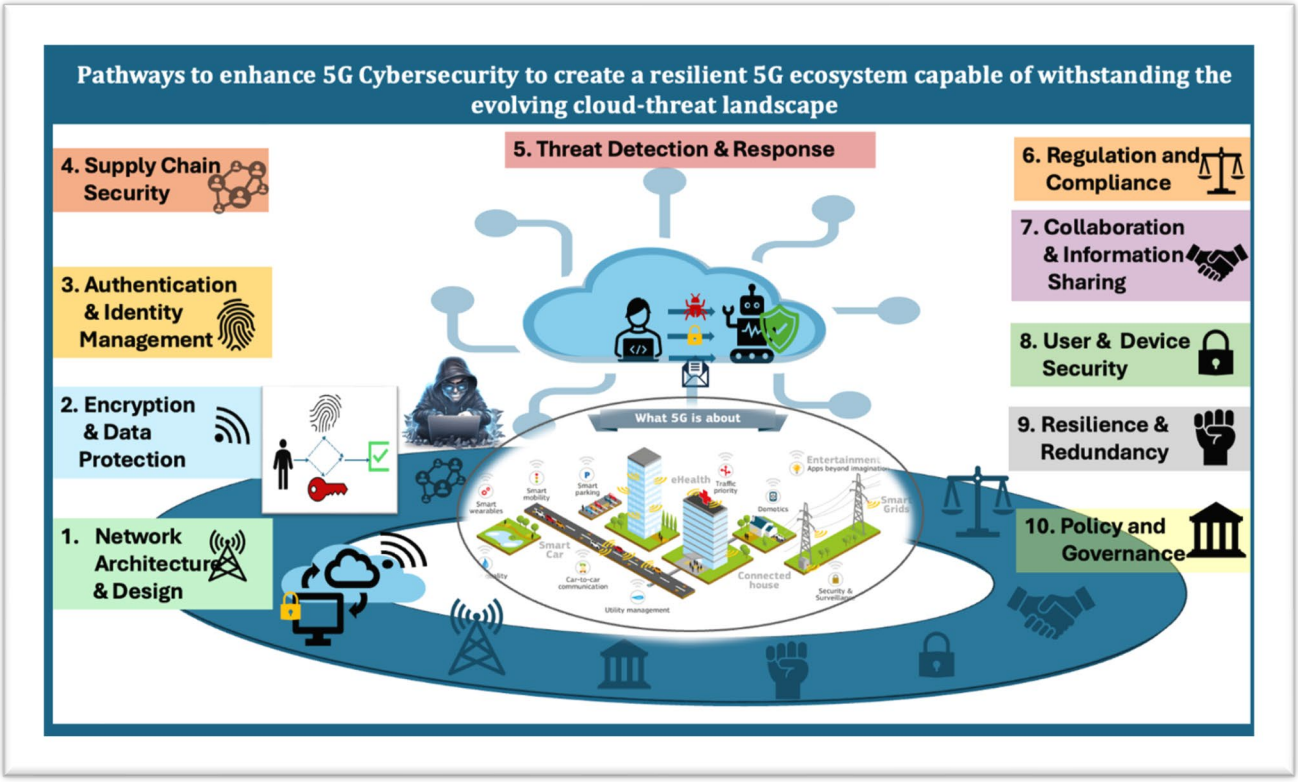
2024
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Phase II:
5G & CLOUD-BASED CYBERSECURITY



TEAM INTRODUCTIONS

MEMBERS	COMPANY
Thomas G.	Private Sector
Jack L.	Private Sector
Deelip Mhaske	State of New Jersey
Chandra Pauline Daniel* (March 18, 1974 - July 15, 2024)	USA-UNFPA
Champion	*Champion Agency*
Eric R.	DHS
Stephen M.	USG

*Our team is deeply saddened by the loss of Dr. Chandra Pauline Daniel, a shining example of team spirit, who passed away on July 15, 2024. Pauline dedicated countless hours to the AEP program, and her presence will be greatly missed.

I. INTRODUCTION

The introduction of 5G technology is a game-changer in telecommunications, shifting the industry toward an architecture that resembles modern cloud IT systems rather than the traditional cellular networks we've known for decades. To fully grasp the implications of 5G, it's essential to look at it from two key angles:

- **Telecommunications Standards:** This includes the frameworks and protocols set by organizations like the Third Generation Partnership Project (3GPP).

- **Implementation of 5G:** How 5G networks are practically deployed and integrated into existing and new infrastructures.

