# Securing 5G: NATO's Role in Collaborative Risk Assessment and Mitigation

**Luiz A. DaSilva**
Bradley Professor of Cybersecurity and Executive Director
Commonwealth Cyber Initiative
Virginia Tech

**Jeffrey H. Reed**
Willis G. Worcester Professor
Bradley Department of Electrical and Computer Engineering
Virginia Tech

**Sachin Shetty**
Associate Director and Associate Professor
Virginia Modeling, Analysis, and Simulation Center
Old Dominion University

**Jerry Park**
Professor
Bradley Department of Electrical and Computer Engineering
Virginia Tech

**Duminda Wijesekera**
Professor
Computer Science
George Mason University

**Haining Wang**
Professor
Bradley Department of Electrical and Computer Engineering
Virginia Tech

**Abstract:** The 5th generation of mobile systems (5G) unleashes a new cohort of services that promise to revolutionise transportation, manufacturing, and healthcare and to have a major economic impact. 5G systems are also being adopted by military organisations. They introduce a unique set of security challenges related to the trend towards a 'softwarisation' of the network, the support for high-reliability services, and the international supply chain for these networks. This paper outlines measures that governments, and in par-

ticular the NATO Alliance, should put in place for risk assessment and the certification of secure 5G components and systems. We also make the case for NATO's coordination and support for enhanced international collaboration through articulating a common 5G strategy that informs participation in the standardisation process and public-private partnerships to maintain databases of security threats and their mitigation.

**Keywords:** *5G, cyber security, virtualisation, certification, standards, public-private partnership*

## 1. INTRODUCTION

If any doubt remained about communication networks making up a key component of our critical infrastructure, the COVID-19 crisis has put it to rest. With the increased role that these networks play in keeping the economy going, new threats have emerged and existing ones intensified. For example, the healthcare industry has been experiencing a surge in ransomware attacks, with an increase of 350 per cent reported for the last quarter of 2019, a trend that has only worsened in 2020 (Corvus Insurance, 2020). With 5G networks starting to be deployed worldwide, there is justified concern about new cyber threats associated with this technology.

The introduction of any network technology creates the potential for new security attacks, but in some respects 5G is different. It builds on previous generations of cellular technology by improving the bandwidth, capacity, latency and reliability of mobile broadband services. With its promise to enable a new generation of services through ultra-reliable low-latency communications, 5G can also significantly expand the attack surface of the network (Frost and Sullivan, 2020). If applications such as smart homes and blended autonomous vehicles depend on 5G, an attack on the network can have safety-of-life consequences. The apparent dominance of Chinese vendors in the 5G space has also raised questions in the US and elsewhere about the level of independence of vendors from national governments (Iplytics, 2019).

Addressing both technical and geopolitical challenges in 5G security will require strong international cooperation that goes beyond the standardisation process that already takes place in the 3rd Generation Partnership Project (3GPP) and other standards bodies. We believe that this must include the development of international benchmarks for 5G security and a certification process for hardware and software to pass stringent security tests. Recent strides in artificial intelligence can be leveraged for the creation of automated tools to check for security vulnerabilities.

The core principles for 5G security can benefit strongly from international consensus and NATO member states can have a role in establishing the mechanisms for this consensus to emerge. Relevant metrics should be identified and tracked through an international 5G cyber security-focused Infor-

mation Sharing and Analysis Centre (ISAC). An open vulnerabilities database should be created, thereby increasing transparency and affording industry, government and academic stakeholders access to shared information on those security threats plaguing the 5G infrastructure.

The geopolitical issues in the supply chain for 5G networks also require a coordinated approach. The open radio access network concept and, more broadly, the reliance upon 5G systems that are open by design, will encourage the disaggregation of those software and hardware ecosystems associated with 5G. This process has the potential to mitigate the threat posed by supply chain attacks and promote a diversification of 5G vendors.

The broad problem of cyber security in 5G can only be handled adequately through coordination between researchers, industry and policymakers from across the globe. With the strategic role that 5G is starting to play in national security and military organisations, NATO is well placed to facilitate this coordination. This article summarises unique security aspects brought about by the advent of 5G and presents recommendations for how the international community and NATO, in particular, can respond to these challenges.

## 2. 5G SECURITY: WHAT'S NEW?

The vision for 5G security includes security by design, flexibility to respond to new threats, and automated security systems leveraging artificial intelligence (Ahmad et al., 2019). The International Telecommunication Unit Telecommunication Standardisation Sector (ITU-T) has a number of study groups involved in drafting security standards and recommendations. These efforts are complemented by those of other international standardisation bodies such as the 3GPP, the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF).

