) to make them do unintended things.
- Jailbreaking – Bypassing safety controls in AI systems to access restricted or harmful outputs.

Attackers can hide malicious programs within trained and tested AI/ML packages. An AI/ML package is a software package that contains machine learning models, along with their associated code, scripts, or data components, designed to be reused, distributed, or integrated into other systems. AI/ML packages can hide malicious programs or introduce vulnerabilities through several mechanisms. They may contain embedded malicious code or scripts, including trojans that alter model behaviour, or backdoors inserted during training that activate with specific triggers. Vulnerabilities also arise from compromised third-party dependencies, leading to malware injection throughout the software supply chain. Impacts potentially include:

- Network Flooding – Overwhelming the network with fake traffic to slow or stop services.
- Configuration Tampering – Changing network settings to cause errors or open security holes.
- Network Optimisation Disruption – Making the network run less efficiently or misallocating resources.
- Intrusion Facilitation – Helping attackers sneak into the network undetected.
- Information Leakage – Exposing private data such as user info or network structure.
- Malicious Software Deployment – Installing harmful programs that can spy, steal, or damage systems.
- Network Slice Attacks – Targeting specific parts of the network that serve different users or services.
- Exploitation of Large Language Models (LLMs) – Changing the behaviour of AI tools like chatbots to manipulate or attack network systems, by tricking users into revealing sensitive data or providing false information.

A.3 Adversarial AI/ML use

Potential impacts of adversarial use of AI/ML on telecommunication infrastructure components [37]:

- Software-defined networks – AI/ML is used to plan smarter attacks, bypass defences, and automate intrusion.
- Network function virtualisation – Attackers use AI/ML to misuse shared resources, hide inside channels, and poison data.
- Network slices – AI/ML helps attackers break isolation, move across slices, and flood the network with fake traffic.
- Software – AI/ML finds weak spots in software, poisons supply chains, and manipulates decision-making systems.
- Containers – AI/ML enables attackers to scan for entry points, hide malware and escape containers.

Appendix B Location and trajectory privacy-preserving techniques

B.1 Differential privacy

Differential privacy (DP) is a privacy-preserving technique that protects individual data by introducing carefully calibrated noise into datasets. This ensures the presence or absence of any single individual in the dataset cannot be confidently determined, even by an attacker with extensive background knowledge. The strength of this protection is governed by a "privacy budget"—a lower budget offers stronger privacy but may reduce data utility. DP provides mathematically provable guarantees. In the context of trajectory data, DP works by blending individual movement patterns into group trends, making it difficult to isolate specific paths. While it effectively obscures individual data points, it does not inherently protect relationships between data points (e.g., connections between locations), which may require additional mechanisms.

B.2 Markov chains

Markov modelling (MM) is used to generate synthetic trajectories by learning patterns from real movement data and then producing artificial paths that mimic those patterns. This approach captures how trajectories evolve, allowing the model to explain, predict, or simulate new paths. However, while the synthetic outputs do not directly replicate any real trajectory, they can still leak sensitive information if queried extensively, as patterns in the model may reflect real data points. To mitigate this, the project integrates MM with local DP, which applies privacy protections directly at the user level without relying on a trusted central authority. While MM alone lacks formal privacy guarantees, the addition of DP introduces mathematically provable protections—ensuring that the inclusion or exclusion of any individual’s data does not significantly alter the output. This combination enhances privacy but introduces a trade-off: stronger privacy may reduce the accuracy or utility of the synthetic data.

Shortened forms

SHORT FORM	EXPANSION
AI	Artificial Intelligence
API	Application Programming Interface
AISM	AI-enabled Spectrum Management
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
BMBF	Federal Ministry of Education and Research
CISA	Cybersecurity and Infrastructure Security Agency
CN	Core Network
CR	Cognitive Radio
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DES	Digital Economy Strategy
DP	Differential Privacy
DT	Digital Twin
ECDH	Elliptic Curve Diffie-Hellman (key exchange protocol)
ECDSA	Elliptic Curve Digital Signature Algorithm
ENISA	European Union Agency for Cybersecurity
EU	European Union
GPRS	General Packet Radio Service
GPU	Graphics Processing Unit
GTP-U	GPRS Tunnelling Protocol – User Plane
HN	Home Network
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange version 2
IMT	International Mobile Telecommunications
iNIKE	Identify based Non-Interactive Key Exchange
IoT	Internet of Things
ISAC	Integrated Sensing and Communication
ITU	International Telecommunication Union
LITEON	An instance of an Open RAN Radio Unit
LLM	Large Language Model
MEC	Multi-access Edge Computing
MIIT	Ministry of Industry and Information Technology
MIMO	Multiple Input Multiple Output (wireless communication)
ML	Machine Learning