The 5G Telecommunications Standards

The standardization of 5G technology is driven by several key international bodies, most notably the Third Generation Partnership Project (3GPP). 3GPP is a collaborative effort that unites seven major telecommunications standard development organizations: Association of Radio Industries and Businesses (ARIB -Japan),Alliance for Telecommunications Industry Solutions (ATIS - USA),China Communications Standards Association (CCSA - China), European Telecommunications Standards Institute (ETSI - Europe),Telecommunications Standards Development Society, India (TSDSI - India), Telecommunications Technology Association (TTA - Korea), Telecommunication Technology Committee (TTC - Japan). These organizations, known as "Organizational Partners," work together to create the Reports and Specifications that define 3GPP technologies, which include cellular telecommunications technologies covering radio access, core networks, and service capabilities. This comprehensive framework provides a complete system description for mobile telecommunications.

One of the most significant aspects of 5G is its adoption of a Service-Based Architecture (SBA). Unlike previous generations, which relied on traditional network elements, 5G uses a set of modular Network Functions (NFs). Each Network Function offers a specific service to other NFs within the network and operates in a stateless manner, meaning it does not retain data between requests. This architecture provides immense flexibility, allowing network operators to build and configure the network in a way that best meets their

needs, facilitating easier updates, scaling, and integration of new services.[1]

The Implementation of 5G

Because it operates within a cloud environment, effectively running as Software as a Service (SaaS), this has given rise to the concept of Telco as a Service (TaaS), where telecommunications services are delivered through cloud-based infrastructure. In this model, applications run in data centers but are connected to and authenticated by the 5G network services, allowing for seamless integration and management. These networks can be implemented in three primary configurations:

- **Public Land Mobile Network**: A public as opposed to private network that is offered by a service provider in a specific country.
- **Stand-Alone Non-Public Network (SNPN):** Fully independent networks managed by the private entity, without reliance on a Public Land Mobile Network (PLMN). Non-Public Networks are sometimes called Private Networks.
- **Public Network Integrated NPN (PNI-NPN):** Non-public networks that leverage the support and infrastructure of a PLMN. Certain network functions are managed independently by the NPN operator while utilizing PLMN infrastructure for other aspects. This hybrid model strikes a balance between the benefits of public and private networks.

The different configurations of 5G offer unparalleled flexibility in how these networks can be deployed to meet the unique needs of private entities. This flexibility is a key advantage of 5G, but the rise of Private 5G, goes even further in transforming industries. These networks are poised to drive substantial economic growth and innovation across various sectors. While private (NPN) networks were technically feasible in earlier generations of cellular technology (2G-4G), they often fell short due to the rigid architectures of those systems. In contrast, 5G's Service-Based Architecture (SBA) provides enterprises and industry providers with the ability to design highly customized solutions tailored to their specific needs, marking a significant leap forward in network capability and adaptability.

The potential applications of 5G Non-Public Networks (NPNs) are extensive, offering transformative possibilities across a wide range of industries. In manufacturing and factory automation, 5G NPNs enable highly efficient and

[1] 5G networks can be highly dynamic and responsive in real time to use demands. This dynamism can be driven by services such as kubernetes that do not require human action to change network components and connections. Instead the network adjusts to find an optimal solution to a desired end state defined by predetermined metrics and characteristics. .

precise operations, while in food and beverage distribution, they streamline logistics and ensure better quality control. Transportation systems, including rail networks, can benefit from enhanced connectivity and real-time data management. In the pharmaceutical sector, NPNs support secure and efficient management of production and supply chains.

For industries dealing with heavy machinery and industrial control, 5G NPNs provide robust and reliable communication networks that can handle the demands of large-scale operations. In energy and utility management, particularly power grids, these networks facilitate more responsive and efficient management of resources. The logistics and warehouse management sectors can leverage NPNs for improved tracking and inventory management.

In defense and military applications, 5G NPNs offer secure and controlled communication channels critical for national security. Academic campuses and research institutions can use these networks to support cutting-edge research and enhance campus connectivity. The mining industry benefits from NPNs by enabling remote monitoring and automation of mining operations.

Healthcare facilities and hospital systems will be reliant on 5G NPNs for secure and fast data transmission, vital for telemedicine and patient care. The oil and gas industry can use these networks for more effective monitoring and management of remote operations. In media distribution, NPNs ensure high-quality and reliable content delivery.

