THE FUTURE OF NEXT-GEN NETWORKING AND TRANSPORT TECHNOLOGY

INNOVATIONS DRIVING SECURE, HIGH-SPEED, AND ADAPTIVE CONNECTIVITY

White Paper

5285 Shawnee Road, Suite 400
Alexandria, Virginia 22312
(703) 564-3800
www.mtsi-va.com

Technical Point of Contact
Dr. Marc Kolenko, ScD, MTSI Telecommunications Technical Fellow
for Command, Control & Communications
(703) 638-5977
marc.kolenko@mtsi-va.com

Written: January 2026

AI Usage Disclosure (Optional)

This document was created with assistance from AI tools and has been reviewed and edited by a human. Please note that AI-generated content may contain errors or inaccuracies. Users should exercise caution and conduct their own verification before relying on this information.

CONTENTS

ABBREVIATIONS AND ACRONYMS

Acronym	Definition
AI	Artificial Intelligence
C3	Command, Control & Communications
DDoS	Distributed Denial-of-Service
DWDM	Dense Wavelength Division Multiplexing
ECC	Elliptic Curve Cryptography
IEEE	Institute of Electrical and Electronics Engineer
IoT	Internet of Things
IT	Information Technology
ITU	International Telecommunication Union
LEO	Low Earth Orbit
MEC	Multi-access Edge Computing
ML	Machine Learning
MTSI	Modern Technology Solutions Incorporated
NFV	Network Function Virtualization
QKD	Quantum Key Distribution
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SATCOM	Satellite Communications
SDN	Software-Defined Network

1 EXECUTIVE SUMMARY

Modern Technology Solutions, Inc. (MTSI) is a 100% employee-owned engineering services and technology solutions company headquartered in Alexandria, Virginia. Since its founding in 1993, MTSI has been a trusted partner to the Department of Defense and Federal Agencies, delivering innovative solutions to complex challenges in national defense. Guided by a clear mission and a distinct employee-owner culture—where every team member is empowered to "Own and Solve Our Customer's Problems"—MTSI is committed to addressing mission-critical needs with precision and dedication.

Our expertise spans next-generation networking, seamless program integration, rigorous testing and evaluation, and forward-looking sustainment strategies. By designing adaptable and dependable dependable command, control & communications (C3) solutions, we help our customers achieve immediate objectives while preparing for future challenges. This steadfast commitment to excellence ensures operational readiness and continuity, even in dynamic and unpredictable environments.

As we advance into a new technological era, MTSI is currently at the forefront of assessing quantum encryption and networking, software defined networking, next gen SATCOM and Wireless (e.g., pLEO, vLEO, 6G), edge computing and multi-cloud networking to redefine the standards of secure communications. This transformative approach not only strengthens security but also expands the boundaries of technological possibilities. By emphasizing innovation rooted in practicality, MTSI is dedicated to delivering solutions that are as reliable as they are cutting-edge. Together with our partners, we are unlocking new potentials for ensuring mission success and safeguarding the nation's interests.

2 INTRODUCTION

Why next-gen networking and transport tech matter?

In an era defined by rapid technological evolution, the demand for faster, more secure, and adaptive networking solutions has never been greater. From addressing bandwidth bottlenecks to mitigating cybersecurity threats, next-generation networking and transport technologies are poised to revolutionize how we connect, communicate, and collaborate. This whitepaper explores the cutting-edge advancements shaping the future of connectivity, offering insights into the challenges, opportunities, and transformative potential of these innovations.

3 DESCRIPTION OF THE PROBLEM

Current Challenges in Networking – Bottlenecks in bandwidth, security concerns, and inefficiencies. Networking today faces several critical challenges that hinder its ability to meet the growing demands of modern applications and users:

1. **Bandwidth Bottlenecks**:
    - The exponential growth in data consumption, driven by streaming services, cloud computing, and Internet of Things (IoT) devices, has led to significant strain on existing network infrastructure.
    - Legacy systems struggle to scale effectively, resulting in congestion and reduced performance during peak usage.
2. **Security Concerns**:
    - Cyberattacks are becoming increasingly sophisticated, targeting vulnerabilities in network protocols and infrastructure.
    - The rise of ransomware, phishing, and Distributed Denial-of-Service (DDoS) attacks poses a constant threat to businesses and individuals alike.
    - Ensuring data privacy and protection in a hyper-connected world remains a daunting task.

