ABIresearch®
TRUSTED INTELLIGENCE SINCE 1990

6GWORLD™

Conceptualizing Security in a 6G World

Conceptualizing Security in a 6G World

Michela Menting, Analyst, ABI Research

CONTENTS

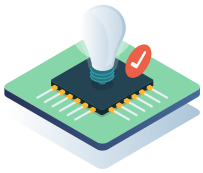
6G CONCEPTS AND WHAT THEY MEAN FOR SECURITY

The advent of 6G wireless communications is still about a decade away. Nonetheless, initial discussion around emerging technologies and potential applications for this next generation has already begun. Broadly speaking, the current focus is on whether 6G should be an improvement on 5G in terms of core capabilities, or whether it should go beyond existing coverage to new areas, such as undersea and in space or even on a molecular level. Ultimately, if 6G is to achieve the latter, it must first, address the former.

While 5G is setting the stage for low transmission latency, reliability, high data rates, and capacity for massive connectivity, the various concepts still need to be offset against each other (e.g., reliability versus latency; high data rate versus massive capacity, etc.). 6G must improve significantly on these concepts and minimize the trade-off between them. In order to achieve this, new enabling technologies need to be devised, from developing and using new frequency bands (sub-mmWave, Terahertz, and visible light), to achieving spectrum and energy efficiency, and implementing Deep Learning (DL)-based communications. Only then can there be meaningful discussions around creating micro- and macro-level networks.

As with any new technologies, new threats will emerge that need to be addressed, in addition to any existing threats that will be carried over from past generation networks. The nature of these threats will depend, in large part, on any inherent vulnerabilities in the design, development, and implementation of 6G wireless communications; and on efforts to remediate existing vulnerabilities. As always with security, its successful application will depend on the due diligence of appropriate risk assessments and threat modeling.

Currently, it is difficult to envision such pre-emptive measures as 6G technologies themselves remaining undefined. But it is important that they be acknowledged as part and parcel of the technology development and the standardization process. Some preliminary security assessments can already be initiated by examining the risk exposure of proposed 6G technologies.



Artificial Intelligence

One of the core ideas is that 6G networks should be imbued with pervasive and distributed Artificial Intelligence (AI). Discussions abound about an "AI-empowered" network with a deep integration of AI tools in network functions and decision-making processes.

However, AI technologies present two major dangers in general that will affect 6G profoundly. The first is a vulnerability to attack. Adversarial manipulation to a Machine Learning (ML) model, such as subtle changes to input, can be carefully crafted either at training or at test time to undermine their predictions or to extract information through reverse engineering. Even deep Convolutional Neural Networks (CNNs), likely to be used in 6G, are sensitive to adversarial perturbations due to their nature and tendency to overfit. This poses a problem with the deployment of novel AI systems, which may inadvertently open themselves up to attacks that can exploit these inherent vulnerabilities.

The second danger is a threat of misuse through the creation of models that can be used for harmful purposes: either maliciously (for the perpetration of crime—cyber and physical), or within the context of military or law enforcement (to defensive or offensive ends).

There is little doubt that AI presents an opportunity for malicious actors on both fronts. The more pervasive the AI, the greater the incentive to exploit it. AI undoubtedly poses a danger to modern technologies in its decision-making capacity and, more broadly, as interdependency with 6G networks becomes intrinsically embedded into the functioning of modern societies. All these risks need to be considered throughout the 6G development—and deployment—process.

RESOURCES

Adversarial Machine Learning: A Brief Introduction for Non-Technical Audiences

READ NOW

The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation

READ NOW

IT-OT Convergence

The Internet of Things (IoT) will be a key use case for 5G in Massive Machine-Type Communications (mMTC), especially as Operational Technology (OT) continues to converge with Information Technology (IT). As for 6G, the enhancement will be to provide greater mobile broadband capabilities generally for the IoT edge, alongside increased high-rate data sharing, and even lower latencies. A 6G network that can provide a real-time intelligent edge will be critical for the success of fully autonomous processes in driverless cars, Industry 4.0 management, and smart healthcare, among others.

IoT devices today are high-risk assets generally lacking in cybersecurity. The difficulty in securing them often lies in the inherent characteristics of the IoT devices themselves. On one end of the scale, their limited computing and connectivity capabilities makes them unfit for the more traditional resource-intensive IT security applications. On the other end, for those devices serving mission-critical and hard real-time functions, delay and latency are simply unacceptable, with a missed deadline potentially resulting in catastrophic failure. Traditional cybersecurity, which prioritizes confidentiality and integrity, is often in direct opposition to functional safety and deterministic requirements.