Retail industry applications are transformed by 5G NPNs through enhanced customer experiences and more efficient operations. Agricultural systems benefit from smart farming techniques enabled by these networks. Finally, smart city initiatives are powered by 5G NPNs, supporting everything from traffic management to public safety and urban planning.

Building on these diverse applications, this paper specifically explores the positive implications of 5G in healthcare and power grid management, focusing on how advancements in efficiency, connectivity, and service delivery can revolutionize these critical areas.

II. HARNESSING 5G TECHNOLOGY IN HEALTHCARE

The transformative potential of 5G technology in healthcare, particularly in telemedicine, telesurgery, and the Internet of Medical Things (IoMT), is widely recognized across recent studies. These advancements are largely attributed to 5G's high-speed connectivity, low latency, and enhanced bandwidth, which are crucial for supporting real-time healthcare services and applications.

Telemedicine and Telesurgery:

5G is set to revolutionize telemedicine by enabling real-time remote healthcare services that were previously limited by slower, less reliable networks. Studies by Kalra et al. (2020) emphasize the importance of 5G's low latency and high-speed connectivity in facilitating telemedicine and the integration of augmented reality (AR) and virtual reality (VR) into patient care. Similarly, Berlet et al. (2022) showcase the application of 5G in emergency telemedicine, such as mobile ultrasound, where low latency and high throughput are essential for accurate preclinical diagnostics. The feasibility of 5G-enabled robotic telesurgery has also been demonstrated, with studies like those by Acemoglu et al. (2020) and Moustris et al. (2023) highlighting successful remote surgeries that benefited from minimal latency and high-definition video transmission. These studies collectively illustrate how 5G can elevate telemedicine and telesurgery to new levels, enabling more effective and timely medical interventions.

Internet of Medical Things (IoMT):

The integration of 5G with IoMT is another area where significant advancements are anticipated. 5G's ability to provide massive connectivity, with a high-speed, low-latency quality of service is crucial for the continuous health monitoring and data collection required by IoMT devices. Research by Preetham et al. (2023) proposes a layered architectural framework to secure 5G-enabled IoMT systems, addressing the vulnerabilities inherent in these technologies. Meanwhile, studies like those by Mathkor et al. (2024) and Razdan and Menon (2021) explore how IoMT, supported by 5G, can revolutionize personalized healthcare management, allowing for continuous health monitoring and more tailored treatment plans. The integration of machine learning with IoMT, as discussed by Pradyumna et al. (2024), further highlights the potential of these technologies to enhance healthcare delivery, although challenges related to security, interoperability, and data privacy remain critical areas for future research.

Network Slicing for Healthcare[2]

The integration of 5G technology into healthcare, through network slicing, is one example of a 5G Non-Public Network that offers a groundbreaking approach to improving the efficiency, reliability, and customization of medical services. Network slicing enables the creation of virtual networks that are specifically tailored to meet the unique needs of various healthcare applications, ensuring that diverse Quality of Service (QoS) requirements are met and that resources are utilized optimally.

Digital twins are rapidly emerging as a transformative technology in healthcare, offering the ability to create precise, real-time digital replicas of physical entities such as patients, organs, or even entire healthcare systems. This technology enables healthcare professionals to simulate, predict, and optimize treatments with unprecedented accuracy, potentially leading to more personalized and effective care. The deployment of 5G is a significant enabler for digital twins, providing the necessary speed, bandwidth, and low latency to handle the massive amounts of data required for real-time updates and analyses. With 5G, healthcare organizations can harness the full potential of digital twins, leading to more innovative and efficient healthcare solutions

Customization and Efficiency:

One of the primary benefits of network slicing in healthcare is its ability to create dedicated virtual networks that can be customized for specific applications. For instance, Pal et al. (2023) discuss how 5G architecture, combined with network slicing, allows for the creation of virtual networks that meet strict requirements for bandwidth allocation, prioritization, and enhanced privacy—critical for healthcare environments. This customization ensures that different healthcare applications, from telemedicine to remote surgery, receive the specific network resources they need to function effectively.

Performance and Scalability:

The performance improvements facilitated by network slicing are particularly noteworthy. Tian et al. (2023) demonstrated that by using a two-sided matching theory-based virtual network embedding (MT-

[2] **Network slicing** is a key feature in 5G technology that allows a single physical network to be divided into multiple virtual networks, each tailored to meet specific requirements. This capability is crucial because 5G is designed to support a wide range of applications, from consumer mobile services to industrial IoT and mission-critical communications, each with different performance and security needs.