3. **Inefficiencies in Resource Allocation**:
    - Traditional networking models often lack the flexibility to adapt to dynamic traffic patterns and user demands.
    - Inefficient routing and resource allocation lead to wasted bandwidth and increased operational costs.
4. **Interoperability Issues**:
    - Integrating new technologies with legacy systems is often complex and costly.
    - Compatibility challenges can delay the deployment of innovative solutions and hinder progress.
5. **Environmental Impact**:
    - The energy consumption of data centers and network infrastructure contributes to carbon emissions.
    - Developing sustainable networking solutions is crucial to reducing the environmental footprint of the tech industry.

Scope and Audience – Who should care about these advancements?
The advancements in next-gen networking and transport technology are relevant to a diverse audience, including:

1. **Military and Intelligence Community**:
    - Defense organizations seeking secure and resilient battlefield communications.
    - Intelligence agencies require advanced encryption and secure data sharing for sensitive operations.
2. **Technology Leaders and Innovators**:
    - Professionals driving innovation in networking, telecommunications, and Information Technology (IT) industries.
    - Researchers and developers working on cutting-edge technologies like Artificial Intelligence (AI), quantum computing, and blockchain.
3. **Business Decision-Makers**:
    - Executives and managers are seeking to leverage advanced networking solutions for competitive advantage.
    - Enterprises aim to enhance operational efficiency, security, and scalability.
4. **Policy Makers and Regulators**:
    - Government officials and regulatory bodies shaping the future of technology adoption and standards.
    - Advocates for sustainable and secure networking practices.
5. **End Users and Consumers**:
    - Individuals and organizations rely on high-speed, secure, and reliable connectivity for daily operations.
    - Communities benefit from improved access to digital services and infrastructure.

4 EMERGING TECHNOLOGIES SHAPING NEXT-GEN NETWORKING

4.1 AI-Driven Network Automation

4.1.1 Self-healing networks using Artificial Intelligence / Machine Learning (AI/ML)

Self-healing networks represent a transformative leap in networking technology, leveraging artificial intelligence and machine learning to detect, diagnose, and resolve issues autonomously. By continuously monitoring network performance, these systems can identify anomalies, such as latency spikes or hardware failures, and take corrective actions in real-time without human intervention. This not only minimizes downtime but also enhances overall network reliability and efficiency. For instance, self-

healing mechanisms can reroute traffic around congested nodes or faulty links, ensuring seamless connectivity even during unexpected disruptions. [1]

4.1.2 Predictive analytics for traffic optimization

Predictive analytics harnesses the power of AI to analyze historical and real-time data, enabling networks to anticipate and adapt to traffic patterns proactively. By forecasting demand surges or potential bottlenecks, these systems can allocate resources dynamically, optimizing bandwidth usage and reducing latency. This capability is particularly valuable in scenarios with fluctuating traffic loads, such as live streaming events or e-commerce sales. Moreover, predictive analytics can inform strategic decisions, like preemptively scaling infrastructure or prioritizing critical data flows, to deliver superior user experience.[2]

4.2 Quantum Networking

4.2.1 Quantum key distribution (QKD) for ultra-secure communications

QKD represents a groundbreaking advancement in secure communications, leveraging the principles of quantum mechanics to ensure the confidentiality and integrity of transmitted data. Unlike traditional encryption methods, QKD uses quantum states to encode information, making it virtually immune to interception or tampering. Any attempt to eavesdrop on a quantum channel disrupts the quantum state, alerting the sender and receiver to potential security breaches. This technology is particularly valuable for safeguarding sensitive information in sectors like defense, finance, and healthcare, where data security is paramount.[3]

4.2.2 Potential impacts on encryption and cybersecurity

The advent of quantum networking is poised to revolutionize encryption and cybersecurity by introducing quantum-safe cryptographic methods that can withstand attacks from quantum computers. As quantum computing capabilities advance, traditional encryption algorithms may become vulnerable to decryption, necessitating the adoption of quantum-resistant protocols. Quantum networking also enables the development of ultra-secure communication channels, reducing the risk of cyberattacks and data breaches. Furthermore, the integration of quantum technologies into existing networks can enhance overall security frameworks, paving the way for a more resilient and trustworthy digital ecosystem.[4]

