Securing 5G: A Call to Harness Software Innovation

Governments across the globe are racing to develop and deploy 5G technologies because of the enormous potential of 5G networks to transform businesses and individual lives. 5G networks will bring quantum leaps in speed, latency reduction, and flexibility that enable a wide range of new applications. In particular, 5G will support massive expansion of the Internet of Things (IoT), which is expected to grow to more than 200 billion devices by 2023. Together, these technologies will fundamentally reshape the global economy, improve the quality of life for billions of individuals, reshape the digital ecosystem, and transform how humans interact with the physical world.

Cloud services will be so important to 5G that many have referred to 5G as the "cloudification" of telecommunications.

HOW SOFTWARE POWERS 5G SECURITY

Cloud-based Architecture

- Greater resilience
- Scalable security
- Dynamic response

Virtualized Network Functions

- Customized security solutions
- Rapid mitigations
- Diverse and competitive supply chains

Advanced Software Tools

- Artificial Intelligence-driven security
- Robust network threat-monitoring
- Strong encryption and identity management

5G networks are fundamentally different from previous generations of communications technology. Whereas previous iterations of communications networks have relied upon hardware components that quickly become outdated, 5G will leverage software and cloud infrastructure to "virtualize" network functions using the Internet Protocol (IP). In fact, cloud services will be so important to 5G that many have referred to 5G as the "cloudification" of telecommunications. Virtualization and cloudification of network functions will unlock myriad new possibilities for managing and securing networks. For example, software-defined networks will enable the creation of tailored virtual environments that apply security controls customized to the data and devices used within the environment. Such individually tailored network environments will also create substantial operating efficiencies for customers, freeing up human and financial resources that can be reinvested in strengthening security and modernizing infrastructure.

These advancements will create the potential for major cybersecurity gains with 5G adoption. The combination of resilient cloud-based infrastructure and virtualization of key network functions will enable the creation of customized secure networks, scalable security solutions, and standardization of essential security features across a much broader user base. These advantages mean that 5G networks will have a running start on cyber defense, opening the door for policymakers to harness and capitalize on these advancements.

THE BUILT-IN SECURITY ADVANTAGES OF 5G

- **Scalable Security.** Because 5G networks will be largely software based, users will be able to access telecommunications as an on-demand service, adding or reducing capabilities—including security capabilities—on demand. This model also allows network defenders to allocate security resources, such as threat monitoring and analytics tools, to where they're needed most.

- **Stronger Identity and Data Protection.** 5G networks are building in protocols to prevent tracking and spoofing of individual users, to strengthen identity management and authentication, and to encrypt more data, such as a user's unique identifier.

- **Customized Security Solutions.** 5G will enable customized security solutions to address unique needs of individuals and devices, including through private networks with customized security controls, network slices that can apply different rules to different types of devices or traffic, and tailoring software-based security updates to individual devices.

- **Resilient Networks.** Because 5G's cloud-based infrastructure will leverage a broad network of servers to remotely and virtually store data instead of relying on physical hardware systems, 5G networks will improve resilience by storing data at multiple physical locations, limiting service outages, enhancing agility, and removing targets for cyberattack.

- **The Power of AI.** 5G's cloud-based infrastructure will make it easier for network defenders to use cutting-edge Artificial Intelligence (AI) and data analytics tools to identify threats and stop malicious attacks.

Inherent to the monumental increases in data flows and connected devices powered by 5G networks are increased security risks. With exponentially more data in transit and a more decentralized network architecture than in previous generations of communications technologies, 5G networks, like other cutting-edge technologies, bring new opportunities for malicious actors. Securing the next generation of telecommunications technology requires working proactively to build security into 5G networks at every layer.

Governments must seize the opportunity to harness the security advantages 5G technologies can bring, and to address emerging security challenges in an increasingly connected environment. Governments can help unlock the potential of 5G by playing a vital role in incentivizing industry prioritization of security considerations, facilitating development of new security technologies and methodologies, and building international consensus around effective and sustainable approaches to security. Effective 5G security policies will enable governments to capitalize on the immense economic and cybersecurity benefits of 5G.