VNE) solution, healthcare networks could significantly enhance their efficiency and responsiveness. This approach allows the network to accept more healthcare services while making the best use of physical network resources. Similarly, De Silva et al. (2022) explored both vertical and horizontal slicing approaches, showing how these strategies can optimize performance in smart healthcare scenarios, ensuring that critical applications receive the necessary support even as demand fluctuates.

Data Security and Privacy:

In addition to enhancing performance, the implementation of a 5G Non-Public Network through network slicing also addresses key concerns related to data security and privacy. Kapassa et al. (2019) highlighted an innovative eHealth system that leverages isolated 5G network slices to enhance data security and increase patient health awareness. This approach ensures that sensitive medical data is handled with the highest levels of security, minimizing the risk of breaches. Furthermore, Basu et al. (2021) introduced a programmable slicing approach that not only optimizes resource provisioning but also simplifies the processing of medical data, making it easier to manage while maintaining strict privacy controls.

III. HARNESSING 5G TECHNOLOGY IN POWER GRIDS

The global deployment of 5G technology is profoundly transforming various industries, catalyzing growth, innovation, and economic evolution. One sector experiencing substantial impact is the power grid, where improved energy demand management facilitated by 5G can lead to decreased investment requirements. Integrating 5G into smart grids enhances energy load balancing, mitigates electricity peak demands, and generates cost savings.

The implementation of 5G technology offers significant advancements in grid management through several pivotal enhancements. The low latency characteristic of 5G enables instantaneous data transmission, crucial for real-time grid monitoring and control. This capability ensures swift identification and resolution of issues, thereby enhancing reliability and minimizing downtime (Porcu et al.). Additionally, 5G facilitates the incorporation of IoT devices within smart grids, supporting advanced metering infrastructure, automated demand response, and the management of decentralized energy resources (Porcu et al.). The high data transfer rates of 5G also play a vital role in precise energy management by optimizing energy distribution, reducing waste, and improving the forecasting and integration of renewable energy sources, thus boosting overall grid efficiency (Porcu et al.).

These collective advancements contribute to the development of a more resilient, efficient, and sustainable energy grid.

IV. SECURITY CONCERNS

- **Healthcare** The integration of 5G technology and the Internet of Medical Things (IoMT) into healthcare has brought significant advancements, but it also introduces a host of cybersecurity risks and concerns that must be carefully considered. As healthcare systems become increasingly connected, they are exposed to a broader range of cyber threats that can compromise patient data, disrupt critical medical services, and undermine the overall security of healthcare infrastructures.

  One of the primary concerns is the expanded attack surface that the multi technology 5G echo-system introduces. This is exacerbated by the more widespread deployment of 5G and IoMT devices. This multi technology which increases connectivity between medical devices, healthcare networks, and cloud-based systems, creates more entry points for potential cyberattacks. This heightened vulnerability poses a serious risk to the integrity and confidentiality of sensitive medical data. A breach could not only lead to the unauthorized access of patient information, but also disrupt the functioning of vital medical devices, potentially putting patient lives at risk.
  Moreover, the development of the 5G system involves a number of different technologies that are developed by different vendors. These vendors have not always prioritized security over functionality when performing interoperability and integration testing. This could potentially result in critical vulnerabilities within healthcare systems. As noted by Khan et al. (2020), this focus has left gaps in the security frameworks of 5G technologies, making them susceptible to a range of cyber threats. The integration of IoT devices within 5G networks further exacerbates these vulnerabilities, as these devices are often not designed with robust security in mind. Sicari et al. (2020) highlights the particular challenges associated with securing IoT devices, which are frequently targeted by cybercriminals due to their relatively weak security protocols.

  Another significant concern is the potential erosion of patient trust. As Coventry and Branley (2018) point out, the increased connectivity in healthcare systems exposes medical devices to cybersecurity risks that can destabilize health systems and reduce public confidence. Patients rely on the secure handling of their personal health information and the safe operation of medical devices. Any breach or disruption in these areas could have far-reaching consequences, not only for individual patients but also for the broader healthcare system.

  The financial implications of addressing these cybersecurity risks are considerable. Protecting healthcare systems from the vulnerabilities

introduced by the multiple technology aspect of 5G and IoMT integration, requires substantial investment in advanced security measures, and the introduction of very tight and controlled Development, Security, and Operations (DevSecOps) processes throughout the IT lifecycle.

The integration of 5G and IoMT into healthcare offers significant benefits, it also brings with it a range of cybersecurity risks and concerns that cannot be ignored. The expanded attack surface, the erosion of patient trust, and the financial and technological burden of implementing robust security measures, all pose serious challenges to the healthcare sector as it embraces this new technology.

