NEXT G ALLIANCE
An ATIS Initiative

Trust, Security, and Resilience
Sustainability
Digital World Experiences
Audacious Goals
AI-Native Wireless Solutions
Cost-Efficient Solutions
Distributed Cloud and Communications Systems
Trust, Security, and Resilience

Next G Alliance Report: **Trust, Security, and Resilience for 6G Systems**

TABLE OF CONTENTS

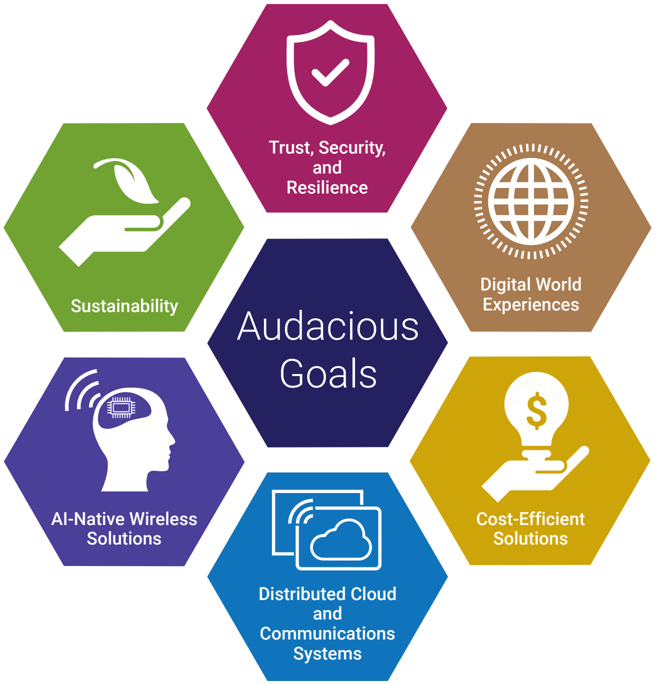
FOREWORD

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's business priorities. ATIS' 150 member companies are currently working to address network reliability, 5G, robocall mitigation, smart cities, artificial intelligence (AI)-enabled networks, distributed ledger/blockchain technology, cybersecurity, IoT, emergency services, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open-source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL).

For more information, visit www.atis.org. Follow ATIS on Twitter and on LinkedIn.

The ATIS Next G Alliance is an initiative to advance North American wireless technology leadership over the next decade through private sector-led efforts. With a strong emphasis on technology commercialization, the work will encompass the full lifecycle of research and development, manufacturing, standardization, and market readiness.


Trust, Security, and Resilience
Sustainability
Digital World Experiences
Audacious Goals
AI-Native Wireless Solutions
Cost-Efficient Solutions
Distributed Cloud and Communications Systems

EXECUTIVE SUMMARY

The introduction of 5G networks has seen the manifestation of a desire to accommodate use cases of a more critical nature that span broad societal objectives, including ones that seek to automate manufacturing, process control, utilities, transportation, logistics, etc. It has become apparent that many of these scenarios demand levels of performance, security, and resilience that will significantly alter the landscape of attack surfaces presented by faults, disturbances, threats, and anomalies within the connectivity and computational services provided by the network. Additionally, it has become clear that there is an imminent need to eliminate all single points of failure. There is also a clear need to architect a network based on zero-trust principles in a manner that affords users high levels of reliability, availability, functional safety, and privacy. The development of 6G technologies will accommodate these needs more effectively, even as standalone 5G systems continue to be improved to meet immediate concerns associated with earlier design choices.

Trustworthiness is defined in this paper as confidence in the ability of the 6G system to perform as expected in the face of environmental disturbances, impairments, errors, faults, and attacks. This definition has several proof points specific to the establishment of Information and Communications Technologies (ICT) and pertinent to 6G:

1. Business processes and economic value chains are organized not to create doubt in equipment, actors, and processes associated with network services.
2. Diligence in developing standards that can be tested and certified for consistency with well-defined requirements.
3. Networks and associated services that are secure, privacy-preserving, reliable, available, and resilient.
4. Assurance that the network equipment and associated services are interoperable across the ecosystem and that networks are deployed and operated in accordance with user expectations.

As the network evolves to 6G, new applications will be added that enhance digital world experiences utilizing the internet of senses and improvements related to extended reality (XR) capabilities. Although cellular technologies can be deployed to serve all these use cases, it has been challenging to establish the ability of these technologies to meet industry stakeholders' security, privacy, and resilience requirements. Stakeholders are concerned about the adoption of wireless technologies into their workflows: cyber-attacks, privacy violations, data theft, exposure of vulnerabilities due to the introduction of distributed cloud computation and storage, and the increased use of AI through adaptive learning algorithms that will depend on assurance of data integrity, privacy, and explainability. Governments have concerns about the trustworthiness of the supply chain and the ecosystem's ability to overcome dynamic threats rapidly.