Governments should lead the way toward establishing trust and security in 5G networks. Specifically, governments should **harness software innovation, secure the 5G ecosystem, harden the cloud, manage supply chain risk,** and **build smart, effective 5G governance.**

These priorities will help governments and their citizens reap the security benefits that 5G can bring. Yet, 5G networks will not develop in a vacuum. Underpinning government and industry efforts to deploy and secure 5G technologies will be a qualified workforce, one that is trained to meet tomorrow's cybersecurity challenges. BSA's *Policy Agenda to Build Tomorrow's Workforce* outlines priorities for building a 21st century workforce that are essential to economic and social innovation broadly, including supporting robust 5G security.

Governments must seize the opportunity to harness the security advantages 5G technologies can bring, and to address emerging security challenges in an increasingly connected environment.

Priorities for a Secure 5G

Harness Software Innovation

As the backbone of 5G networks, innovative software-powered tools and techniques will fundamentally reshape how 5G networks operate—and how they can be secured. 5G networks embrace software solutions to security challenges, and governments should lead the adoption of such solutions. Specifically, governments should:

- **Invest in Promising Technologies to Virtualize Key Network Functions.** Hardware infrastructure in critical 5G network nodes, such as Radio Access Networks (RAN), can create security challenges due to supply chain compromises, proprietary standards, and other issues. Governments should invest in the development and rapid deployment of software solutions to these challenges, such as Open RAN (RAN that uses open, or non-proprietary, interfaces) and virtualized RAN (or V-RAN, which implements RAN functions through software-based platforms) technologies that could unlock competition and advance security at the network's edge.

- **Harness Software Innovation to Enhance Cybersecurity.** Software-based technologies such as software-defined networking , secure network slicing, and network function virtualization bring new opportunities to mitigate cyber risks. Policymakers should develop guidance, support research and development (R&D),

and pilot promising approaches to apply these technologies to develop new security techniques to segregate suspicious traffic, protect sensitive information, authenticate users, and address other key security needs.

» **Prioritize Security in 5G Research and Development.**
As user demand for 5G service rises, governments must invest robustly in technologies and methodologies that can help deliver on 5G's potential. Security must be a priority for these investments. R&D funding can support the development and demonstration of promising approaches such as secure network slicing, automated vulnerability screening, AI applications, supply chain management tools, and more.

Secure the 5G Ecosystem

Securing 5G networks requires more than just securing 5G network infrastructure—it also means securing the vast, dynamic ecosystem of devices that connect to it. This ecosystem includes software applications, AI engines, IoT devices, and other systems that constantly create and transmit new data. Governments should incentivize the secure design, deployment, configuration, and maintenance of systems operating on 5G networks with true end-to-end cybersecurity. Specifically, governments should:

Securing 5G networks requires more than just securing 5G network infrastructure—it also means securing the vast, dynamic ecosystem of devices that connect to it.

» **Promote Secure Software.**
Because 5G is powered by software, mitigating the risk of software vulnerabilities will be more important than ever. To do so, governments should adopt guidance and best practices to help software developers and vendors produce and maintain secure software. The *BSA Framework for Secure Software* is a roadmap for governments and industry to meet this goal. Software security should be integrated with best practices for securing hardware, such as roots of trust, to ensure seamless security throughout the 5G ecosystem.

» **Support Strong Encryption.**
Among the most critical security tools in the 5G environment will be encryption, which will be vital to maintaining the confidentiality and integrity of the vast volumes of data transiting the networks. Governments should commit to enabling networks and applications to use the strongest available encryption tools, and should invest in developing new generations of encryption technologies to keep pace with evolving threats or security challenges arising from the uptake of emerging technologies like quantum computing.

» **Leverage Machine Learning and Artificial Intelligence.**
AI and similar technologies will play a vital role in securing 5G networks, enabling identification and isolation of threats across enormous data sets, automating monitoring, supporting incident response, and more. Governments can help AI bolster 5G security by making data sets available to train AI systems; encouraging the development of secure, transparent AI systems; and investing in AI-focused R&D. BSA has outlined Five Key Pillars for Responsible AI to guide policymakers in this area.