4.3 6G and Beyond: The Next Wireless Evolution

4.3.1 Expected capabilities of 6G networks (terahertz spectrum, ultra-low latency)

The next generation of wireless technology, 6G, is set to revolutionize connectivity by leveraging the terahertz spectrum to deliver unprecedented data speeds and ultra-low latency. With capabilities far surpassing those of 5G, 6G networks will enable seamless communication between devices, supporting applications like holographic telepresence, immersive virtual reality, and advanced IoT ecosystems. The terahertz spectrum offers immense bandwidth potential, allowing for faster data transmission and reduced congestion in densely populated areas. Additionally, 6G networks are designed to minimize latency to

---

[1] Microsoft. (2025). *Configure secure networking for Azure AI platform services*. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/ai/platform/networking

[2] Terrizzano, H., & Boaglio, M. (2024). *Networking best practices for generative AI on AWS*. Amazon Web Services. https://aws.amazon.com/blogs/networking-and-content-delivery/networking-best-practices-for-generative-ai-on-aws/

[3] National Quantum Initiative. (n.d.). *Quantum security*. U.S. government. https://www.quantum.gov/security/

[4] Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), & National Institute of Standards and Technology (NIST). (2023, August 21). *CISA, NSA, and NIST publish factsheet on quantum readiness*. https://www.cisa.gov/news-events/alerts/2023/08/21/cisa-nsa-and-nist-publish-factsheet-quantum-readiness

near-zero levels, ensuring real-time responsiveness for critical applications such as autonomous vehicles and remote surgery.[5]

4.3.2 How AI-native architectures will drive future wireless networks

AI-native architectures are poised to be a cornerstone of 6G networks, enabling intelligent and adaptive network management. By integrating AI at the core of network operations, 6G systems can optimize resource allocation, predict traffic patterns, and enhance security measures. AI-driven algorithms will facilitate dynamic spectrum sharing, ensuring efficient utilization of available bandwidth and reducing interference. Furthermore, AI-native architectures will empower networks to self-configure and self-optimize, adapting to changing user demands and environmental conditions. This level of intelligence will not only improve network performance but also pave the way for innovative applications that require high levels of reliability and precision.[6]

4.4 Satellite and Space-Based Networking

4.4.1 Advances in LEO (Low Earth Orbit – "proliferated" and "very") satellite constellations

Low Earth Orbit (LEO) satellite constellations are transforming global connectivity by providing high-speed internet access to remote and underserved regions. These satellites operate closer to the Earth than traditional geostationary satellites, resulting in reduced latency and improved data transmission rates. Companies like SpaceX and OneWeb are leading the charge in deploying LEO constellations, enabling seamless communication for applications ranging from disaster response to telemedicine. The scalability and flexibility of LEO networks make them ideal for bridging the digital divide and supporting emerging technologies like IoT and autonomous systems.[7]

4.4.2 How space-based networking supports global connectivity

Space-based networking is revolutionizing global connectivity by leveraging satellite technology to overcome geographical barriers. By integrating satellite networks with terrestrial infrastructure, space-based systems can deliver reliable and high-speed internet access to even the most remote locations. This approach is particularly valuable for disaster recovery efforts, where traditional communication networks may be compromised. Additionally, space-based networking supports the deployment of IoT devices and autonomous systems, enabling real-time data exchange and enhancing operational efficiency. As the demand for global connectivity continues to grow, space-based networking will play a pivotal role in shaping the future of communication.[8]

4.5 Edge Computing and Decentralized Networking

4.5.1 Reduced latency through local processing

Edge computing is revolutionizing networking by bringing data processing closer to the source, reducing latency and improving efficiency. By decentralizing data processing, edge computing minimizes the need for data to travel long distances to centralized data centers, resulting in faster response times and reduced bandwidth usage. This approach is particularly valuable for applications like autonomous vehicles, smart