1 INTRODUCTION

3G and 4G established engines of transformation that enabled the exponential increase of bandwidth in networks, the expansion of coverage for all users, and the ability to handle mobility and service continuity across the internet for telecommunications and information services, including operational, enterprise, and industrial service scenarios. The importance of networks in society is clear today, and in the 2030s, their role will be even more critical. Users and our societies expect a network they can depend on and trust under all circumstances. This largely means a reliable, resilient system that secures communication and information.

Previous generations of mobile telecommunications systems were designed to provide a minimum grade of service for various human-centric use cases such as telephony. Networks were designed to meet strict requirements that optimized continuity of communications during events such as handovers. Regulations require reliability in locating emergency callers. The mobile subscription identity is routinely used to authenticate users for a variety of everyday tasks, such as by using Short Message Service (SMS) to return one-time passcodes. Restrictions exist against privacy violations of the telecommunications network, making it illegal to eavesdrop on conversations, with exceptions for law enforcement activities covered by a warrant. From the time of 2G, the airlink has been protected by encrypting the control and user planes, while successive generations have strengthened security. The 5G New Radio (NR) waveform has integrity protection and encryption for Network Access Signaling (NAS), Radio Resource Control (RRC), and user plane data, while 4G LTE initially offered integrity protection for control and signaling information alone. Adoption of more recent integrity protection features will be driven by the market. The Subscriber Identity Module (SIM) has evolved to support multiple strong user identities for devices and subscription profiles with Enhanced Integrated Circuit Cards (eUICC). Responsible system building practices ensure the use of authenticated hardware and software with encryption across network interfaces and tunnels.

As mobile phones and other devices started to support an IP-centric network, information services and applications were dissociated from network operator control. The result has been transforming the network into a rich and diverse set of capabilities that support a wide variety of use cases: web access, navigation, entertainment, and the Internet of Things (IoT). The introduction of 4G and 5G networks has seen the manifestation of a desire to accommodate use cases of a more critical nature that span broad societal objectives, including critical use cases that seek to automate manufacturing, process control, utilities, transportation, logistics, etc. It has become apparent that many of these scenarios demand levels of performance, security, and resilience that will significantly alter the landscape of attack surfaces presented by faults, disturbances, threats, and anomalies within the connectivity and computational services provided by the network.

Another aspect of trust has to do with providing an assurance of safety to end users. The system must be reliable enough to minimize the probability that a loss of network connectivity will result in personal harm to individuals interacting with their environment or functional harm to machinery. The development of 6G technologies will accommodate these needs more effectively, even as standalone 5G systems continue to be improved to meet immediate concerns associated with earlier design choices.

The 5G system was designed to ensure a high degree of compatibility with the requirements of many of these use cases. However, it has been realized that there is a long and complicated path toward a highly available, resilient network that meets associated security, reliability, and privacy considerations. Several network trends are imposing new requirements on 6G:

> Viability of general-purpose hardware for real-time functionality.

> Disaggregation of RAN and core functions.

> Introduction of the service-based architecture that deploys virtualized network functions that can be dynamically and elastically deployed on demand.

> Use of network slices to meet a variety of operational objectives such as virtualization of services, customization of experience, etc.

> Use of edge computational or storage resources for local connectivity, storage caching, low latency, and computational offloading from user equipment to the network.

> Introduction of specialized computational resources that can integrate artificial intelligence and inferential learning into many service and operational workflows, as well as customer-facing features.

> Introduction of XR applications and joint communication and sensing pose challenges for performance, privacy, and security.

> Introduction of multipath communication and other redundancy and recovery mechanisms that address challenges posed to the reliability, security, and network resilience by faults and failures.

These trends are expected to improve the flexibility of the network immensely, but they also pose tremendous challenges for network resilience and security. Security threats will vastly expand the attack surfaces within the network, further complicated by the sheer numbers of devices connected to 6G networks. The applicability of 6G in many critical applications places strict requirements on dependability, resilience, attack resistance, detection, and mitigation that surpass those of previous generations.

Trustworthiness may be defined as the measure of confidence in the behavior of a person, organization, or technological solution. For mobile communication networks, trust is built up from sentiments gathered from a variety of sources that include geopolitical realities, supply chain reliability, design requirements, standardization of interfaces, technological tools, operational resilience, risk management, and comprehensive test and certification. The technological implications of trustworthiness may be isolated as follows. In the case of engineering systems, including networks, trustworthiness is defined as the confidence in the ability that a system performs as expected in the face of environmental disturbances, impairments, errors, faults, and attacks. This definition of trustworthiness has several proof points specific to the establishment of ICT and pertinent to 6G:

- Business processes and economic value chains are organized in a manner that does not create a lack of confidence in equipment, actors, and processes associated with network services.
- Diligence in developing standards that can be tested and certified for consistency with well-defined requirements.
- Networks and associated services that are secure, privacy-preserving, reliable, available, and resilient.
- Assurance that the network equipment and associated services are interoperable across the ecosystem and that networks are deployed and operated in accordance with the expectations of users.

This brings us to the primary purpose of trustworthy lifecycle practices as applied to 6G networks:

The 6G system will be trusted by people, businesses, and governments to be resilient, secure, privacy-preserving, safe, reliable, dependable, and available under all circumstances.