SHORT FORM	EXPANSION
MM	Markov Modelling
NFV	Network Function Virtualisation
NGAP	Next Generation Application Protocol
NIKE	Non-Interactive Key Exchange
NIST	National Institute of Standards and Technology
NRF	Network Repository Function
NS	Network Slicing
O-RAN	Open Radio Access Network
OAI	Open Air Interface
OAIBOX	Ablesmart's implementation of OAI
OFDM	Orthogonal Frequency-Division Multiplexing
OQS	Open Quantum Safe (project for post-quantum cryptography)
PFCP	Packet Forwarding Control Plane
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
PT	Physical Twin. Mini is single UE, full is multiple UE.
QPSK	Quadrature Phase-Shift Keying
RAN	Radio Access Network
RF	Radio Frequency
RIS	Reconfigurable Intelligent Surfaces
RSA	Rivest–Shamir–Adleman (public-key cryptosystem)
RSP	Remote SIM Provisioning
RU	Radio Unit
SAFER	Secure And Fast Encryption Routine
SDN	Software-Defined Networking
SN	Serving Network
SNR	Signal-to-Noise Ratio
SIM	Subscriber Identity Module
SUCI	Subscription Concealed Identifier
SUTD	Singapore University of Technology and Design
SVM	Support Vector Machine
TLS	Transport Layer Security
TTS	Transformer Time Series
UAV	Uncrewed Aerial Vehicle
UE	User Equipment
URLLC	Ultra-Reliable Low Latency Communication
USA	United States of America

Glossary

API (Application Programming Interface): A set of rules that lets different software programs talk to each other and share information.

Artificial Intelligence: A way for computers to do tasks that usually need human thinking, like understanding language or recognising images.

Authentication and Key Agreement: A process in mobile networks to confirm a user's identity and set up secure communication.

Cognitive Radio: A smart radio that can automatically find and use the best available frequencies to avoid interference.

Core Network: The central part of a mobile network that manages data, connections, and services for users.

Denial of Service (DoS) Attack: A cyberattack that floods a system with traffic to make it slow or stop working.

Differential Privacy: A method to protect personal data by adding small changes so individual information cannot be identified.

Digital Twin: A virtual copy of a real-world object or system used to test and monitor it digitally.

Eavesdropping: Secretly listening to private communication, often using technology to intercept signals.

Edge Computing: A way to process data closer to where it is created instead of sending it away to a big data centre.

Encryption: A way to scramble information so only someone with the right key can read it. It keeps data private and secure.

Fuzz Testing: A way to find bugs in software by feeding it random or unexpected inputs.

Latency: The delay between sending a request and getting a response. Lower latency means faster communication.

Machine Learning: A type of AI where computers learn from data and improve over time without being directly programmed.

Man-in-the-Middle Attack: A cyberattack where someone secretly intercepts and possibly changes the communication between two people or systems.

Markov Modelling: A way to predict future events based on the idea that the next step depends only on the current state.

Network Slicing: Dividing a network into separate parts so each can be used for different purposes or services.

Non-Terrestrial Networks: Communication systems that use satellites or drones instead of ground-based towers.

Open Radio Access Network (O-RAN): A new way to build mobile networks using open standards and parts from different companies.

Orchestrator: A system that manages and coordinates different parts of a network to make sure everything works together smoothly.

Post-Quantum Cryptography: New types of encryptions designed to be secure even against future quantum computers.

Public Key Infrastructure (PKI): A system that uses digital keys to secure communication and verify identities online.

Quantum Computing: A new kind of computing that uses quantum physics to solve problems much faster than regular computers.

Radio Access Network: The set of components that translates radio signal from devices into communication with a specific user. It interacts with the core network.

Reinforcement Learning: A type of machine learning where a system learns by trying things and getting rewards or penalties.