---

[5] Cheng, S. (2023, August 15). *Curving Terahertz Signals Around Obstacles for 6G*. IEEE Spectrum. https://spectrum.ieee.org/6g-network-curved-terahertz-signals

[6] Siddiqui, F. (2021). *5G and beyond: Future trends in wireless networks*. Springer. https://link.springer.com/book/10.1007/978-3-030-72777-2

[7] International Telecommunication Union (ITU). (2025, April). *Space: Connecting earthbound networks by enabling LEO constellations*. https://www.itu.int/hub/2025/04/space-connect-earthbound-networks-enabling-leo-constellations/

[8] Libicki, M. C., & Davis, J. S. (2022). *Securing intellectual property in the era of generative AI: Insights and recommendations*. RAND Corporation.https://www.rand.org/pubs/research_reports/RRA3139-1.html

cities, and IoT devices, where real-time data processing is critical. Edge computing also enhances data security by reducing the exposure of sensitive information to potential cyber threats during transmission.[9]

4.5.2 Integration with IoT and autonomous systems

The integration of edge computing with IoT and autonomous systems is driving innovation across industries. By enabling real-time data processing and decision-making, edge computing supports the deployment of smart devices and autonomous technologies that require high levels of reliability and precision. For example, edge computing allows autonomous vehicles to process sensor data locally, ensuring rapid responses to changing road conditions. Similarly, IoT devices can leverage edge computing to optimize energy usage, monitor environmental conditions, and enhance overall performance. As the adoption of IoT and autonomous systems continues to grow, edge computing will play a crucial role in enabling seamless and efficient operations.[10]

5 Next-Gen Transport Technologies

5.1 Software-Defined Networking (SDN) and Network Function Virtualization (NFV)

How SDN and NFV enable dynamic and scalable network management:

SDN and NFV are revolutionizing network management by decoupling hardware from software, enabling dynamic and scalable operations. SDN provides a centralized control plane that allows network administrators to programmatically manage and optimize network resources. This approach enhances flexibility, reduces operational costs, and simplifies network configuration. NFV complements SDN by virtualizing network functions, such as firewalls and load balancers, on standard hardware, eliminating the need for dedicated appliances. Together, SDN and NFV enable rapid deployment of new services, improve network agility, and support the demands of modern applications.

5.2 Smart Fiber and Optical Networking Enhancements

Innovations in ultra-high-speed optical transport:

Smart fiber and optical networking technologies are pushing the boundaries of data transmission speeds, enabling ultra-high-speed optical transport. Advances in fiber optics, such as Dense Wavelength Division Multiplexing (DWDM) and coherent optical systems, allow for increased bandwidth capacity and improved signal quality over long distances. These innovations are critical for supporting the growing demands of data-intensive applications, including cloud computing, video streaming, and IoT. Additionally, smart fiber technologies incorporate intelligent monitoring and management systems that optimize network performance and ensure reliability.

Security and reliability improvements in fiber optics:

Fiber optic networks are inherently secure due to their resistance to electromagnetic interference and eavesdropping. Recent advancements in encryption protocols and intrusion detection systems further enhance the security of optical networks, making them ideal for transmitting sensitive data. Reliability improvements, such as automated fault detection and self-healing capabilities, ensure uninterrupted connectivity and minimize downtime. These features are particularly valuable for mission-critical applications in sectors like healthcare, finance, and defense.

[9] Exploding Topics. (n.d.). *Top networking trends for 2024*. https://explodingtopics.com/blog/networking-trends
[10] Cisco. (2024). *Global networking trends*. https://www.cisco.com/c/en/us/solutions/enterprise-networks/global-networking-trends.html

6 Security and Resilience in Next-Gen Networks

6.1 Quantum-Safe Cryptography

Developing encryption methods resistant to quantum computing attacks:

Quantum-safe cryptography emerges as a critical solution to address the vulnerabilities posed by quantum computing advancements. Traditional encryption algorithms, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), rely on mathematical problems that quantum computers can potentially solve efficiently, rendering them insecure. Quantum-safe cryptographic methods, such as lattice-based cryptography and hash-based signatures, are designed to withstand attacks from quantum computers, ensuring the confidentiality and integrity of sensitive data. These methods leverage complex mathematical structures that are resistant to quantum decryption techniques, providing a robust defense against future cyber threats. For instance, lattice-based cryptography uses multidimensional grids to encode information, making it computationally infeasible for quantum computers to break. As quantum computing capabilities continue to evolve, the adoption of quantum-safe cryptography will be essential to safeguarding critical systems and data.[11]