2 DRIVING FORCES AND NORTH AMERICAN IMPERATIVES

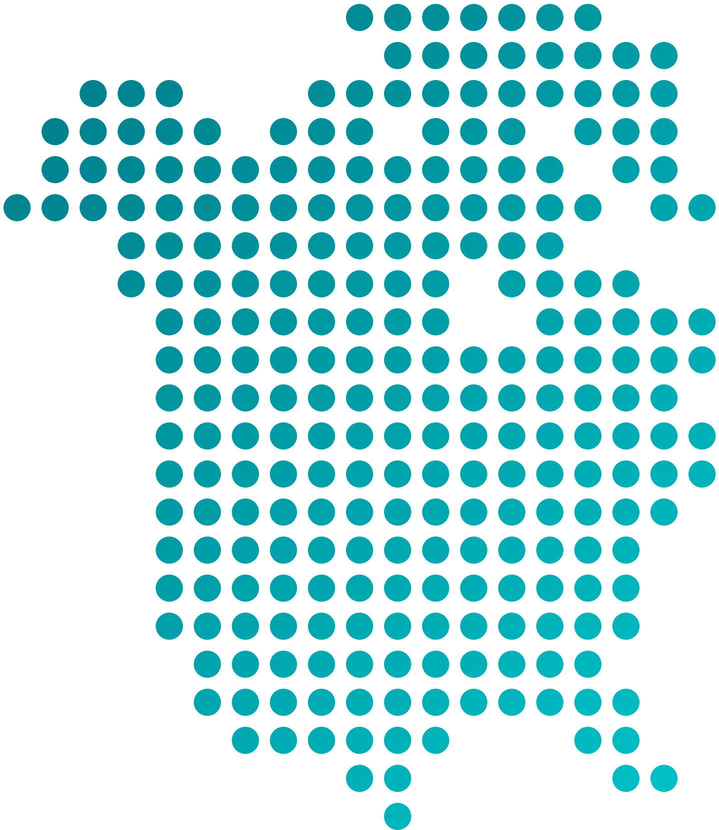
Wireless technologies are at the frontier of automation of society, while wireless telecommunications systems have achieved a grade of service equivalent or superior to wired telephony or internet service for a limited number of human-centric or best-effort applications. However, the opportunities available for expansion of wireless technologies into new applications are limited by several challenges. The most significant opportunities are identifiable in the potential of automated systems from bespoke wired technologies to standardized wireless technologies. Cellular technologies based on 5G, and future generations, meet some gating requirements (e.g., spectrum with high quality and availability, interference resistance, a well-structured security architecture, cost-effective equipment with global scale, wide-area mobility, and local-area connectivity).

Cellular technologies have been considered for inclusion within many critical societal services since IMT-Advanced and the introduction of 4G LTE and 5G NR. Services such as industrial automation, automotive/transportation, healthcare, utilities, and public safety create significant demand on communication system reliability. As the network evolves to 6G, new applications will be added that enhance digital world experiences utilizing the Internet of senses and improvements related to XR capabilities. Although cellular technologies can be deployed to serve all these use cases, it has been challenging to determine whether these technologies can meet the security, privacy, and resilience requirements demanded by those industry stakeholders. The introduction of cloud technologies and the trend toward disaggregation of the RAN and core network components into a Service-Based Architecture (SBA) have created great promise and greater uncertainty to the confidence needed in wireless technologies.

The use of cellular technologies in automation tasks also introduces new concerns among stakeholders, namely industry partners, regulators, and national security entities. These concerns are sometimes related to the exposure of networks to larger threat surfaces. Examples include greater vulnerability to cyberattacks such as denial of service attacks, privacy violations by way of eavesdropping or traffic analysis, and man-in-the-middle attacks. Additional threats to data privacy and integrity are exposed by the use of cloud computing and storage; multi-tenanted network infrastructure may be susceptible to side-channel attacks that are not common in dedicated or bespoke networks. Critical services such as industrial automation, feedback control loops that provide real-time automation of processes across transportation, and utility grids may place further demands on network availability and resilience that surpass those experienced in carrier-grade networks. In some scenarios (e.g., manufacturing), a network's security, privacy, safety, availability, and resilience should be flexibly configurable, so that capacity can be traded off in favor of resilience.

In North America, the above uncertainties are further complicated by the absence of self-sufficiency in ICT equipment. Much of the supply chain is sourced globally, raising concerns about the resilience of a nation's communication infrastructure to threats that might be inadvertently or maliciously introduced into the supply chain. The U.S. government has also shown interest in dual-use technologies, where commercial and off-the-shelf technology systems (COTS) can be employed for non-classified use by government and security agencies; such utility can be exploited for significant advantage in cost and flexibility. A parallel concern arises out of more traditional use cases, where networks must remain operational in the event of disasters or emergencies. An example is local survivability of networks in the event of a tornado or hurricane.