» **Secure IoT Devices.**
Among the most transformative uses of 5G technology will be the massive machine-to-machine interactions across billions of IoT devices. Governments should establish policies incentivizing device manufacturers to design and maintain secure IoT devices. These policies should build upon available internationally recognized standards and industry best practices, and should adopt risk-based, outcome-focused frameworks to achieve optimal results.

» **Create a Zero Trust Environment to Build Defense-in-Depth.** Zero trust architectures assume that all users and data within a network could be threats, and build flexible layers of protections to mitigate those threats, which can range from supply chain disruptions to insider attacks. Building zero trust 5G environments requires decoupling hardware and software systems wherever possible, robust user authentication protocols, ubiquitous encryption, and a strong open source-driven architecture. Governments can advance zero trust approaches through contributing to standards development, best practice guidance, and R&D.

Harden the Cloud

Cloud services will play a central role in the 5G network architecture from core operating services to edge computing environments. Cloud infrastructure will drive many of the security benefits of 5G, including enabling rapid deployment of mitigations, dynamic assignment of computing resources to meet security and resource demands, and greater overall network resilience. Fully capitalizing on these benefits will require secure and trustworthy cloud environments. Governments should:

Cloud infrastructure will drive many of the security benefits of 5G.

» **Adopt Risk-Based Cloud Security Policies.** Securing cloud platforms must be a priority for ensuring the security of 5G networks as a whole. To do so effectively, policies must be risk-based and account for the different types of data cloud services will handle and the different functions they will provide depending on their location within the network. Risk-based approaches, such as the ISO/IEC 27103 standard and the National Institute for Standards and Technology (NIST) Framework for Enhancing Critical Infrastructure Cybersecurity, ensure optimal security outcomes while maintaining necessary flexibility and adaptability to providers to meet customer and security needs within the specific context in which they operate.

» **Align Cloud Security Policies with Internationally Recognized Standards.** Internationally recognized standards, such as the International Organization for Standardization (ISO) 27000 series or the Service Organization Controls (SOC), provide a clear, repeatable basis for assuring and evaluating cloud security. When governments align cloud security policies with these standards, they enable cloud providers to ensure a consistent basis for securing cloud environments around the world, and promote technical interoperability. Moreover, they reflect consensus guidance on the best practices that make cloud services most trustworthy. Governments should also consider establishing reciprocity agreements with other nations that maintain similar security requirements in order to make compliance activities as efficient as possible.

» **Understand Roles and Responsibilities within Complex Cloud Environments.** As cloud services become more integral to 5G networks and the many applications and services they support, the cloud environments become more complex and dynamic. Vendors offer a range of security services that customers embed within their cloud environments, such as embedded identity management or threat monitoring services. As the number of actors within a cloud environment grow, there is a risk of confusion about the aspects of security and privacy for which each actor is responsible. For example, a cloud provider may build in certain security controls, but leave it to customers to configure others; those customers may contract with embedded service providers to address some of these controls. Roles and responsibilities may also differ across different types of cloud services, such as Infrastructure-as-a-Service or Software-as-a-Service. Governments seeking to evaluate cloud security must ensure that policies enable careful distinction of roles and responsibilities within such complex environments.

Manage Supply Chain Risk

Securing 5G networks requires making strategic choices about the hardware and software that makes up the network infrastructure. Effective supply chain risk management practices limit vulnerabilities and make it easier for defenders to protect networks. BSA supports the "Prague Proposals" issued at the May 2019 Prague 5G Security Conference, which guide governments to pursue security objectives in a manner that simultaneously fosters competition and innovation while ensuring that security doesn't undermine the benefits that make 5G technology so promising. Specifically, governments should:

» **Adopt Risk Management Approaches to Supply Chain Security.**
Risk management entails understanding risk by identifying likely threats, vulnerabilities, and potential consequences; tailoring mitigation strategies to risks; and prioritizing actions based on the most relevant and potentially impactful risks.

» **Advance Policy Interoperability.**
The consistency and compatibility of regulations and technical standards across national borders enables transnational cooperation and avoids disrupting innovation. Policymakers should reject categorical prohibitions against the acquisition or integration of technologies simply because they are developed abroad, and instead rely on standards-based risk management frameworks.