7 Industry Adoption and Use Cases

7.1 Enterprise Applications

Enhancing business operations with next-gen networking solutions:

Next-generation networking solutions are transforming enterprise operations by enabling faster, more secure, and scalable connectivity. These advancements empower businesses to optimize their workflows, enhance collaboration, and improve customer experience. For instance, SDN allows enterprises to dynamically manage their network resources, ensuring seamless operations even during peak demand. Additionally, edge computing enables real-time data processing, reducing latency and enhancing decision-making capabilities. By leveraging these technologies, businesses can achieve greater operational efficiency, reduce costs, and gain a competitive edge in their respective industries.[12]

Supporting digital transformation initiatives:

Digital transformation is a key driver for the adoption of next-gen networking solutions. Enterprises are increasingly relying on advanced connectivity to support cloud migration, IoT deployments, and AI-driven analytics. These technologies enable organizations to harness the power of data, automate processes, and deliver innovative services to their customers. For example, 6G networks and AI-native architecture provide the foundation for immersive experiences like virtual reality training and remote collaboration. By embracing next-gen networking, businesses can accelerate their digital transformation journeys and unlock new growth opportunities.[13]

8 Deployment Challenges

8.1 Regulatory and Policy Hurdles

Navigating the complexities of global technology standards:

---

[11] Salem, A.H., Azzam, S.M., Emam, O.E. (2024). *Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Big Data Analytics, 9(1)*. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00957-y; Check Point Research. (2025). *The state of AI in cybersecurity*. https://research.checkpoint.com/2025/sate-of-ai-in-cyber-security/

[12] Google Cloud. (2025). *Networking innovations at Google Cloud Next '25*. https://cloud.google.com/blog/products/networking/networking-innovations-at-google-cloud-next25

[13] Gartner, Inc. (2024, October). *2025 Strategic Roadmap for Enterprise Networking*. https://www.gartner.com/en/documents/5856779

The deployment of next-gen networking technologies is often hindered by a complex web of global technology standards and regulations. These standards, while essential for ensuring interoperability and security, can create significant barriers to innovation and adoption. For instance, differing regulatory requirements across countries can lead to delays in the deployment of new technologies, as companies must navigate a patchwork of compliance obligations. Additionally, the rapid pace of technological advancement often outstrips the ability of regulatory bodies to update and harmonize standards, resulting in uncertainty and inefficiencies.

To address these challenges, stakeholders must engage in collaborative efforts to develop and align global standards that balance innovation with security and interoperability. Organizations like the International Telecommunication Union (ITU) and the Institute of Electrical and Electronics Engineers (IEEE) play a crucial role in facilitating these efforts. By fostering international cooperation and dialogue, these organizations can help create a regulatory environment that supports the seamless integration of next-gen networking technologies.

8.2 Integration with Legacy Systems

Overcoming challenges in adopting new technologies:

Integrating next-gen networking technologies with existing legacy systems presents a significant challenge for organizations. Legacy systems, often built on outdated architecture, may lack the flexibility and scalability required to support modern networking solutions. This incompatibility can result in increased costs and complexity during the transition process, as organizations must invest in custom solutions or extensive system overhauls to bridge the gap.

Moreover, the integration process can disrupt ongoing operations, leading to potential downtime and productivity losses. To mitigate these risks, organizations must adopt a phased approach to integration, prioritizing critical systems and gradually transitioning to next-gen technologies. Leveraging tools like SDN and NFV[14] can also help streamline the integration process by decoupling hardware from software and enabling more flexible and scalable network management.

9 CONCLUSION

Next-generation networking is more than just a technological advancement; it is a transformative enabler for mission success and sustained operational capability in dynamic and contested environments. The innovations detailed in this paper not only enhance efficiency, security, and resiliency but also provide the federal government and its mission partners with a strategic decision advantage during times of uncertainty or conflict. By enabling scalable growth and seamless collaboration, these advancements position MTSI to confidently achieve mission objectives while supporting the nation's evolving needs.