The ICT industry should be proactive in meeting these requirements by designing networks to meet these new requirements holistically. There is also the need to ensure that the entire value chain — business processes, technological solutions, and certification of network equipment — follows well-defined compliance and assurance processes. These concerns cannot be solved by the mere protection of markets. Therefore, it is important for the ICT industry to address the problems in a way that allays fear, uncertainty, and doubt from all stakeholders regarding the application of wireless access to automation and critical services.



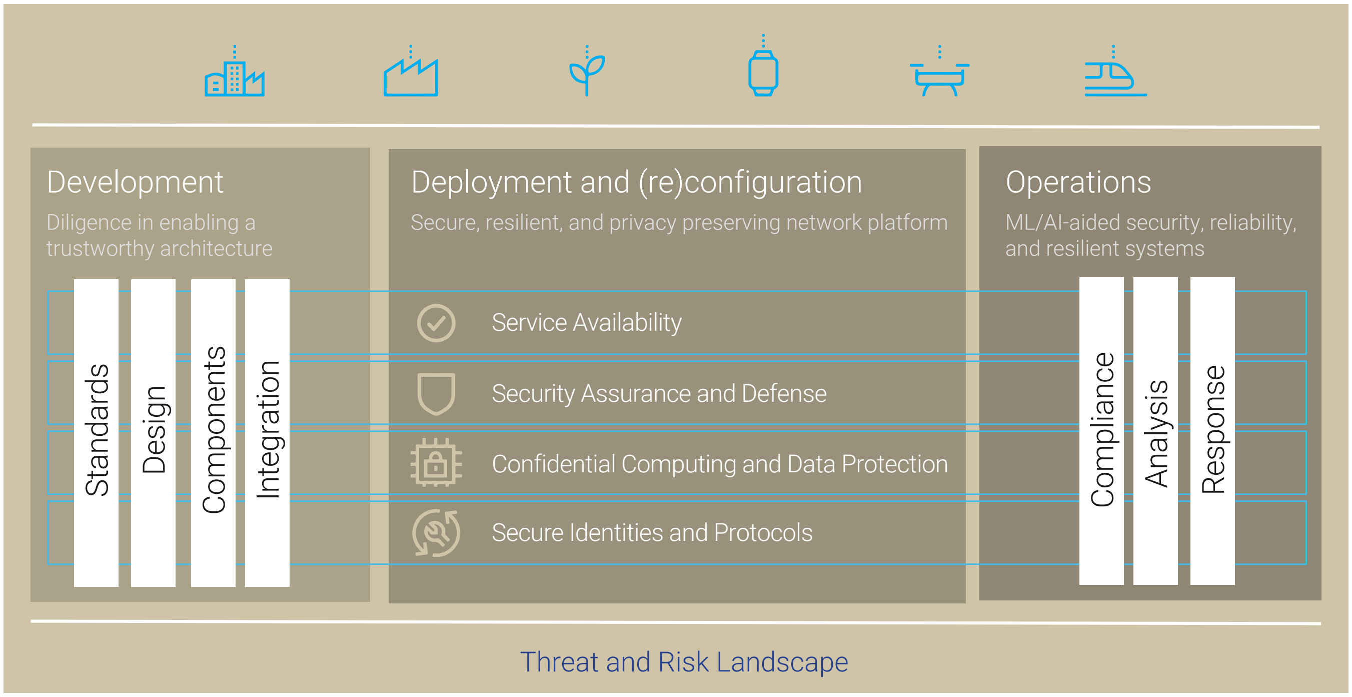

Development
Diligence in enabling a trustworthy architecture
Standards
Design
Components
Integration
Deployment and (re)configuration
Secure, resilient, and privacy preserving network platform
Service Availability
Security Assurance and Defense
Confidential Computing and Data Protection
Secure Identities and Protocols
Operations
ML/AI-aided security, reliability, and resilient systems
Compliance
Analysis
Response
Threat and Risk Landscape

Figure 1: Trustworthy systems for secure, resilient, and privacy-preserving networks.

Figure 1 illustrates the organization of a trustworthy network as a lifecycle that includes a strong assurance of security, privacy, reliability, availability, and functional safety. The entire construct is built on an understanding of the risk and threat landscape that will be addressed by a process that spans development, deployment and management/configuration, and operation of the network or service. The development of the network must exhibit diligence toward trustworthy design through the standardization, design, development, and integration phases. The operational aspects of the trustworthy 6G network will be based on an automated approach to security assurance and defense, and a strong focus on performance management that is customized to the resources available and the use case.

In addition, the network must be resilient to severe disruptions, allowing for predictive analysis and response to threats and disturbances. In what follows, specific research directions toward important objectives are provided as listed in the four focus areas in the figure, adding research on post-quantum cryptographic techniques and quantum computing advances as a separate research priority towards security.

3 RESEARCH AND TECHNOLOGY DIRECTIONS

3.1 Security Assurance and Defense

The security assurance process is used to determine that a system meets its security requirements and is resilient against security vulnerabilities and failures. For critical infrastructure, security assurance activities during product development are complemented by security evaluations performed before a product is deployed. Given the role envisioned for the 6G infrastructure and the new use cases that it will support, security evaluations are expected to become the lynchpin in establishing 6G system trustworthiness.