Nevertheless, some unique concerns attach to the issue of security in 5G systems: a) the virtualisation of network functions and resources; b) the 5G pillars of massive machine-type and ultra-reliable, low-latency communications (Sexton et al., 2017); and c) concerns about the international supply chain for 5G equipment. These are summarised in Figure I.

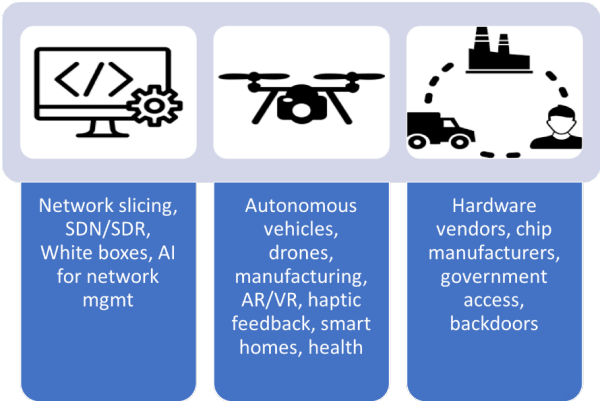
First, softwarisation—that is, moving functionality that was traditionally provided in hardware to software—is a major trend in networks with the advent of Software Defined Network (SDN) and Software Defined Radio (SDR) and the replacement of network-specific hardware with white boxes. In 5G, this trend gains additional steam through a concept called slicing. Network virtualisation and slicing techniques enable the running of multiple logical networks as independent business operations on a common physical infrastructure (Afolabi et al., 2018). In essence, each network slice represents an independent virtualised end-to-end network and allows operators to deploy multiple services with distinct architectures in parallel over the same physical network. While virtualisation and slicing play a critical role in 5G systems,

they also introduce potential security vulnerabilities due to the challenge of simultaneously providing strong resource isolation and efficient resource use in a virtualised environment. Exploiting the shared physical platforms in 5G infrastructure, adversaries could construct side channels or covert channels to impose serious security threats on 5G communications. Thus, it is essential to protect the slice-provisioning process in 5G infrastructures against malicious attacks and to ensure strong slice isolation.

Second, the specifications for 5G are built on three pillars: enhanced mobile broadband; Massive Machine Type Communications (MMTC); and Ultra-Reliable Low Latency (URLL) communications. The last two present a paradigm shift for wireless networks in terms of the need to scale massively (in the case of MMTC) and in the support of stringent reliability requirements (for URLL). They also expand the attack surface of the network to a new class of devices—sensors and Cyber Physical Systems (CPSs)—and services from autonomous transportation to Augmented and Virtual Reality (AR/VR). Attacks on those services can present safety-of-life risks: imagine, for example, a hacker taking control of an autonomous vehicle.

The third area of specific concern in 5G relates to the reliability and trustworthiness of the supply chain for those networks. Huawei Technologies currently leads in the number of declared 5G patent families (Iplytics, 2019), followed by Samsung and LG Electronics. Among the top ten companies in this category, only two are based in Europe (Nokia and Ericsson, in fourth and sixth positions, respectively) and two in the US (Qualcomm and Intel, in seventh and eighth, respectively). The geopolitics of 5G have dominated the news of late, with the US exerting pressure on its allies to not deploy 5G testbeds based on Huawei equipment. Concerns are around a close relationship between the vendor and the Chinese government, with the potential for privacy and security violations (Kaska et al., 2019).

Figure I. Unique aspects of 5G security include issues related to softwarisation (left), high-reliability services (centre) and the supply chain (right).



The softwarisation and virtualisation of 5G, including the introduction of service orientation in the 5G ecosystem, bring advantages and disadvantages. The 5G architecture introduces mobile edge computing (Liu et al., 2018; Mao et al., 2017) as a key component of its architecture that will enable faster and diverse services for new use-cases such as e-health or connected autonomous vehicles. However, virtualised service-oriented architectures have a long history of vulnerabilities (Riaz & Tahir, 2018; Tank et al., 2019), kill chains (Kim et al., 2019; MITRE, 2020) and post-attack forensics (Sharevski, 2018). In addition, the newer application domains may connect their specialised equipment and controllers to 5G base stations. This makes vulnerability tracking and associated risk evaluation and post-attack forensic examinations more complex and issues such as supply chain security and attack attribution more challenging.

The deployment of 5G services will involve re-architecting the wireless cellular network with new capabilities such as software-defined networking, network function virtualisation and a cloud-native architecture. These enhancements bring the need for cyber defence in the edge, secure network slicing, secure multi-access edge computing and access control policies for a disaggregated radio access network.