Side-Channel Attack: A hacking method that uses indirect clues like power use or timing to steal information.

Subscription Concealed Identifier: A way to hide a mobile user's identity when connecting to a network.

Supply Chain Attack: A cyberattack that targets software or hardware during its development or delivery before it even reaches the user.

Transport Layer Security (TLS): A protocol that keeps internet communication private and secure, such as https.

Virtualisation: Creating virtual versions of physical things like servers or networks to make them more flexible and efficient.

References

1. Nokia, “6G Technologies | Nokia.com,” 2025; Accessed on 13 August 2025; https://www.nokia.com/bell-labs/research/6g-networks/6g-technologies/.

2. Nokia Communications, “Nokia to lead the next phase of Europe’s 6G flagship project,” 7 October 2022; https://www.nokia.com/newsroom/nokia-to-lead-the-next-phase-of-europes-6g-flagship-project/.

3. Ericsson newsroom, “Ericsson in multi-million GBP 6G research program,” 22 November 2022; https://www.ericsson.com/en/press-releases/3/2022/ericsson-in-multi-million-gbp-6g-research-program-investment-in-the-uk.

4. Samsung, “6G: The next hyper - connected experience for all.,” 2020; https://cdn.codeground.org/nsr/downloads/researchareas/20201201_6G_Vision_web.pdf.

5. F. Pica and L. Awoniyi-Oteri, "Path to 6G: Envisioning next-gen use cases for 2030 and beyond," blog, 13 August 2024; https://www.qualcomm.com/news/onq/2024/06/path-to-6g-envisioning-next-gen-use-cases-for-2030-and-beyond.

6. NTT DOCOMO INC, “White paper 5G Evolution and 6G (Version 5.0),” 26 January 2023, Accessed on 13 August 2025; https://www.docomo.ne.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_v5.0.pdf.

7. R. Stephens, “InterDigital Awarded Five Horizon Europe 6G Flagship Projects Targeting Revolutionary Technology Advancement and Experimental Infrastructures,” 7 November 2022; https://ir.interdigital.com/news-events/press-releases/news-details/2022/InterDigital-Awarded-Five-Horizon-Europe-6G-Flagship-Projects-Targeting-Revolutionary-Technology-Advancement-and-Experimental-Infrastructures/default.aspx.

8. Hexa-X-II, “Hexa-X-II - European level 6G Flagship project,” 2025; Accessed on 13 August 2025; https://hexa-x-ii.eu/.

9. 6gnext.de, “6G NeXt,” 2025; Accessed on 13 August 2025; https://6gnext.de/.

10. Department of Defense, “Three New Projects for DOD's Innovate Beyond 5G Program,” 2 August 2022; https://www.defense.gov/News/Releases/Release/Article/3114220/three-new-projects-for-dods-innovate-beyond-5g-program/.

11. National Science Foundation, “Verticals-enabling Intelligent Network Systems (VINES),” 2025, Last updated on 19 May; Accessed on 13 August 2025; https://www.nsf.gov/funding/opportunities/vines-verticals-enabling-intelligent-network-systems/nsf25-539/solicitation.

12. National Institute of Standards and Technology, “Shaping the 6G Era | NIST,” 2025, Last updated on 18 June; Accessed on 9 July 2025; https://www.nist.gov/news-events/news/2025/06/shaping-6g-era.

13. Alliance for Telecommunications Industry Solutions, “Research Priorities: North American Audacious Goals,” 2025; Accessed on 13 August 2025; https://nextgalliance.org/research-priorities/north-american-audacious-goals/.

14. Ministry of Internal Affairs and Communications, “Beyond 5G Promotion Strategy Roundtable: Recommendations,” 02 January 2021, Japan, Accessed on 13 August 2025; https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/Beyond_5G_Promotion_Strategy_Roundtable_Recommendations.pdf.

15. L. Jong-Ho, “MSIT Launches the K-Network 2030 Strategy,” 23 March 2023, South Korea; https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=6&bbsSeqNo=42&nttSeqNo=783&searchOpt=ALL&searchTxt=6g.

16. D.A. Sherman and S. Brawley, “6G mobile technology,” 2 December 2024; https://researchbriefings.files.parliament.uk/documents/POST-PN-0734/POST-PN-0734.pdf.