- **Power Grid** The deployment of 5G technology within power grids introduces several new security challenges and vulnerabilities, particularly in the context of power grid management.

  Expanded Attack Surface

  The integration of 5G technology into power grids significantly increases the number of connected devices and communication pathways. This along with the complex and multi technology aspect of the 5G system can lead to areas between previously stovepiped technologies that are vulnerable to exploitation due to a failure to prioritize security during the inter vendor integration and interoperability testing. In addition to the security implications between diverse technologies, the proliferation of IoT devices within smart grids has been identified as a significant risk factor. According to NIST Special Publication 800-82 Revision 3, the addition of numerous IoT devices can create more entry points for cyberattacks, especially if these devices lack adequate security measures (Ahmad et al., 2019).

  Denial of Service (DoS) Attacks

  The incorporation of IoT devices within the 5G ecosystem, particularly in power grids, increases the potential severity and ease of cyberattacks. Unlike the 4G LTE ecosystem, which has a limited number of non-mobile operating systems, 5G will support a wide range of devices, including cameras and other devices that often run outdated versions of Linux with embedded web servers. This increases the risk of attacks similar to the Marai botnet, which could exploit these vulnerabilities in the 5G domain (Fonyi).

Supply Chain Risks

Supply chain vulnerabilities pose a significant risk to the security of 5G-enabled power grids. These risks include the potential for compromised vendors and service providers to introduce hidden hardware, malicious software, and other vulnerabilities into the network. Other concerns involve uncontrolled software updates, functionality manipulations, audit bypass mechanisms, backdoors, and leftover testing features in production versions. Additionally, third-party personnel involved in the Development, Security, and Operations (DevSecOps) lifecycle pose a risk if they engage in unauthorized interactions.

Data Privacy and Integrity

The expansion of the attack surface in 5G networks significantly heightens the risk of unauthorized access, raising substantial concerns about data privacy and integrity. As 5G technology enables the connection of an unprecedented number of devices and supports advanced applications, the potential entry points for cyberattacks multiply.

V. STRATEGIES FOR SECURING 5G APPLICATIONS

The deployment of 5G networks in critical sectors such as power grids and healthcare present immense opportunities but also significant security challenges. To safeguard these sectors, it is crucial to implement a set of globally accepted strategies that address the unique risks posed by the integration of advanced technologies like IoT, cloud computing, and AI. These strategies are in line with recommendations from leading international organizations, including the International Telecommunication Union (ITU), the National Institute of Standards and Technology (NIST), the European Union Agency for Cybersecurity (ENISA), and others.

Robust Network Architecture: A key strategy endorsed by global cybersecurity frameworks is the development of a robust network architecture. This includes the use of network segmentation to isolate critical components, reducing the impact of potential breaches. Redundancy is another critical element, ensuring that backup systems are in place to maintain operations in the event of an attack or failure. Secure communication protocols, including encryption and secure tunneling, are essential to protect data integrity and confidentiality as it traverses the network. These practices align with NIST's guidelines and ENISA's recommendations for critical Infrastructure protection.

Non-Public Networks (NPNs): The implementation of Non-Public Networks (NPNs) is widely recognized as a key strategy for enhancing the security of 5G deployments in sensitive sectors. NPNs provide organizations with greater control over their network infrastructure, reducing the risk of unauthorized access. In the context of power grids, NPNs allow utilities to manage their own networks, safeguarding operational data and ensuring that critical functions are protected from external threats. Similarly, in healthcare, NPNs are vital for protecting sensitive patient data and ensuring the reliability of medical devices. The use of private networks that can include but not limited to network slicing, as recommended by the ITU, allows for tailored performance criteria that meet the specific needs of these sectors.

Access Control Measures: Implementing stringent DevSecOps[3] and access control measures is critical for securing 5G networks in both power grids and

[3] **DevSecOps** is an extension of DevOps that integrates security practices into the continuous integration, continuous delivery (CI/CD), and operational processes. In the context of **5G networks**, DevSecOps ensures that security is a fundamental component throughout the development, deployment, and operation of 5G infrastructure and services.

healthcare. Global standards advocate for the use of Role-Based Access Control (RBAC), which ensures that only authorized personnel can access sensitive systems. Multi-Factor Authentication (MFA) is recommended to add an additional layer of security by requiring multiple forms of verification. The adoption of Zero Trust Architecture, which assumes that threats could originate from within the network, is increasingly being endorsed by leading cybersecurity organizations as a best practice to continuously verify user and device credentials.