Security evaluations are done within a security assurance framework that defines a product's security requirements. The testing methodology is developed to determine the confidence level that the system is resilient. Common Criteria (CC) is one of the most common security assurance frameworks used in the computing industry, especially in North America [1]. CC evaluations are performed against a Protection Profile (PP) that describes the functional and assurance requirements that apply to a specific family of devices. Although CC is a generic framework that can be readily tailored to new applications through the development of new protection profiles, specific application domains have chosen to develop other frameworks. One such example is Security Evaluation Standard for IoT Platforms (SESIP), which focuses on IoT devices and claims to be simpler and more agile than CC [2]. Typically, evaluations done under one framework can be mapped under a different framework if done against similar protection profiles.

Data provenance and privacy are important parts of the design and operational considerations for 6G. Section 3.2 addresses one aspect of privacy that relates to the use of strong identities that cannot be exploited by attackers who eavesdrop or act maliciously. The other aspect of privacy is respecting the principles of data ownership by proprietary actors within the network. The widespread use of machine learning (ML) within an AI-native environment suggests that cloud services within network premises should seek to protect proprietary models and data. Joint sensing and communications functions will generate vast amounts of data such as range, environmental mapping, and precise location coordinates for use within many virtual environments; here the authority to use data must be mediated.

In a world where networks are not vertically integrated, and hardware and software functions supporting well-architected interfaces interact within, zero-trust architectures have been suggested as a design requirement. While the realization of a zero-trust network is still awaiting decision, it is recognized that the principles of zero-trust design can be realized now through the use of strong authentication and integrity protection between mutually interacting software and hardware interfaces. Many 5G networks already account for such design principles. Further research into progressing static design towards a dynamic analysis of operational integrity still awaits development.

6G should standardize the security assurance framework and protection profiles under which 6G system nodes should be evaluated. If possible, different 6G system node types can reuse existing frameworks and protection profiles. But when such standards don't exist, the 6G specifications should cover any gaps. In addition, 6G should standardize the mechanisms by which security assurance levels for a product are attested by security labs. This would enable other system nodes to establish its trustworthiness and apply the corresponding policies automatically when interacting with it. One of the key challenges for 6G standardization in this area will be to coordinate with industry consortiums and regulatory bodies worldwide to ensure consistency of the defined standards with existing or forthcoming regulatory requirements.

The NIST cybersecurity framework will be a critical tool in maintaining the security posture of the 6G devices and infrastructure. However, there must be additional attention into extending the security assurance mechanism toward active defense against dynamic threats.

With AI/ML already being used extensively in the field of cyber security defenses, there is little reason to expect the situation to be different for 6G systems. With the NIST Cybersecurity framework as a point of reference, the following observations are offered:

- Most current uses of AI for security functions relate to threat ***detection***, where it is being applied to (e.g., network traffic, end-point detection, API security, and user and entity behavior analysis). Other areas being explored include the monitoring of VM/container behavior, interconnect signaling, and air interfaces.

- For ***prevention***, AI can support authentication controls and help with proactively identifying vulnerabilities or auditing of implementation of policies.

- For ***response***, AI/ML supports threat intelligence collection. Enhancing existing security orchestration, automation, and response solutions with more intelligence is a clear future goal. However, response automation is a challenging goal and will need significant care during application. It is expected that further strides will be made in this direction by the time 6G is deployed.

Even considering the novel use cases for 6G being proposed — such as Internet of Senses, connected intelligent machines, digitalized and programmable world, and connected sustainable world — many of the security threats and required controls map back to well-understood principles as described. Thus, despite a gap in understanding the operational implications of AI/ML use in adversarial situations, academic research in the area is rich and a variety of techniques have been developed that merit closer examination. Additional areas of study include the integration of AI/ML mechanisms in different network functions and the associated need for data and integrity protection for those AI/ML mechanisms against adversarial attacks.

3.2 Confidential Computing

Virtualization and cloud-native realization of network functionality will be prevalent in 6G. Although these approaches are powerful for building network solutions, cloud-based realization creates security challenges around identities used to protect connectivity, network management, privacy protection, and data ownership. These concerns grow immensely when deploying 6G mission-critical network slices. Here, confidential computing can offer the required protection, and, via attestation features, one can realize zero-trust principles. Attestation enables secure orchestration of the identities needed by network functions in a manner that can be technically verified. Confidential computing addresses tenants' concerns about how proprietary and application-specific information can be protected. Confidential computing can also be used for data protection related to third-party functionality, including confidential handling of datasets and model parameters for ML. Lastly, confidential computing gives the tenant and the cloud service provider better control over the types of data extracted through EDR or monitoring tools. The objective is to balance the interests of both parties to monitor performance without handling sensitive information and thereby to leak information.