The adoption of emerging technologies, such as SDN, multi-access edge computing (MEC), and advanced cybersecurity measures, represents a significant leap forward in operational agility, communications resiliency, and data-driven decision-making. Realizing the full potential of next-generation networking requires deliberate collaboration across federal agencies, industry leaders, and academia. Through coordinated efforts, stakeholders can accelerate the integration of innovative designs, rigorous testing protocols, and forward-thinking sustainment strategies, ensuring robust solutions that adapt to ever-changing threats and mission demands.

By prioritizing strategic investments and fostering collaboration, the federal government can build secure, adaptable, and resilient digital infrastructure to support seamless mission execution. These investments will not only enhance operational effectiveness but also strengthen the nation's long-term technological

[14] VMware. (n.d.). *VMware vCloud NFV reference architecture v2.0*. https://www.vmware.com/docs/vmware-vcloud-nfv-reference-architecture-v2.0

leadership and security posture, safeguarding future capabilities while empowering dynamic success in an increasingly interconnected world. With next-generation networking technologies forming the foundation for tomorrow's missions, MTSI is committed to supporting federal agencies every step of the way. Together, we can deliver the digital resilience and operational agility critical to protecting national interests and ensuring mission readiness in the face of tomorrow's challenges.

9.1 Future Outlook

9.1.1 Emerging Trends in Networking

Predicting the next wave of innovations in connectivity.[15]

Emerging trends in networking are set to redefine the landscape of connectivity, driven by advancements in technology and evolving user demands. Key trends include:

1. **AI-Driven Network Optimization**:
    - The integration of AI into network management systems is enabling real-time optimization of resources, predictive maintenance, and enhanced security measures.
2. **Quantum Networking**:
    - Quantum technologies are paving the way for ultra-secure communication channels and quantum-resistant encryption methods.
3. **6G and Beyond**:
    - The next generation of wireless technology promises unprecedented data speeds, ultra-low latency, and support for advanced applications like holographic telepresence and immersive virtual reality.
4. **Edge Computing**:
    - Decentralized data processing is reducing latency and improving efficiency, particularly for IoT devices and autonomous systems.
5. **Sustainable Networking Solutions**:
    - The focus on reducing the environmental impact of networking infrastructure is driving innovations in energy-efficient technologies and sustainable practices.

9.1.2 Long-Term Impacts on Society

How next-gen networking will shape the future of communication and collaboration.[16]

The long-term impacts of next-gen networking on society are profound, influencing various aspects of communication, collaboration, and daily life. Key impacts include:

1. **Enhanced Connectivity**:
    - Next-gen networking technologies are bridging the digital divide, providing high-speed internet access to underserved regions and enabling global connectivity.
2. **Improved Collaboration**:
    - Advanced networking solutions are facilitating seamless collaboration across borders, supporting remote work, virtual meetings, and real-time data sharing.
3. **Economic Growth**:

[15] Howarth, Josh. (2024). *5 Top Networking Trends* (2024 & 2025). https://explodingtopics.com/blog/networking-trends

[16] Cisco. (2024). *Global networking trends*. https://www.cisco.com/c/en/us/solutions/enterprise-networks/global-networking-trends.html

- The adoption of next-gen networking technologies is driving economic growth by enabling new business models, enhancing productivity, and creating job opportunities.

4. **Social Inclusion**:
    - Improved access to digital services is empowering communities, fostering social inclusion, and enhancing quality of life.
5. **Technological Innovation**:
    - The evolution of networking technologies is spurring innovation across industries, from healthcare and education to entertainment and transportation.