» **Ensure Transparent and Fair Supply Chain Policies.**
Absent exceptional circumstances, government supply chain risk management policies and their implementation should be transparent to the public, with impacted stakeholders notified about specific actions. They should also establish meaningful mechanisms for resolving disputes, including opportunities for stakeholders to appeal or protest decisions, provide defense against any alleged offenses, and remediate past concerns. Dispute resolution mechanisms create an environment of certainty and predictability without limiting tools for mitigating risk.

» **Promote Government-Industry Collaboration to Strengthen Security.**
These policies should enable governments and industry to share information, collaborate to disrupt threats, and work cooperatively to develop common solutions to shared challenges. Governments have found success in establishing joint government-industry task forces, multi-stakeholder policy development initiatives, and other collaborative forums; these models should be replicated to address supply chain priorities.

» **Drive Innovation and Competition across the Supply Chain.**
Government policies should incentivize innovation, not only in 5G, but also in technical and procedural approaches to managing supply chain risk. R&D efforts should be targeted to develop new approaches to addressing identified systemic risk—as, for example, development of virtualization technologies holds the potential to address systemic risk associated with Radio Access Network (RAN) vulnerabilities. Moreover, reducing barriers to new entrants in the supply chain will contribute to a healthy and dynamic supplier ecosystem.

The consistency and compatibility of regulations and technical standards across national borders enables transnational cooperation and avoids disrupting innovation.

Build Smart, Effective 5G Governance

Strong security controls and technical measures rely upon effective 5G governance, particularly regarding the technical standards that underpin 5G development around the world. 5G governance will require cooperation between nations and between different government agencies within nations. To establish mechanisms for responsible governance of 5G networks and supporting technologies, governments should:

» **Adopt Open Standards with Built-in Security.**
Open standards promote interoperability—ensuring transparency and consistency in implementations and enabling technologies from one vendor to communicate with those of others; conversely, proprietary standards support closed, proprietary systems. Interoperability is essential to ensure that network operators gain increased visibility into network traffic, and that users have diverse options for security tools. When open standards build security in—a vital priority—they drive a consistent level of protection across diverse networks. For secure, open standards to take root, governments must invest in supporting standard development organizations and processes and working with industry partners to ensure that 5G networks are built on a strong foundation.

» **Cultivate Trustworthy Open-Source Cloud Architectures.**
Governments should incentivize development of trustworthy open source-driven architectural solutions by supporting the establishment of open source licensing and governance regimes and pressing for standards that support open source. Open source-driven architectures can speed innovation and reduce costs, creating a more open, dynamic marketplace. From a security standpoint, such an approach has the potential to improve transparency into critical code and potential vulnerabilities and can reduce risks of supply chain attack by decoupling hardware and software ecosystems. To realize these benefits, government should invest in initiatives to improve confidence in the security and trustworthiness of open source solutions.

» **Establish Flexible, Coordinated Governance Mechanisms.**
As 5G becomes increasingly critical across numerous sectors, there is a risk of incoherent and overlapping governance. 5G as a critical technology in the communications sector, the transportation sector (where 5G will enable broader adoption of autonomous vehicles), the health care sector (where 5G will support life-critical medical devices), the financial sector (where 5G will underpin online financial transactions), and others. Whereas previous generations of communications networks could be regulated strictly as telecommunications services, 5G depends on core infrastructure—such as cloud services—that simultaneously serves multiple functions and clients, making it a poor fit for telecommunications-specific regulations. Successful governance will require a unified approach across sectors and agencies. Such governance mechanisms must be flexible and build risk-based approaches that tailor compliance requirements to each 5G network's specific uses and threats.

5G technologies have the potential to transform the global economy, improve the quality of life for billions of individuals, reshape the digital ecosystem, and transform how humans interact with the physical world, but with 5G comes emerging security challenges in an increasingly connected environment. Governments must seize the opportunity to harness the security advantages 5G technologies can bring, and capitalize on the immense economic and cybersecurity benefits of 5G.