Real-time intelligence for the edge must offer precise timing, reliability, predictability, and consistency in its responses. Today, there are few applications of effective cybersecurity in intelligent IoT devices that can guarantee confidentiality and integrity in an autonomous, real-time manner, although efforts in the automotive space are promising for self-driving cars. 6G networks achieving security in an IT-OT converged world and real-time intelligence for the edge will require increased efforts in developing appropriate cybersecurity mechanisms that can support the primary directives of functional safety and mission-critical systems on the massive scale at which IoT deployments are projected to grow in the next decade.

RESOURCES

Insecurity in the Internet of Things, IOT Security Foundation

READ NOW

OWASP Internet of Things Project, Top 10 2018

READ NOW

Self-Adaptive and Self-Preserving Networks

In a 6G scenario, self-adaptive and self-preserving networks (such as those planned for intelligent radio) aim to achieve a communication framework that can be dynamically configured and updated, but that can also autonomously respond to adverse events, while continuing normal operations.

Realizing such self-adaptive/self-preserving networks is not yet feasible on a commercial level because they intrinsically rely upon automation and real-time intelligence processing. There are numerous theoretic research efforts in the space, although they remain relatively isolated and independent. The key ingredient, but also the main barrier to achieving cyber-resilient networks, is cybersecurity, primarily because automation and AI are not yet fully exploited in this space.

On the one hand, network security and traffic management, malware signature and patch delivery, and adverse event alerts, for example, are all areas where automation and ML have been mastered. On the other hand, complex threat discovery, incident response, defensive maintenance, and adaptive remediation have yet to fully take advantage of either.

Offensive security, in particular, as an extension of incident response, involves proactively hunting for indicators of compromise in advance of detective controls identifying them. The offensive market is still largely dominated by manual input and human interaction, and is not as mature as the more traditional defensive security market.

The difficulty is not so much in responding, but in automatically correlating an incident with the appropriate response. The determination of that response, especially when faced with unknowns (e.g., zero-days), needs to rely on some form of intelligent understanding that can effectively decide the appropriate response; this will be AI's task in 6G networks. Short of employing AI, human intelligence is currently the best technique for that determination. Consequently, many features pertaining to on-the fly dynamic reconfiguration, dynamic positioning, realignment, and unpredictability techniques, which are key to achieving self-preserving networks, cannot be automated due to human limitations. The advent of automation and AI in 6G may change this significantly and will accelerate the development of self-adaptive architectures. But for the foreseeable future, the autonomous adaptation and self-preservation of networks, especially those composed of massively connected endpoints, remains elusive.

RESOURCES

Cyber Security Automation: Benefit or a Threat? DFLabs

READ NOW

Automation is now No. 1 for SecOps: How to put it to work on your team, TechBeacon

READ NOW

Quantum Computing

Quantum developments pose a critical threat to modern cybersecurity technologies and are of grave concern to the confidentiality, integrity, and privacy of personal information, business interests, and national security. And most certainly, this will be of key concern to 6G as it is predicated on emerging at the same time as attack-capable quantum computers (a possible reality by 2030). Such computers would be able to break complex asymmetric encryption algorithms, such as RSA and elliptic curve cryptography. New algorithms will need to be developed and standardized.

The development of quantum-resistant primitives today is already late when looking at estimates for the commercialization of attack-capable quantum computers. Therefore, it is imperative that 6G take this threat into account when standardizing around acceptable cryptographic algorithms. The security of modern Information and Communications Technology (ICT) and digital data is already at risk, not the least because there are threat actors (both organized crime and state-sponsored) that are already actively harvesting encrypted data and holding on to it, with the goal of decrypting it later when quantum-attack-capable computers become available. The imperative is to develop quantum-resistant cipher suites as soon as possible, if they are to be leveraged in 6G networks.

RESOURCES

Does quantum computing put our digital security at risk?
Internet Society

READ NOW

Quantum Computing and Cryptography,
EDPS TechDispatch

READ NOW

Technology	Risk Level	Primary Cause	Time Frame
AI	Medium	Adversarial manipulation and malicious AI development	<3 years
IT-OT Convergence	High	Lack of cybersecurity designed and deployed in IoT devices	Immediate
Self-Adaptive Networks	Medium	Lack of automation and real-time intelligence processing	>5 years
Quantum Computers	High	Break complex encryption asymmetric algorithms	>10 years

AND VICE VERSA: THE IMPACT OF SECURITY ON 6G

The decade until the advent of 6G provides time enough for the industry to assess a number of future risks and to start working (and advance existing work) on potential security solutions. Certainly, in many of the areas raised earlier, efforts are underway to mitigate risks.