REFERENCES

Microsoft. (2025). *Configure secure networking for Azure AI platform services*. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/ai/platform/networking

Terrizzano, H., & Boaglio, M. (2024). *Networking best practices for generative AI on AWS*. Amazon Web Services. https://aws.amazon.com/blogs/networking-and-content-delivery/networking-best-practices-for-generative-ai-on-aws/

National Quantum Initiative. (n.d.). *Quantum security. U.S. government*. https://www.quantum.gov/security/

Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), & National Institute of Standards and Technology (NIST). (2023, August 21). *CISA, NSA, and NIST publish factsheet on quantum readiness*. https://www.cisa.gov/news-events/alerts/2023/08/21/cisa-nsa-and-nist-publish-factsheet-quantum-readiness

Cheng, S. (2023, August 15). *Curving Terahertz Signals Around Obstacles for 6G*. IEEE Spectrum. https://spectrum.ieee.org/6g-network-curved-terahertz-signals

Siddiqui, F. (2021). *5G and beyond: Future trends in wireless networks*. Springer. https://link.springer.com/book/10.1007/978-3-030-72777-2

International Telecommunication Union (ITU). (2025, April). *Space: Connecting earthbound networks by enabling LEO constellations*. https://www.itu.int/hub/2025/04/space-connect-earthbound-networks-enabling-leo-constellations/

Libicki, M. C., & Davis, J. S. (2022). *Securing intellectual property in the era of generative AI: Insights and recommendations*. RAND Corporation.https://www.rand.org/pubs/research_reports/RRA3139-1.html

Exploding Topics. (n.d.). *Top networking trends for 2024*. https://explodingtopics.com/blog/networking-trends

Cisco. (2024). *Global networking trends*. https://www.cisco.com/c/en/us/solutions/enterprise-networks/global-networking-trends.html

Salem, A.H., Azzam, S.M., Emam, O.E. (2024). *Advancing cybersecurity: a comprehensive review of AI-driven detection techniques.* Big Data Analytics, 9(1). https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00957-y; Check Point Research. (2025). The state of AI in cybersecurity. https://research.checkpoint.com/2025/sate-of-ai-in-cyber-security/

Google Cloud. (2025). *Networking innovations at Google Cloud Next '25*. https://cloud.google.com/blog/products/networking/networking-innovations-at-google-cloud-next25

Gartner, Inc. (2024, October). *2025 Strategic Roadmap for Enterprise Networking*. https://www.gartner.com/en/documents/5856779

VMware. (n.d.). *VMware vCloud NFV reference architecture v2.0*. https://www.vmware.com/docs/vmware-vcloud-nfv-reference-architecture-v2.0

Howarth, Josh. (2024). *5 Top Networking Trends* (2024 & 2025). https://explodingtopics.com/blog/networking-trends

APPENDIX A: NETWORK DIAGRAMS

1. NETWORK DIAGRAMS

Network diagrams that illustrate assured, resilient, reliable, and obfuscated networks are characterized by high redundancy (mesh/hybrid topologies), multi-layered segmentation (demilitarized zone (DMZ), Zero Trust), and hidden pathways that mask critical infrastructure. These networks utilize techniques such as dynamic IP routing, multi-layered encryption, and virtual obfuscation networks to conceal assets.

Below are conceptual representations and key elements of such network architectures:

1.1. Resilient and Reliable Network Diagram Concepts

A resilient network focuses on redundancy and "bouncing back" from failures.

- **Mesh/Hybrid Topologies:** Devices are connected to multiple other nodes to ensure continuity, as shown in this article about Network Topologies[17].
- **Multi-Availability Zone (AZ) Architecture:** Redundant cloud infrastructure such as in this CloudDefense.AI post[18], replicates data across different geographical locations to ensure high availability.
- **Load Balancing and Redundant Paths:** Traffic is distributed across multiple servers to prevent overload and ensure uptime.
- **Dual-Homing:** Devices connect to two different networks for increased redundancy.

1.2. Assured and Segmented Network Architecture

An "assured" network incorporates security, monitoring, and validation into the architecture, often visualized with segmented zones.

- **Zero Trust Segmentation:** The network is broken into separate subnets or VLANs (departments, functions) to isolate potential issues.
- **Defense-in-Depth (Multi-firewall):** A diagram featuring multiple firewalls (e.g., edge firewalls, DMZ firewalls, internal firewalls) to protect critical data, as shown in this Firewalls article[19].
- **Operational Technology (OT) and SCADA:** Specialized, isolated network segments that are secured away from IT networks to ensure reliability.