The versatility of confidential computing hardware technologies can find applications in various security functions. With the expected wide use of AI/ML support for different network functions, it can be highly beneficial to leverage ongoing work on protecting data and model assets through confidential computing. The state of the art has reached a level of performance that overcomes issues such as enclave memory limitations in relation to potentially large data volumes for ML. Also, recent emerging support for hardware accelerators like GPUs allows promising advances toward 6G development.

Hardware-based confidential computing is already being adopted in cloud computing. Other techniques like homomorphic encryption and multi-party computation maturing for practical use cases are also rising in the 6G timeframe, current performance bottlenecks when using these technologies are likely to become less of a hindrance.

3.3 Secure Identities and Protocols

Strong cryptographic identities have been a foundation of mobile networks ever since 2G. Besides the SIM, mobile networks have been using other identities when parts of the mobile system interact with other parts and identities used to secure the management of the mobile networks (e.g., equipment identifiers, cell group identifiers, PLMN identifiers, IP addresses, tunnel endpoints, etc.). The 6G standard will see definition of non-SIM device identities used for mobile network access using modern hardware security features. This is already happening in 5G, and extensions of those solutions will be especially attractive for Standalone Non-Public Networks (SNPNs).

In 6G, most services, particularly the 6G core services, will see heavy use of cloud-native solutions. Tenants utilizing these solutions will spread applications over multi-cloud environments. Each layer of the service and communication domains (e.g., Kubernetes layer, application layer, and 6G network functions) will require identities (often in form of digital certificates) that have to be orchestrated into the system and managed as the system components are dynamically lifecycled. This will require a distributed handling of the highly automated identities, by virtue of the scale and volume of use cases. Automation can thus establish trust among multi-cloud systems. The 6G system will secure the access components and management of edge compute services with secure identities, as well. Mutually trusted permissioned ledgers can provide new ways to automatically handle trust relations and required logging/auditing of cross use between edge computing, roaming functions, and interconnectivity between networks.

Privacy-enhancing technologies and anonymous credentials are also of great relevance to managing identities. Every time a device uses an identity, it exposes some information about the user and their activity. When multiples uses of an identity can be linked together, this can pose a threat to user privacy. Identities should be managed to prevent linkability and must attest only to the property relevant to the service it is used for in order to protect user privacy. With anonymous credentials, the identity of a user or device is not always strictly necessary to attest to the permission to use a service, which mitigates excessive leakage of user information. There is still work to be done in reconciling the transparency required toward service availability with the anonymity benefits of ephemeral identifiers.

Secure identities are essential to privacy and can counteract against information leakage. As a result, significant attention must be given to increasing focus on these identities' security within 6G deployments. Here, greater importance is shown for confidential compute technologies and root-of-trust attestation being put into use as a general approach that secured the orchestration and storage of identities in a verifiable and trustworthy manner.

3.4 Service Availability and Resilience

As wireless technologies are integrated into automation workflows in various societal and industrial use cases, the reliability of components, functions, and processes in the network must account for overall end-to-end performance. The goal here is to reach levels of service availability that can enable confidence in the network as an integral component of an objective to the extent that failure may result in unsafe conditions for the end user, damage to people or property, or inefficiency in business outcomes. The first step toward achieving service availability is to gain situational awareness and to know the numbers. This effectively translates to robust and reliable observability of metrics and using knowledge of the use case, the system performance, and the environmental conditions to manage the utility of network resources across core and RAN. This step includes provisioning and management of distributed computational and storage resources that may be employed in the network slice. Observing the system and knowing the expectations of the quality of experience expected for the service must be integrated into a comprehensive design and operational compliance process.

In 6G, there is an opportunity to borrow concepts that have been proposed for security assurance by developing an assurance methodology for service availability. As in the case of security, the proposed assurance of service availability would seek to achieve resilience in the network to a host of known and unanticipated disturbances based on a characterization of the various anomalies that can impede a service. Security assurance would be subsumed into this grand approach while continuing to achieve the original purpose.

Resilience in this context is the network's ability to meet a diverse set of service objectives and to be able to identify, anticipate, detect, and respond to the evolution of state of the network. This means that the network should be robust but adaptive. There are many opportunities for achieving service availability and resilience. One important research problem here is the elimination of single points of failure. This can be done at a macroscopic level by enabling adequate redundancy in the network – the ability to reconfigure network paths, sites where functions can be deployed, and the ability for computational resources and protocol contexts to be reconfigurable and mobile – which may be important for many use cases. Response to security threats is another opportunity to improve resilience. It is important to address the ability to isolate compromised devices or network infrastructure and react to cyberattacks and information leakage from improperly stored data or exposure of network operational information. Resource allocation is another important aspect of assurance around service availability, especially in situations where a network is operating at a high load with limited resources. This can happen in regions with insufficient coverage or constrained deployment conditions such as rural geographies. Additional factors are the use of multi-RAT connectivity, the use of non-terrestrial networks, and the role of sharing resources with previous generations of 3GPP technologies during the long transition period. Lastly, network users must be confident in the integrity of the assigned resources. Techniques such as secure boot mechanisms, confidential computing, and trustworthy AI are very much a part of achieving those goals.