Vulnerability Management: Effective vulnerability management is a cornerstone of global cybersecurity strategies. Regular vulnerability scans and assessments are essential to identify and mitigate potential security risks. International guidelines from organizations like NIST and ENISA recommend the prioritization of vulnerabilities based on their severity and the implementation of continuous integration and Continuous Deployment (CI/CD) practices processes to ensure that security updates are promptly applied. This proactive approach helps reduce the likelihood of exploitation by cyber attackers.

Incident Response Preparation: Preparing for potential security incidents is a critical aspect of securing 5G networks in both power grids and healthcare. The development of detailed incident response plans, as recommended by global cybersecurity standards, is essential for ensuring a swift and effective response to cyber threats. Conducting regular tabletop exercises, as advocated by NIST and other organizations, allows teams to practice their response strategies in a controlled environment and refine their plans based on the outcomes. Continuous improvement of these plans, informed by real-world incidents and evolving threats, is necessary to maintain readiness.

Securing the Supply Chain: Securing the Supply Chain particularly the software supply chain for third party applications. The use of third-party applications that can directly communicate with the 5G ecosystem and its associated devices will be extensively used in 5G. This represents a significant security vulnerability. Global cybersecurity frameworks emphasize the importance of securing the supply chain to prevent vulnerabilities from being introduced through third-party components. Rigorous vetting of suppliers, continuous monitoring for supply chain risks, and ensuring compliance with security standards throughout the supply chain are critical steps in mitigating these risks. Organizations like ENISA and the ITU highlight the need for robust supply chain security measures to protect the integrity of critical infrastructure components.

Data Privacy and Integrity: The expansion of 5G networks and the associated third party applications, particularly in sectors dealing with sensitive data like healthcare and power grids, significantly increases concerns about data privacy and integrity. Globally accepted strategies include the implementation of strong encryption protocols, both for data in transit and at rest, to protect against unauthorized access. The ITU and other organizations also advocate for stringent access controls and continuous monitoring to detect and respond to potential breaches, ensuring the confidentiality and integrity of critical data.

Regular Security Audits: Conducting regular security audits is a globally accepted practice for maintaining the security and resilience of 5G networks and the cloud environment that this Software as a Service (SaaS) runs on. These audits should include compliance checks to ensure adherence to international standards and regulations, penetration testing to identify vulnerabilities, and continuous monitoring to detect emerging threats with solid configuration management best practices. The recommendations from global organizations like NIST and ENISA emphasize the importance of these audits in identifying and rectifying security gaps, thereby strengthening the overall security posture of 5G networks.

This comprehensive approach aligns with international standards and best practices, providing a robust framework for protecting the integrity, confidentiality, and availability of critical services in these vital sectors.

VI. KEY FINDINGS

The deployment of 5G technology, which functions as Software as a Service (SaaS) within a cloud-based environment, has created a complex and multifaceted communications ecosystem. This ecosystem relies heavily on the seamless interoperability of various advanced technologies, including Artificial Intelligence (AI) and the Internet of Medical Things (IoMT). However, this very interoperability introduces significant security vulnerabilities that present substantial challenges for both the private sector and government agencies.

One of the most pressing concerns is the lack of a standardized process for conducting comprehensive interoperability security testing across these diverse technologies. Many of these technologies, such as AI, are still in their emerging stages, making it difficult to fully anticipate and mitigate potential security risks. The inherent insecurities within the cloud infrastructure that supports 5G further exacerbate these vulnerabilities, creating a significant national security concern across the entire 5G cloud ecosystem.

This issue is particularly critical in sectors like healthcare and power grids, where the integration of 5G offers transformative capabilities but also heightens the risk of cyber threats. In healthcare, 5G enables significant advancements in telemedicine, remote monitoring, and IoMT, but it also exposes sensitive patient data and critical medical systems to potential breaches. Similarly, in power grids, 5G enhances grid management, real-time responsiveness, and operational efficiency, but it increases the risk of disruptions that could have far-reaching consequences for national energy infrastructure.

To address these challenges, 5G Non-Public Networks (NPNs) present a viable solution by allowing specific verticals, such as healthcare facilities and power grid operators, to take full ownership and control of their networks. This control extends to determining who has access to the network and managing critical operations and maintenance, including updates through continuous integration and deployment (CI/CD) processes. Furthermore, NPNs offer the flexibility of a hybrid approach, where less sensitive or critical components of the network can be shared with a public network, while maintaining tighter control over the more sensitive segments.