1.3. Obfuscated Network Diagrams (Topology Hiding)

Obfuscated networks use techniques to hide the network map from attackers.

- **Virtual Obfuscation Networks:** Critical assets are placed behind hidden servers, accessible only through a "cloak" of virtual, shifting pathways.

---

[17] O net. (2018). *Network Topologies: Star, Mesh and Hybrid*. https://www.ad-net.com.tw/network-topologies-star-mesh-hybrid/#:~:text=A%20mesh%20topology%20has%20connections,would%20have%20a%20hybrid%20topology

[18] CloudDefense.AI. (n.d.). *Multi-az Deployment in AWS*. https://www.clouddefense.ai/glossary/aws/multi-az-deployment

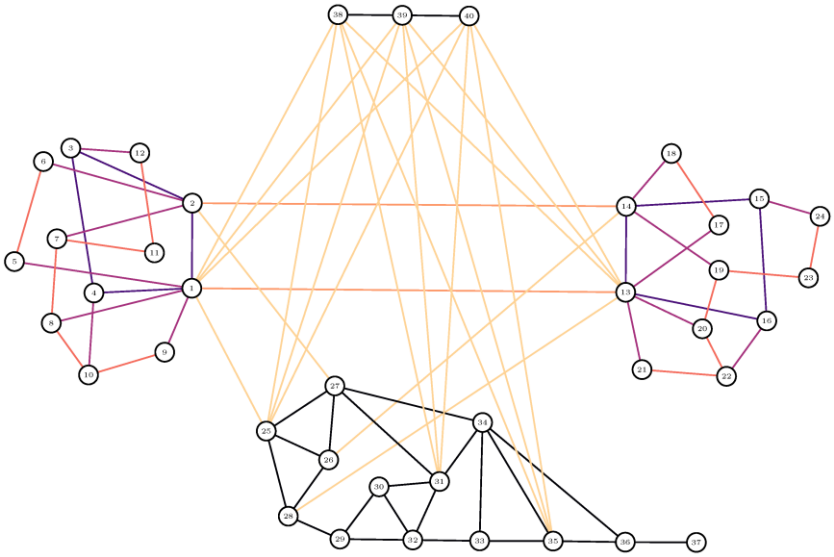
[19] OMSCS. (n.d.). *Firewalls*. https://www.omscs-notes.com/information-security/firewalls/

- **Dynamic IP Routing and Varying Pathways:** The diagram shows traffic taking non-linear or randomized routes to prevent traffic mapping.
- **Honeypots and Decoys:** Anomaly detection systems and honeypots are included in the DMZ to lure and detect intruders, this CrowdStrike[20] article describes how they work and the different types. Umang software provides visualization[21] of these anomaly detection systems.
- **Tunneling/Overlay Networks:** The use of tunnels (e.g., VPNs, overlay networks) to hide the underlying physical structure of the network.

1.3.1. Key Components to Look For:

- **Nodes:** Firewalls (FW), Intrusion Detection Systems (IDS), VPN Concentrators, Load Balancers.
- **Layers:** Internet→Edge Router→DMZ (Public Services)→Internal Firewall→Internal Network. Example[22]: https://study-ccna.com/firewalls-ids-ips-explanation-comparison/ .
- **Flows:** Redundant, encrypted paths (represented by arrows connecting to multiple points).

These architectures ensure that even if one node is compromised or fails, the overall network remains secure, functional, and hidden from unauthorized inspection.



The figure above is the structure of an exemplary multilayer communication system. The two access networks on the left and right have similar topological structures although their geographical formation may be different. A backbone network is depicted in the lower part of the figure, and a satellite system is in the upper part of the figure.

[20] CrowdStrike. (2025). *Honeypots in Cybersecurity Explained*. https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/#:~:text=A%20honeypot%20is%20a%20cybersecurity,architecture%2C%20information%20and%20network%20security

[21] Umang software. (n.d.). *Honeypot_2*. https://www.umangsoftware.com/wp-content/uploads/images/honeypot_2.png

[22] CCNA. (n.d.). *Firewalls, IDS, and IPS Explanation and Comparison*. https://study-ccna.com/firewalls-ids-ips-explanation-comparison/