17. 5G Americas, “Mobile communications towards 2030,” 2021; https://www.5gamericas.org/wp-content/uploads/2021/11/Mob-Comm-Towards-2030-WP.pdf.

18. Monash University, “AI/ML-Driven Spectrum Security and kAdversarial Radio Defence for 6G,” 16 June 2025.

19. Swinburne University of Technology, “Final Report,” 13 June 2025.

20. C. Thapa, R. Holland, S. Ali Siddiqui, H. Suzuki, T. Wijaya and S. Camtepe, *Software Supply-Chain Security*, Milestone 2 in Project 2: Network Softwarisation and Cyber Vulnerabilities, CSIRO, 2024.

21. M. Lourencso, L. Marinos and ENISA, *ENISA threat landscape for 5G networks*, European Union Agency for Cybersecurity (ENISA), 2019; https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20threat%20landscape%20for%205G%20Networks.pdf.

22. Cybersecurity & Infrastructure Security Agency, National Security Agency and Office of the Director of National Intelligence, *Potential threat vectors to 5G infrastructure*, 2021; https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%2520%25281%2529.pdf.

23. C. Clancy, J. Feraro, R. Martin, A. Pennington, C. Sledjeski and C. Wiener, *Deliver uncompromised: Securing critical software supply chains*, 24 in MITRE Technical Papers, 2021.

24. N. Ziv, L. Arzi, P. Eyal, D. Cross, H. Suezawa, N. Penso, S. Sivan, D. Sahni, M. Kovalsky, C. Wang, R. Feintuch, H. Harel Lavie, R. Atias and G. Evron, “Open Software Supply Chain Attack Reference (OSC&R):,” 2024, Last updated on 17 July; Accessed on 30 May 2023; https://pbom.dev/#overview.

25. ETSI Technical Specification Groups, *3GPP TR 21.918 version 18.0.0 Release 18*, DTR/TSGS-0021918vI00 ETSI, 2025.

26. CSIRO, *Final Project Report*, Milestone 4a in Project 1: Security and Privacy Protocols for Future Telecommunication Systems, CSIRO, 2024.

27. B. Sabir, D. Nguyen, N. Wu, S. Yang, S. Abuadbba, M. Ding, W. Ni, H. Suzuki and S. Lai, *Design and Implementation of attack strategies and defences using AI/ML methods for secure AI/ML spectrum management in 6G*, Milestone 4 in Project 4: AI/ML Spectrum Management and Adversarial Radio Characterisation, CSIRO, 2025.

28. B. Sabir, D. Nguyen, N. Wu, S. Yang, S. Abuadbba, M. Ding, W. Ni, H. Suzuki and S. Lai, *Initial assessment of AI/ML models for AI-enabled spectrum management in 6G*, Milestone 4 in Project 4: AI/ML Spectrum Management and Adversarial Radio Characterisation, CSIRO, 2024.

29. CSIRO, *6G Security and Privacy Mechanism Design*, Milestone 3 in Project 1: Security and Privacy Protocols for Future Telecommunication Systems, CSIRO, 2024.

30. V. Cheval, C. Jacomme, S. Kremer and R. Kunnermann, “SAPIC+: protocol verifiers of the world, unite!,” *Proc. 31st USENIX Security Symposium*, 2022.

31. D. Moody, R. Perlner, A. Regenscheid, A. Robinson and D. Cooper, “Transition to Post-Quantum Cryptography Standards,” *NIST Internal report*, 12 November 2024, Gaithersburg, MD; https://doi.org/10.6028/NIST.IR.8547.ipd

32. D. Liu, S. Jang, N. Sultan, S. Lai and S. Chau, *Integration of Post-Quantum Cryptography into CSIRO 5G Test Network: Final Report*, Final Report in Project 1 Extension Stream 3: Quantum-Safe Encryptiion Upgrade, CSIRO, 2025.

33. allbesmart.pt, “OAIBOX: The Ultimate Open Source 5G Platform for Academic and Industrial Research,” 2025, Last updated on 2 July 2025; Accessed on 15 August 2025; https://oaibox.allbesmart.pt/.

34. strongSwan project, “strongSwan - IPsec VPN for Linux, Android, FreeBSD, macOS, Windows,” 2025; Accessed on 17 July 2025; https://www.strongswan.org/.