This tailored approach to network security allows healthcare and power grid operators to implement security measures that are specifically designed to meet the unique needs of their sectors. By doing so, it significantly enhances the resilience and security of these critical infrastructure sectors in the context of 5G and cloud integration. These findings underscore the importance of developing robust, sector-specific security strategies to protect against the evolving threats posed by the widespread adoption of 5G technology.

VII. IMPACT TO GOVERNMENT AND PRIVATE SECTOR

The integration of 5G technology, particularly within a cloud-native environment, introduces significant security challenges that have yet to be fully addressed. As 5G becomes more deeply embedded in critical infrastructure like healthcare and power grids, the risks associated with cyber threats grow exponentially. The shift to a cloud-based model reshapes the security landscape, bringing new vulnerabilities that demand immediate and sustained attention. This is especially critical as healthcare systems increasingly rely on 5G for telemedicine, remote monitoring, and data-intensive applications, while power grids use 5G to enhance grid management, efficiency, and real-time responsiveness.

For government agencies, the stakes are incredibly high. With 5G set to play a pivotal role in sectors such as healthcare and energy, ensuring the security of these systems is a matter of national importance. The ability to protect against cyberattacks that could disrupt essential services—like patient care or power supply—is crucial. In healthcare, a breach could lead to compromised patient data or disruptions in critical medical services, while in the energy sector, a successful attack on a power grid could result in widespread outages and economic fallout. This scenario demands not only robust cybersecurity measures but also a strategic approach to managing the risks associated with a more interconnected, cloud-dependent world.

In the private sector, the emergence of 5G Non-Public Networks (NPNs) offers both opportunities and significant responsibilities. NPNs give industries greater control over their network infrastructure, allowing them to implement customized security measures tailored to their specific needs. For instance, hospitals can use NPNs to secure sensitive patient data and ensure uninterrupted telemedicine services, while energy companies can protect the integrity of their power grids against potential cyber threats. However, this also means that these entities must take full ownership of their network security. They will need to invest in advanced security solutions and be vigilant in monitoring and responding to emerging threats. The reliance on cloud-based infrastructure only heightens the need for continuous oversight and adaptability.

Both government and private sectors must recognize that traditional approaches to cybersecurity are insufficient in the face of 5G's complexities, especially when combined with the growing reliance on cloud technology in critical areas like healthcare and energy. A new paradigm of collaboration between these sectors is essential to develop and implement strategies that can effectively mitigate the risks. By working together, government bodies, industry leaders, and cybersecurity experts can ensure that the transformative benefits of 5G—such as improved

healthcare services and more resilient power grids—are realized without compromising security.

VIII. FORECASTS

The evolution of 5G, 5G Advanced, and the eventual transition to 6G is anticipated to accelerate at an unprecedented rate, driven by the cloud environment's ability to quickly adapt, introduce new features, and expand into emerging industry verticals. In this rapidly changing landscape, it is essential for both private sector leaders and government agencies to enhance their agility and responsiveness. This adaptability is not just a matter of staying competitive, but also of addressing the critical security and economic challenges that will arise as these technologies continue to evolve. Proactive engagement and strategic planning are necessary to ensure that the nation remains at the forefront of these advancements, fully prepared to manage the risks and seize the opportunities that lie ahead. As we look ahead, several key threats and considerations must be addressed to ensure the security and resilience of 5G technology and its integration with cloud environments.

Expanding Attack Surface:

With the widespread deployment of 5G and the increasing reliance on cloud-based infrastructure and third-party applications the attack surface is rapidly expanding. The proliferation of connected devices and systems introduces new vulnerabilities that cybercriminals could exploit, making it essential to continuously assess and strengthen security measures.

Risk of Cloud Monopolization:

The growing dominance of a few major players in the cloud industry poses a significant risk to critical infrastructure. If key cloud services become monopolized, a single point of failure could have far-reaching consequences, potentially disrupting essential services like healthcare and power grids. It is vital to encourage diversity and competition in the cloud market to mitigate these risks.

The Importance of Ongoing Research and Collaboration:

As 5G technology becomes more ingrained in our society, ongoing research and collaboration across sectors will be crucial to improving security. Governments, private industry, and academia must work together to develop new strategies, share knowledge, and implement best practices to safeguard 5G networks and the cloud infrastructure that supports them.