Modern wireless infrastructure offers multiple options for a transmitter to utilize multiple independent data paths. Examples include simultaneous connections via multiple radio access technologies (multi-RAT), dual/multi-connectivity, multipoint transmission/reception, and carrier aggregation in 5G. Such network infrastructure redundancies could provide an extra degree of freedom to achieve reliable data communication with low latency over the inherently unreliable wireless media. In this context, for 6G, linear coding at the packet level — referred to as linear packet coding, Forward Error Correction (FEC), erasure coding, or network coding in various literature — can be considered a good candidate to efficiently utilize such multipath infrastructure redundancy and supplement link-level channel coding techniques to further enhance reliability with low latency.

3.5 Post-Quantum Cryptographic Techniques for Security and Privacy

Future advances in quantum computing may compromise classical symmetric and public-key cryptographic algorithms by breaking legacy security mechanisms. Quantum computers running Grover's algorithm have been shown to weaken symmetric cryptographic algorithms. The implications are more severe for public-key cryptography. Quantum computers can use Shor's algorithm to break public key cryptographic techniques like Elliptic-Curve Cryptography (ECC) and the Rivest-Shamir-Adleman algorithm (RSA). In the case of public-key cryptography, algorithms for key exchange, asymmetric encryption, and digital signatures will need to be replaced by alternatives.

For symmetric cryptography, such as block ciphers and hash functions, the threat may nominally be diminished with a longer key length. The 6G system will also need to introduce new algorithms as they become available. Thus, the ability to replace the cryptographic protocols partly or completely, and without needing redesign of interfaces to the protocol stack, will be essential to maintaining long-term defenses against advances in the state of the art of quantum algorithms.

For asymmetric cryptographic algorithms, merely increasing key size is insufficient or impractical. Asymmetric cryptography is widely used in 5G systems and internet services (e.g., the Subscription Concealed Identifier (SUCI) scheme, Transport Layer Security (TLS), and the SBA security) that employ asymmetric cryptography are therefore affected. The cryptographic community has been investigating algorithms that rely on different hardness assumptions to resist attacks using quantum computers. The National Institute of Standards and Technology (NIST) has initiated a worldwide process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. The cryptographic community must extensively evaluate any new asymmetric cryptographic primitives introduced into the 6G standard. Security is not the only challenge because these algorithms have significant overheads in one or many areas of efficiency, key size, signature size, and ciphertext size.

Government organizations such as NIST issued a call for key encapsulation, encryption, and digital signature algorithms in 2016 that has gone through three rounds of evaluation in the competition since then. The algorithms being considered include members of the Lattice, Code, and Multivariate families, in addition to NIST-provided alternatives. Most of the proposed algorithms have large key, ciphertext, and signature sizes compared to the classical algorithms and may have implications for both computational complexity and communication overhead.

There is additional promise in the application of post-quantum cryptographic techniques to network coding, in a manner that provides information theoretic security guarantees and computational security in a post-quantum sense for individual links by encrypting only a small part of the information being transmitted. Such techniques can be robust to the attentions of an eavesdropper who has access to all the information on the network. Network coding with integrated post-quantum security has the added advantage of mixing dataflows via trusted and untrusted sub-networks flexibly toward offering end-to-end confidentiality [3].

Quantum technologies have other applications that may be of interest to communication networks. One such application is Quantum Random Number generation, which provides a robust source of entropy. It is an alternative to analog circuits used in conventional silicon processors and is not required to build post-quantum cryptographic solutions. A second application is Quantum Key Distribution (QKD), which provides a way to distribute key material between two endpoints with protection against interception. Such technologies seem to be applicable to fiber or short-range line-of-sight links alone, so their applicability is limited. The use of such technologies will depend on clear understanding of the value of QKD to specific scenarios. It is unlikely that 6G will see immediate interest.

4 PATH TO REALIZATION

The paths to the realization of the technological solutions for trust and resilience will reside with a variety of actors and stakeholders. Standards organizations such as 3GPP and the Internet Engineering Task Force (IETF) will obviously play an important role in the development of access-specific functionality and integration of internet technologies. Government organizations such as NIST are important participants in the standards process and are a valuable resource from North America. A partnership between the National Science Foundation (NSF), industry, and the academic institutions toward realizing a high degree of security, privacy, safety, and resilience from 6G networks is expected. The NSF Resilient & Intelligent NextG Systems (RINGS) program is one example of a significant public-private partnership toward this goal. Lastly, industry action must consider the interaction between 6G and 5G toward reducing the vulnerabilities of 6G due to backward compatibility requirements.

5 CONCLUSION

This document covered five major research topics for consideration toward the enhancement of trust, security, and privacy in 6G:

- Security assurance and defense.
- Confidential computing, including for integration of AI/ML workflows.
- Secure identities and protocols for network integrity and privacy preservation.
- Service availability and resilience.
- Post-quantum cryptographic techniques for security and privacy.