35. Open Quantum Safe, “Open-source software for prototyping quantum-resistant cryptography,” 2025; Accessed on 17 July 2025; https://openquantumsafe.org/.

36. Y. Qu, M. Ding, S. M'rabet, X. Guan and S. Liu, *Design of Fuzz Testing Module*, Milestone 2 in Project 1 Extension Stream 2: Fuzz Testing, CSIRO, 2025.

37. C. Thapa, G. Jarrad, R. Holland, S. Ali Siddiqui, W. Shao and S. Camtepe, *Attacks on AI/ML Systems and AI/ML-Based Attacks and Countermeasures*, Milestone 3a in Project 2: Network Softwarisation and Cyber Vulnerabilities, CSIRO, 2024.

38. C. Thapa, G. Jarrad, R. Holland, S. Ali Siddiqui, W. Shao and S. Camtepe, *AI/ML-Based Security Solutions and An Example Tool*, Milestone 3b in Project 2: Network Softwarisation and Cyber Vulnerabilities, CSIRO, 2024.

39. N. Risse and M. Bohme, “Uncovering the Limits of Machine Learning for Automatic Vulnerability Detection,” *arxiv*, vol. Computer Science > Cryptography and Security, 2024.

40. Y. Chen, Z. Ding, L. Alowain, X. Chen and D. Wagner, “DiverseVul: A New Vulnerable Source Code Dataset for Deep Learning Based Vulnerability Detection,” *Proc. Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses*, Association for Computing Machinery, 2023, pp. 654–668.

41. R. Russell, L. Kim, L. Hamilton, T. Lazovich, J. Harer, O. Ozdemir, P. Ellingwood and M. McConley, “Automated Vulnerability Detection in Source Code Using Deep Representation Learning,” *Proc. 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2018, pp. 757-762.

42. F. Yamaguchi, N. Golde, D. Arp and K. Rieck, “Modeling and Discovering Vulnerabilities with Code Property Graphs,” *Proc. 2014 IEEE Symposium on Security and Privacy (SP)*, 2014, pp. 590-604.

43. W. Ni, L. Nguyen, S. Wei, M. Yang and S. Camtepe, *Design of Virtualisation and Segregation Strategy*, Milestone 1 in Project 2 Extension Stream 1: Virtualisation and Segregation of Data, CSIRO, 2024.

44. W. Ni, L. Nguyen, S. Wei, Y. Qu and S. Camtepe, *Implementation and Results of Virtualisation and Segregation Strategy*, Milestone 2 in Project 2 Extension Stream 1: Virtualisation and Segregation of Data, CSIRO, 2025.

45. International Standards Organisation, "ISO - IEC/ISO SMART," 2022, Last updated on 16 September; https://www.iso.org/smart.

46. L. Ly, M. Bahutair, M. Kim, C. Thapa and S. Camtepe, *GapCheckMate: Finding the Inconsistencies*, Milestone 2b in Project 3: The gap between standards and implementation, CSIRO, 2024.

47. M. Kim, M. Bahutair, C. Thapa, R. Holland, S. Ali Siddiqui, D. Wang, W. Shao, S. Camtepe and H. Suzuki, *CompCheck: A Security Compliance Check Tool*, Milestone 3b in Project 3: The gap between standards and implementation in future telecommunication systems, CSIRO, 2025.

48. National Institute of Standards and Technology Computer Security Resource Center, "Cryptographic Module Validation Program | CSRC," 2025, Last updated on 25 June; https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules.

49. C. Thapa, R. Holland, W. Shao, M. Kim, M. Bahutair, S. Ali Siddiqui, D. Wang, S. Camtepe and H. Suzuki, *Compliance guidelines for telecomunications in the Australian Context*, Milestone 3a in Project 3: The gap between standards and implementation in future telecommunication systems, CSIRO, 2025.

50. International Standards Organisation, "ISO 31000 Risk Management," *Book ISO 31000 Risk Management*, Series ISO 31000 Risk Managemented., Editor, ed.^eds., iso.org, 2021.

51. International Standards Organisation, "ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on Managing information security risks," *Book ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on Managing information security risks*, Series ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on Managing information security risksed., Editor, ed.^eds., iso.org, 2022.

52. International Standards Organisation, "IEC 31020:2019Risk management — Risk assessment techniques," *Book IEC 31020:2019Risk management — Risk assessment techniques*, Series IEC 31020:2019Risk management — Risk assessment techniquesed., Editor, ed.^eds., iso.org, 2022.