Adversarial Machine Learning

In terms of AI threats, the development of AI-based and cognitive cybersecurity has been in development for some time. Cybersecurity is a discipline that exists in an adversarial environment, and adversarial manipulation is an expected response. The vulnerability of ML to adversarial inputs has led to a research field focusing on better evaluating their robustness and developing defenses against potential attacks, known as adversarial ML. A nascent generic movement is addressing the potential misuse of AI more broadly, and 6G is well placed to accelerate developments in this area if it means imbuing its infrastructure with AI.

In order to address the current ML shortcomings, the industry is focused on developing the ability to "detect the seemingly undetectable" and "predict the unknown threat." The first effort is aimed at continuously monitoring behavioral data and deciphering patterns in order to root out existing threats on a network before they can be actualized, and minimizing the amount of time it takes to detect them.

Predicting the unknown threat is part of the broader predictive/proactive movement in cybersecurity that rests within DL applications and focuses on the continuous and autonomous retraining of ML algorithms with large amounts of unstructured, unlabeled data.

Currently, the fields of research are focused on adversarial ML, security evaluations, adversarial training, game theoretic models, generative adversarial networks, and multiple classifier systems. Methods in the field of cognitive computing are also providing promising, if still very preliminary, results for more accurately detecting the unknown. All of these areas should be explored in detail for strengthening AI in 6G networks, and for anticipating AI-based threats.

RESOURCES

Adversarial Machine Learning, DeepAI

READ NOW

Artificial Intelligence: Adversarial Machine Learning, NCCOE

READ NOW

Cyber-Resiliency

The achievement of self-adaptive and self-preserving 6G networks requires adopting a cyber-resiliency approach. The overarching objective of implementing a cyber-resilient strategy within an infrastructure is to maintain operations in an environment that contains faulty or hostile elements. In the deployment of such a strategy, the infrastructure must accept that a potentially malicious element is disrupting the operating environment or may do so at any point in the future. Therefore, the goal is to prepare for this event, to be able to withstand its effects, and then to evolve and adapt. The concept is a natural progression from cybersecurity and business continuity that requires agility and flexibility.

Crucially, following cyber-resiliency development principles will provide understanding of both the threats and the vulnerabilities that 6G networks may be exposed to, and allow better awareness and the eventual development of more effective response processes. Security, and cyber-resiliency more broadly, must play an operational role, rather than a finite, static one. It is not only about achieving a desired state, but of perpetuating that state, making it flexible enough so that it can bend and change according to the threat and technological environment. Automation, therefore, depends not only on the human understanding of systems and the requirements of cyber-resiliency, but also on translating those accurately to an AI solution. Consequently, machine guidance, behavioral learning, pattern recognition, and security analytics become important concepts in a self-adaptive and self-preserving 6G network.

RESOURCES

Cyber Resiliency Design Principles, MITRE

READ NOW

Cyber Resilience Review (CRR), DHS

READ NOW

Post-Quantum Cryptography

Post-Quantum Cryptography (PQC) is concerned with creating quantum-resistant ciphers that future quantum computers cannot crack. A number of promising algorithms that can be considered quantum-resistant (lattice-based, code-based, multivariate quadratic-based, hash-based, and isogeny-based cryptography) have been developed over the years, although standardization has not yet been finalized on any. All of these advances are promising for a dynamic development of quantum-safe cryptography that can be effectively implemented in 6G architectures.

However, the transition to quantum-resistant cryptography will take time; certainly in terms of standardization and then in application. In the interim, the concept of crypto-agility has begun to take hold. This refers to the ability to transition smoothly from pre- to post-quantum security and can be achieved through hybrid cryptographic solutions. This type of technology encapsulates current existing standards (such as RSA and ECC) into new quantum-resistant ones (like NewHope). The idea is that if one or the other of the schemes fails (or is corrupted), then the other remains in place to provide a dual protection mechanism. There is little doubt that crypto-agility will be a requirement for any 6G standard, even if quantum-attack computers have not yet emerged.

Beyond PQC are developments in Quantum Key Distribution (QKD). QKD relies on quantum-based physical principles to protect against potential quantum attacks. It is already being commercialized as it is achievable using current technologies, such as lasers and fiber optics. In that sense, QKD is one of the first quantum theories to find real-world applications, alongside quantum clocks and quantum satellites. It is already being explored for 5G and, therefore, it is a strong candidate for 6G networks.