As mentioned earlier, trustworthiness must be an expression of confidence from the ecosystem in which 6G networks are standardized, designed, developed, and deployed. This confidence can be increased by employing strong technological solutions around the research topics identified in Section 3. These solutions are going to be composed from a process of diligence that includes reduction of the risks and threat surfaces in 5G, a strong security assurance and defense approach to products, solutions, and operations, the incorporation of an AI-enabled data-driven dynamic response to security, privacy, safety, service availability, and resilience.

6 REFERENCES

1. Global Platform. “SESIP: An optimized security evaluation methodology, designed for IoT devices”. https://globalplatform.org/sesip/

2. Common Criteria, “The Common Criteria for Information Technology Security Evaluation”. https://www.commoncriteriaportal.org/

3. R. G. L. D’Oliveira, A. Cohen, J. Robinson, T. Stahlbuhk and M. Médard, “Post-Quantum Security for Ultra-Reliable Low-Latency Heterogeneous Networks,” MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM), 2021, pp. 933-938, doi: 10.1109/MILCOM52596.2021.9653013.

COPYRIGHT AND DISCLAIMER

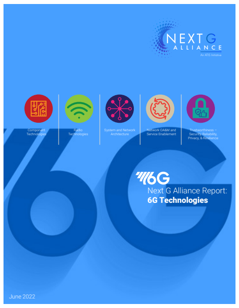
Published July 2022

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

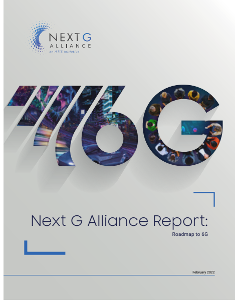
NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NEXT G ALLIANCE REPORTS

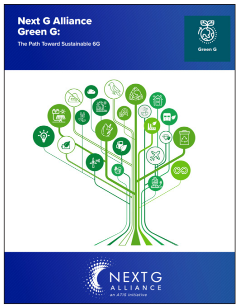


6G Technologies

6G Applications and Use Cases



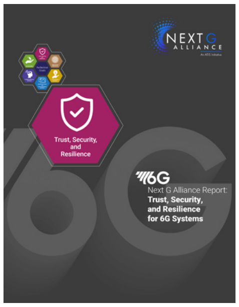
Roadmap to 6G



Green G: The Path Toward Sustainable 6G

NEXT G ALLIANCE
Distributed Cloud and Communications Systems
6G
Next G Alliance Report:
6G Distributed Cloud and Communications System

6G Distributed Cloud and Communications System


NEXT G ALLIANCE
Trust, Security, and Resilience
6G
Next G Alliance Report:
Trust, Security, and Resilience for 6G Systems

Trust, Security, and Resilience for 6G Systems

6G Market Development
A North American Perspective

NEXT G ALLIANCE
An ATIS Initiative

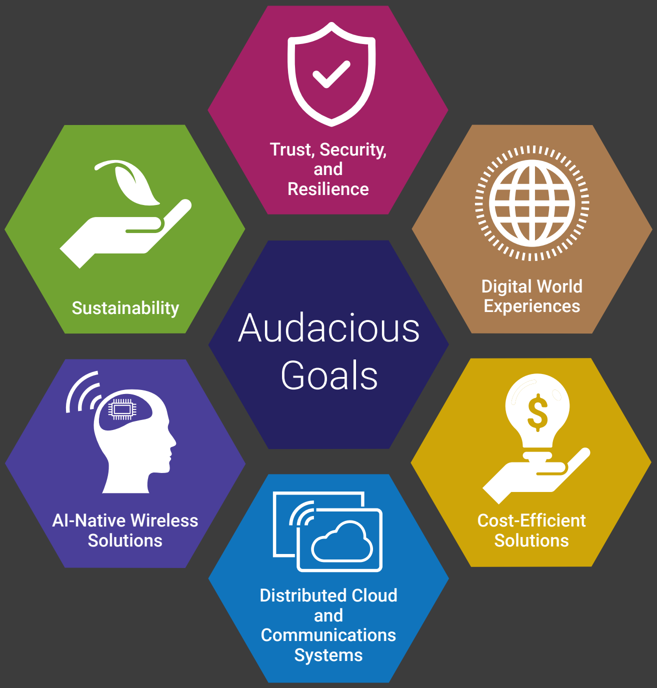
The Next G Alliance (NGA) is a bold new initiative to advance North American mobile technology leadership over the next decade through private sector-led efforts.

With a strong emphasis on technology commercialization, NGA's scope of activities encompasses the full lifecycle of research and development, manufacturing, standardization, and market readiness.

NGA's growing membership reflects support from stakeholders in academia, government, and industry.

This Perspective outlines the strategic importance of 6G and the imperatives that will shape North America's competitiveness, economy, and global leadership.

6G Market Development: A North American Perspective


Trust, Security, and Resilience
Sustainability
Digital World Experiences
Audacious Goals
AI-Native Wireless Solutions
Cost-Efficient Solutions
Distributed Cloud and Communications Systems

Building the foundation for
North American leadership in
6G and beyond.

nextgalliance.org

NEXT G ALLIANCE
An ATIS Initiative