In the next two sections, we propose a number of actions that can be taken to address these challenges and how NATO, together with the broader international community, can establish tighter collaboration in identifying and overcoming the security threats that may arise with this new technology.

## 3. RISK ASSESSMENT AND MITIGATION

The adoption of 5G poses several security risks that not only affect commercial services but may also have national security implications. In this section, we discuss the need for the development of risk assessment techniques, certification and regulation of 5G equipment and networks.

*A. Risk Assessment and Mitigations Efforts in the US*

To date, academic researchers who have studied security risks associated with 5G adoption have focused on assessing the security vulnerabilities in the 5G network protocol or security issues germane to its core functionalities (Cremers & Dehnel-Wild, 2019; Hussain et al., 2019; Jover & Marojevic, 2019). The scope of those works is somewhat narrow, as they focus exclusively on technology-centric issues. For example, Jover and Marojevic (2019) focus on vulnerabilities in the 5G Radio Access Network (RAN) security architecture and procedures, while Hussain et al. (2019) use formal methods to analyse a simplified 5G protocol model covering six key control-layer protocols.

Recently, government agencies of a number of countries including the US and European Union (EU) member states have released reports and white papers that describe their 5G strategy and risk assessment of 5G security and propose strategies for mitigating those risks (CISA, 2019; DoD, 2020; European Commission, 2020; NIS Cooperation Group, 2019, 2020; White

House, 2020). In contrast to the academic literature, these reports take a much broader view in assessing the risks associated with 5G adoption, with a particular emphasis on supply chain vulnerabilities and the risks associated with untrusted 5G equipment vendors.

In particular, the Cybersecurity and Infrastructure Security Agency (CISA) of the US's Department of Homeland Security (DHS) published a note that represents an analysis of the vulnerabilities in the supply chain, network security, deployment of 5G and the lack of diversity of 5G vendors in the market (CISA, 2019), pointing to:

- Supply chain vulnerabilities. Use of 5G components produced by untrusted vendors could expose these networks to vulnerabilities introduced by malicious hardware and software, counterfeit components and flawed components due to substandard manufacturing processes and maintenance procedures. 5G software, hardware and services provided by untrusted entities could also increase the risk of compromise to the confidentiality, integrity and availability of information sent and received over 5G networks.
- Network security vulnerabilities. Some aspects of 5G are based on enhancements to prior generation cellular technologies and most initial 5G deployments will use some components of the legacy 4G LTE infrastructure, as in the 5G non-standalone deployment model. These factors may expose 5G networks to some of the vulnerabilities of legacy systems. 5G may also have unknown vulnerabilities despite its security enhancements.
- Deployment vulnerabilities. Compared to previous-generation cellular technologies, 5G is more complex and is composed of many heterogeneous components that can provide additional attack vectors and surfaces. The efficacy of 5G's security enhancements will partially depend on proper implementation, configuration and deployment of those enhancements.
- Reduction of competition and trusted options. The domination of the 5G equipment and component market by a very small number of vendors increases the likelihood of proprietary 5G technologies proliferating in the market. Proprietary technologies that do not meet interoperability standards would be difficult to upgrade, repair and replace. This may increase the lifecycle cost of 5G equipment and infrastructure and may contribute to delays in 5G deployment. Limited interoperability among 5G technologies would harm competition in the market, raising barriers to the entry of smaller vendors.

*B. Risk Assessment and Mitigation Efforts in the EU*

In 2019, the EU published a report entitled EU coordinated risk assessment of the cyber security of 5G networks (NIS Cooperation Group, 2019) which follows the systematic approach dictated by an international standard on information security risk management, ISO/IEC 27005. The risk assessment described in the report is modelled on assumptions about use-cases

and plausible scenarios. Specifically, this risk assessment focuses on threat vectors; types of threats posed to 5G networks; assets and their degree of sensitivity; vulnerabilities; and risks and relevant scenarios.

The EU coordinated risk assessment report concludes that the cyber security challenges and threats related to the rollout and operation of 5G networks create a new security paradigm, which necessitates the reassessment of current security policies and frameworks. These challenges include, but are not limited to, the following issues:

- 5G networks' increased reliance on software-based virtualised network functions may result in increased exposure to attacks and additional potential entry points for attackers. The softwarisation of the network functions could also make it easier for threat actors to insert backdoors and other attack enablers into products and make them more difficult to detect.
- The network operators' increased reliance on a small number of 5G equipment vendors may increase exposure to security risks. This may also lead to a greater number of attack paths exploited by state-backed attackers, posing a threat to national security.
- To mitigate the threat posed by the increased exposure to attacks facilitated by equipment vendors, the creation of a risk profile of each equipment vendor may be necessary. This profile includes an analysis of the likelihood that the vendor is subject to influence by an adversarial country.
- A major dependency on one or two vendors significantly increases exposure to a myriad of availability and cyber security problems, including potential equipment supply interruption, service disruptions due to design flaws, bugs and vulnerabilities in the equipment hardware and software and possible exploitation of vulnerabilities by threat actors. Major dependency on a vendor with a high degree of risk presents an especially serious security issue.
- The unique attributes of the 5G network architecture and its novel functionalities may increase exposure to certain types of attacks or provide targets for cyber attacks. Management and Orchestration (MANO), which is a key element of a 5G core network's Network Function Virtualisation (NFV) architecture, may provide a tempting target for threat actors who intend to disrupt the services provided by a 5G core network.
- In addition to the traditional security concerns of confidentiality and privacy, threats to the availability and integrity of 5G networks will increasingly pose a significant risk. Unlike prior-generation cellular technologies, 5G networks are expected to enable and support a broad range of commercial and military uses, including smart factories, the Internet of Things (IoT), autonomous vehicles, AR/VR in military training and smart military warehouses. The integrity and availability of those uses will become major national security concerns.

# 4. CERTIFICATION AND VALIDATION

Most governmental regulatory authorities that regulate radio frequency (RF) communications, such as the Federal Communications Commission (FCC) in the US, carry out or oversee a programme to certify that RF-signal-emitting devices are compliant with rules and regulations and do not interfere with existing devices and systems that use their nation's airwaves. Under the direct guidance of regulatory authorities or guided by their regulatory constructs, the industry self-certifies wireless devices in a cost-effective, regulation-compliant manner, often by employing a process that is baked into their production and distribution processes.

Not surprisingly, the conformance testing and certification processes for 5G are extensive and international, as 5G is a set of truly global technologies. There are three types of entities involved in these processes: standards-setting entities, device-certification entities and regulatory entities. Specifically, for 5G testing and certification processes, the 3GPP sets the related standards, the Global Certification Forum (GCF) and the Personal Communications Service (PCS) Type Certification Review Board (PTCRB) mandate 3GPP test cases used for device certification and regulatory agencies around the globe such as the FCC issue regulations to ensure compliance. Test cases defined in 3GPP specifications are verified by using executable scripts. 5G chipset and device manufacturers must comply with the 3GPP test cases that the GCF and PTCRB have mandated to achieve certification. After the test cases are selected by the GCF and PTCRB, the test vendors implement the corresponding test specifications in their conformance test solutions.

At present, there are no systematic conformance testing and certification processes specifically aimed at 5G security. However, the cyber security certification programme for cellular-connected IoT devices (CTIA Certification, 2020) launched by the Cellular Telecommunications Industry Association (CTIA) has obvious relevance to 5G security. By offering cyber security certification for IoT devices, this certification programme aims to protect consumers and wireless infrastructure while creating a secure foundation for IoT use, such as smart cities, smart factories, connected automobiles and e-health. The programme builds on the IoT security recommendations from the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA). Multiple stakeholders, including leading mobile operators, device and equipment vendors, security experts and test labs were involved in the development of the programme's test requirements and plans.

These certification initiatives focus primarily on end-user devices. It is important to establish certification mechanisms for equipment deployed in the core and radio access networks. The EU cyber security certification framework for ICT products, devices and processes, established in the EU Cybersecurity Act (European Union, 2019) may serve as a starting point and can be extended to directly address 5G supply chain risks.

Due to several factors—including increased complexity, inherent heterogeneity and the softwarisation and virtualisation of critical functions—5G is expected to be more exposed to vulnerabilities and cyber attacks than its predecessors. To ensure the long-term success of 5G, it will be critical to certify that its devices and infrastructure are well protected from potential cyber attacks launched by threat actors under various scenarios. The first step in this direction is the establishment of a conformance and certification programme that specifically addresses security issues in 5G devices and systems. Such a programme should involve all relevant 5G stakeholders and follow well-established recommendations and procedures from regulatory agencies and global certification entities.

## 5. RECOMMENDATIONS FOR NATO'S SUPPORT TO GLOBAL 5G SECURITY COOPERATION

*A. International Partnership for Risk Assessment and Product Testing*

Countries must conduct a risk assessment of their security processes and adopt advanced security measures to ensure the successful deployment of 5G. A consortium of NATO nations and its strategic partners working together to develop cyber risk management policies for 5G systems is paramount. For example, the EU toolbox for 5G security (NIS Cooperation Group, 2020) has provided member states with the opportunity to conduct a gap analysis and launch new initiatives to improve existing security measures and enforcement mechanisms. The toolbox has aided a systematic self-assessment and has resulted in several member states being prepared to adopt advanced security measures on 5G cyber security. This initiative should be expanded to and adopted by non-EU NATO nations.