RESOURCES

Post-Quantum Cryptography, NIST

READ NOW

Post-Quantum Cryptography: Current state and quantum mitigation

READ NOW

Blockchain and Quantum Computing, MITRE

READ NOW

Privacy-Aware Networks and Zero-Trust Architectures

In addition to being secure, an AI-based 6G network should be privacy preserving, whether the data be derived from devices or from people directly. However, the two goals of utility and privacy are inherently conflicting. The more accurate and, therefore, useful a ML model is, the less it can preserve the privacy of the training data.

One way of maintaining accuracy and defending against privacy and confidentiality attacks is to use differential privacy, which aims to preserve query accuracy, while minimizing leakage or identification of the data. Alternative solutions include multi-party computation (training ML systems on sensitive data without significantly compromising privacy), disinformation, randomization techniques (e.g., randomizing the collection of training data—or even the output), and using difficult to reverse-engineer classifiers, for example. Federated learning is another potential solution that allows the training of algorithms across decentralized edge devices, with each device holding their data locally without sharing them with the wider group.

In large part, privacy-aware networks in 6G will need to operate around zero-trust models. This goes back to the idea of cyber-resilient networks functioning with the knowledge that they may be operating with known or unknown hostile elements within them. No asset is trusted implicitly, so continuous access control, authentication, and identification are leveraged to ensure only legitimate parties with the right credentials and approved policies can access and process data. Zero-trust networking, which is already being advocated for 5G, will pave the way for end-to-end deployment in 6G, enabling highly personalized security policies, communications, and data privacy.

RESOURCES

Differential Privacy, Harvard University Privacy Tools Project

READ NOW

What is Zero Trust? A model for more effective security, CSO Online

READ NOW

Distributed Ledger Technology

Achieving cyber-resilient and secure AI-infused networks for 6G is a tall order; but not an impossible one when considered through the lens of containerization and decentralization. The creation of connected but contained, independently intelligent subnetworks offers the possibility of customizing protection mechanisms on a much smaller scale. The idea of decentralizing security is key here, with the cognitive abilities of the 6G network capable of assessing and managing risks appropriately for each subnet on a continuous basis. Security in this scenario is not dictated by a higher network function or from the core; it effectively becomes an autonomous, responsive part of a connected whole.

This idea of decentralization can already be found today in Distributed Ledger Technology (DLT), such as blockchain. At its core, these are immutable, transparent, and autonomous ledgers (public or private) that use distributed consensus and cryptography to provide an authoritative record of secure transactions. Digital signatures, hashing, and consensus mechanisms are used to enable untrusted parties to transact directly in a secure manner. DLT effectively operates on a model known as trustless trust, which is a good fit with privacy-preservation notions, zero-trust networks, and cyber-resiliency required for 6G. Without a centralized authority to manage transactions, blockchain assets can operate in relative independence. Business logic can be programmed through smart contracts, with policies and agreements able to automatically execute peer-to-peer at subnet levels. DLT can provide a new level of secure autonomy ins 6G networks, from resource management to spectrum sharing.

RESOURCES

Blockchain Explained, Investopedia	*Ethereum Whitepaper*	*An Introduction to Hyperledger*
READ NOW	READ NOW	READ NOW

Technology	Goal	Time Frame
Zero-Trust Architectures	No asset is trusted implicitly, and continuous access control, authentication and identification are used inside the network.	Immediate
DLT	Immutable, transparent, and autonomous ledgers using distributed consensus and cryptography to provide an authoritative record of secure transactions	Immediate
PQC	The development and standardization of quantum-resistant ciphers.	<2 years
Privacy-Aware Networks	Use of privacy-preserving techniques, such as differential privacy, disinformation, and randomization.	<3 years
Adversarial ML	Better evaluate ML algorithm's robustness and the development of defenses against attacks.	<5 years
Cyber-Resiliency	Continuously prepared for adverse events, ability to with-stand attacks, autonomously evolve, and adapt to threats.	>5 years

AN OPPORTUNITY TO RETHINK SECURITY

Threats and Expanded Risks

Greater connectivity to people, machines and systems, richer data generation, and deeper network integration with AI ultimately expands the 6G threat landscape considerably, with more complex and sophisticated threats likely to emerge. There is little doubt that threat actors will take advantage of this to exploit 6G, so the technology development and eventual standardization processes must take these factors into account. Importantly, there are lessons that can be learned from how 5G security applications will evolve, so the development of 6G security must pay close attention to how the security industry deals with emerging risks and threats in that space.