53. Joint task force transformation initiative, "Risk management framework for information systems and organizations: a system life cycle approach for security and privacy," December 2018, Gaithersburg, MD.

54. I.T.U.-. Telecommunication, "ITU-T X.1055 Risk management and risk profile guidelines for telecommunication orgnanizations," *Book ITU-T X.1055 Risk management and risk profile guidelines for telecommunication orgnanizations*, Series ITU-T X.1055 Risk management and risk profile guidelines for telecommunication orgnanizationsed., Editor, ed.^eds., itu.int, 2018.

55. C. Thapa, S. Ali Siddiqui, D. Wang, M. Bahutair, M. Kim, R. Holland, W. Shao, S. Camtepe and H. Suzuki, *From Detection to Risk Management: A Review of Gap detection in 5G/6G Software Components and Risk Management*, Milestone 2a in Project 3: The gap between standards and implementation in future telecommunications systems, CSIRO, 2024.

56. S. ali Siddiqui, C. thapa, R. Holland, W. shao and S. Camtepe, "Elevating Software Trust: Unveiling and Quantifying the Risk Landscape," *arxiv*, vol. Computer Science > Software Engineering, 2024.

57. A. Alkhateeb, “DeepMIMO: A generic deep learning dataset for millimeter wave and massive MIMO applications,” *arXiv preprint arXiv:1902.06435*, 2019.

58. H. Suzuki, A. Guabtni, M. Lorestani, Q. Fu, L. Nguyen, S. Yu, S. Jang, J. Chan and T. Rakotoarivelo, *Design, Implementation and Characterisation of Physical Twin Research Platform and Radio Testing Environment*, Milestone 1a in Program Extension Stream 1: CSIRO Digital Twin Enabled 6G Research, CSIRO, 2024.

59. H. Suzuki, A. Guabtni, M. Lorestani, Q. Fu, L. Nguyen, S. Yu, S. Jang, J. Chan and T. Rakotoarivelo, *Preliminary Experimental Performance Results of Digital Twin Research Platform*, Milestone 2 in Program Extension Stream 1: CSIRO Digital Twin Enabled 6G Research Platform, CSIRO, 2025.

60. openairinterface.org, “OpenAirInterface 5G software alliance for democratising wireless innovation,” 2025; Accessed on 15 August 2025; https://openairinterface.org/.

61. Ettus Research, “Ettus Research - The leader in Software Defined Radio (SDR),” 2025; Accessed on 15 August 2025; https://www.ettus.com/.

62. NVIDIADeveloper, “NVIDIA Aerial,” 2025; Accessed on 15 August 2025; https://developer.nvidia.com/aerial.

63. mathworks.com, “Antenna Toolbox,” 2025; Accessed on 15 August 2025; https://au.mathworks.com/products/antenna.html.

64. Open Networking Foundation, “AETHER - Open Networking Foundation,” 2024, Last updated on 14 October; Accessed on 15 August 2025; https://opennetworking.org/aether/.

65. Centre Tecnologic de Telecommunicacions de Catalunya, “5G-LENA module,” 2025; Accessed on 15 August 2025; https://5g-lena.cttc.es/.

66. neo4j.com, “Neo4j Graph Database & Analytics – The Leader in Graph Databases,” 2025; Accessed on 15 August 2025; https://neo4j.com/.

67. University of Technology Sydney, “Australian researchers prove world-leading flood sensing technology,” 16 June 2025; https://www.uts.edu.au/news/2025/06/australian-researchers-prove-world-leading-flood-sensing-technology.

68. C. Thapa, R. Holland, S. Ali Siddiqui, S. Abuadbba, S. Camtepe, D. Liu and S. Nepal, *Survey report*, Milestone 1 in Project 2: Network softwarisation and cyber vulnerabilities, CSIRO, 2023.

As Australia's national science agency, CSIRO is solving the greatest challenges through innovative science and technology.

CSIRO. Creating a better future for everyone.

Contact us

1300 363 400
+61 3 9545 2176
csiro.au/contact
csiro.au

For further information

Data61
Surya Nepal
+61 2 9272 4256
surya.nepal@csiro.au
csiro.au/Data61