Societal Impact of Securing the Cloud Environment:

Securing the cloud environment is not just a technical challenge—it has broad societal implications. A secure cloud enables a more interconnected world,

fostering innovation, collaboration, and economic growth. As security measures improve, we can expect higher adoption rates of 5G, the associated third party applications and cloud technologies, leading to a more resilient and efficient global infrastructure. In conclusion, addressing these future considerations through proactive research, collaboration, and strategic planning will be essential to harnessing the full potential of 5G and cloud technologies while minimizing their associated risks.

IX. ANALYTIC DELIVERABLE DISSEMINATION PLAN

Private Sector:

- 5G Leaders (e.g., T-Mobile, Verizon, AT&T)
- Telecommunications and IT Security Professionals
- Industry Associations and Standards Bodies

Public Sector:

- Department of Homeland Security (DHS)
- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal, State, and Local Government Agencies involved in critical infrastructure protection
- Policy Makers and Regulators

REFERENCES

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). 5G security: Analysis of threats and solutions. *Proceedings of the IEEE Conference on Standards for Communications and Networking (CSCN)*, 2017, 1-6. https://doi.org/10.1109/CSCN.2017.8088621

Acemoglu, D., Moustris, G., & Smith, J. (2020). Feasibility of 5G-enabled robotic telesurgery: A study on minimal latency and high-definition video transmission. *Journal of Telemedicine and Telecare*, *26*(4), 237-245. https://doi.org/10.1177/1357633X20904092

Basu, A., Verma, P., & Singh, R. (2021). A programmable slicing approach for resource provisioning in smart healthcare systems. *IEEE Transactions on Network and Service Management*, *18*(3), 1505-1518. https://doi.org/10.1109/TNSM.2021.3102345

Berlet, T., Kalra, A., & Nguyen, M. (2022). Application of 5G in emergency telemedicine: Mobile ultrasound and preclinical diagnostics. *Emergency Medicine Journal*, *39*(7), 510-517. https://doi.org/10.1136/emermed-2021-210805

De Silva, L., Tian, Y., & Gupta, S. (2022). Vertical and horizontal slicing approaches for optimizing performance in smart healthcare scenarios. *IEEE Access*, *10*, 82550-82560. https://doi.org/10.1109/ACCESS.2022.3209012

Enisa. (2019, November 21). *ENISA threat landscape for 5G networks*. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Fonyi, S. (2020, March 23). Overview of 5G security and vulnerabilities. *The Cyber Defense Review*. https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2008_%20Fonyi_WEB.pdf

Kapassa, G., Papadopoulos, A., & Ioannou, N. (2019). Enhancing data security in eHealth systems through 5G network slicing. *Journal of Medical Systems*, *43*(2), 23-30. https://doi.org/10.1007/s10916-018-1146-9

Mathkor, E., Razdan, M., & Menon, S. (2024). Revolutionizing personalized healthcare management with IoMT and 5G: Continuous health monitoring and tailored treatment plans. *Healthcare Technology Letters*, *41*(1), 12-21. https://doi.org/10.1049/htl2.2023.0107

Pal, S., Gupta, N., & Verma, R. (2023). Customizing virtual networks for healthcare applications using 5G and network slicing. *IEEE Communications Magazine*, (5), 110-116. https://doi.org/10.1109/MCOM.2023.3079432

Porcu, D., et al. (2021). 5G communications as "enabler" for smart power grids: The case of the Smart5Grid project. In I. Maglogiannis, J. Macintyre, & L. Iliadis (Eds.), *Artificial intelligence applications and innovations: AIAI 2021 IFIP WG 12.5 international workshops* (Vol. 628, pp. 1-10). Springer, Cham. https://doi.org/10.1007/978-3-030-79157-5_1

Pradyumna, R., Smith, D., & Thompson, L. (2024). Integrating machine learning with 5G-enabled IoMT systems: Enhancing healthcare delivery while addressing security and privacy challenges. *Journal of Machine Learning in Healthcare*, *14*(2), 78-90. https://doi.org/10.1038/s41598-023-32495-5

Preetham, S., Raj, M., & Verma, A. (2023). A layered architectural framework for securing 5G-enabled IoMT systems. *IEEE Internet of Things Journal*, *10*(1), 310-320. https://doi.org/10.1109/JIOT.2023.3254002

Tian, Y., De Silva, L., & Zhang, X. (2023). A two-sided matching theory-based virtual network embedding solution for improving healthcare network performance. *IEEE Transactions on Network Science and Engineering*, *11*(1), 102-113.