Security by Design

6G provides an opportunity to integrate security at the heart of the infrastructure and to imbue the whole network end-to-end with a security strategy that is intelligent and autonomous, building upon what will be adopted in 5G. Enabling flexibility will allow 6G networks to adapt to different situations and novel events as they arise. Importantly, it is a strategy that accepts that 100% security does not exist, and so is aware it needs to operate even in adverse environments. In addition to embedding security in the devices and the networks themselves, designing failsafe mechanisms and contingency plans is key for 6G. These plans must include the potential threats posed by AI, quantum computing, and massively pervasive IoT.

Beyond that, the standardization process for 6G must provide transparency (risk awareness), choice (acceptance, rejection, or modification of that risk), and control (over usage). Ultimately, these prerogatives need to be applied throughout the security stack: at the network and device levels, within applications and with regard to data if a comprehensive security strategy is to permeate end-to-end.

Step-by-Step

Crucial to a truly solid security development process for 6G will be industry-wide participation from: network equipment providers, network operators, hyperscalers, high-performance computing providers, pure-play cybersecurity vendors, service providers, original equipment providers and manufacturers, as well as consortiums, international organizations, governments, and enterprises.

The difficulty with selling security, despite the understood risks, is the cost-risk analysis model used by many stakeholders when they decide whether to integrate security or not. These risks can be accepted or transferred onward (through insurance companies or to end users), without any supplementary security requirements built in and this is acceptable in some cases. But as 6G seeks to connect much further, and more deeply, within societies and with people, such risks require an appropriate security response—and not simply an acknowledgement they exist without requisite safeguards. The digital threat to cyber-physical operations exists today, but this threat will be exponentially greater in a decade.

In order to achieve comprehensive security in 6G, the first step requires investment in security technologies for the infrastructure, its applications, and the users. Security is a necessary cost with a dedicated budget and management strategy, driven by standardization, regulation, business confidentiality, and privacy imperatives.

Beyond that, as a second step, providing security in its own right can be a business enabler and revenue generator; this is where security becomes more palatable to those adverse to security spending. Investments can be turned around to provide a security service or software offering down the line. The big driver here is enterprise interest and adoption.

No doubt, there will be a fragmented approach at first, which standardization can counter to a certain extent, followed by a multi-vendor marketplace. But there can be strength in distribution and fragmentation; if the industry plans ahead and designs, develops, and implements security at the start and throughout 6G technology development and evolution. In fact, it is a golden opportunity to get security right and ensure the success of 6G as a truly transformational technology.

Recommendations for 6G Stakeholders

Stakeholders in the 6G standardization process, as well as the developers and creators of the network, must ensure that security forms a core part of the architecture. It is key that they embrace security throughout the life cycle of 6G: from inception to its obsolescence. Key strategies to keep in mind for the successful implementation and management of security are summarized below:

- Ensure that security is continuously addressed throughout the 6G standardization process, and leverage security lessons learned from 5G networks.
- Engage in security discussions for emerging technologies: IoT, automation, AI, quantum computing; whether that is assessing the risks or using the strengths of that technology in the security field.
- A multi-stakeholder and multi-disciplinary environment is important to ensuring that all assets that will form part of 6G networks are afforded the same security evaluation; even the smallest and most insignificant assets must consider security.
- Understand that security always starts and ends with risk assessment. This provides visibility into vulnerabilities, threats, and detection and response capabilities. It is a fine balance and one that relies on the understanding first and foremost.
- Security is more than just about technology; it is also about people and processes. Education on 6G and security is critical to ensuring comprehensive protection for a network that will be vast, complex, and highly diverse, with participants as wide and varied as the technologies that compose it.

Published March ©2021
ABI Research
249 South Street
Oyster Bay, New York 11771 USA
Tel: +1 516-624-2500
www.abiresearch.com

About 6GWorld

As we step from the birth of commercial 5G today to the birth of commercial 6G, the world will change radically; in technology, business models, attitudes, and needs. How do we navigate through this and deliver the solutions that are actually needed? Only by bringing together a community of advanced researchers, commercial leaders and experts of all kinds to share their insights. www.6GWorld.com is this community!

About ABI Research

ABI Research provides actionable research and strategic guidance – to technology leaders, innovators, and decision makers around the world – that focuses on transformative technologies that are dramatically reshaping industries, economies, and workforces today. ABI Research's global team of analysts publish groundbreaking studies often years ahead of other technology advisory firms, empowering clients to stay ahead of their markets and their competitors.