NATO and the Allies must each develop a strategy to ensure security by design for 5G beyond infrastructure deployment. This should include a rigorous process for vetting vendors and carriers of such networks. This process should be laid out by an international consortium of industry and government stakeholders, including the NATO Standardization Office (NSO) and other entities such as relevant Centres for Excellence that would look at balancing risk mitigation and security. The consortium should explore approaches to establishing and maintaining situational awareness over 5G supply chains and security practices of suppliers and vendors. This organisation would ensure that 5G products comply with security specifications provided by the 3GPP and other key standardisation bodies. It should also develop a framework for assessment, mitigation and management of the range of risks to 5G networks. This includes developing testing tools for automated evaluation of the security of 5G networks; artificial intelligence solutions that rely on shared data are promising candidates for this. Finally, the consortium should incentivise improvements in security with initiatives such as (i) easy access to license-free or lightly-licensed spectrum to incentivise innovation: (ii) incentives for shared accountability in the supply chain that results in access to trustworthy hardware and software: and (iii) investigation of new busi-

ness models that incentivise manufacturers and operators that meet security benchmarks.

As industries race towards deploying 5G networks in operational settings, there is a need to conduct a security analysis of the 5G infrastructure in diverse domain areas. Universities can play a key role in conducting security risk assessments with the potential to uncover exploitable vulnerabilities that could affect the resilience of the 5G infrastructure. Collaboration between research groups in North American and European universities can lead to an international research testbed on which to conduct empirical validation of innovative security technologies.

*B. Cyber Threat Intelligence Sharing*

5G security cannot be under the exclusive purview of technical teams. When a cyber threat emerges, it is generally detected first by private actors or by the public. Therefore, for organisations to be swift in responding to a cyber threat requires the fast sharing of relevant information by those actors. This can be accomplished through an Information Sharing and Analysis Centre (ISAC) (ENISA, 2018). The problem is thus to develop a cyber-threat information sharing capability allowing authorised participants to share real-time Cyber Threat Information (CTI) within an ISAC. That capability also has to ensure trust, anonymity and security to all users both inside and outside the ISAC. The significance of cyber security information sharing has led governments and regulators to mandate or encourage such sharing.

In the US, the Cybersecurity Information Sharing Act (US Congress, 2015) incentivises collaborative sharing among private- and public-sector organisations by providing liability protection to the sharing parties. The EU has also launched several cross- and intra-sector initiatives to enhance member states' capability for preparedness, cooperation, information exchange, coordination and response to cyber threats. ITU-T recommendation X.1215 also discusses how structured threat information expression (STIX) language can be used to support CTI and information sharing, such as knowledge of threats, vulnerabilities, incidents, risks and mitigations and their associated remedies (ITU-T, 2019). To ensure a successful CTI capability, there is also a need for a large number of participants who actively share cyber incidents. Limited participation in this information sharing can significantly impair the ability to manage cyber risks. For example, the DHS has reported that the limited number of participants that ingest cyber threat information is the main barrier to improving the quality of indicators that can provide actionable information to remediate cyber threats (Office of the Inspector General of the Intelligence Community, 2019).

The fundamental concerns of low participation in CTI sharing include lack of trustworthiness from the participating organisations, uncertain authenticity of the exchanged information, improper anonymity, the existence of free-riders, malicious insiders and the possibility of information tampering. Blockchain technology should be investigated for its potential for transparent

and trusted information exchange that would give provenance for vendors' and suppliers' actions. An example of blockchain's use for information sharing has been demonstrated by IBM's Mission Partner Environment (MPE) (IBM, 2018). The MPE is empowered by blockchain private channels that allow the exchange of unclassified information between unclassified and classified networks. The MPE facilitates multinational information sharing and ensures the number and size of each shared MPE are essentially reduced to ledger. The shared private channel ledger capability lowers implementation costs through the reuse of existing MPE resources, increases sharing by enabling countries to use their indigenous technologies and provides accountability via immutable ledger and fine-grained lifecycle security control.

*C. Expansion of Standardisation to the 5G Ecosystem*

There will be a need for several standardisation efforts focused on secure 5G infrastructure and secure 5G-enabled use cases. Although 3GPP provides 5G infrastructure security specifications, there is a need for additional standard bodies at the intersection of 5G and technologies such as blockchain, IoT and autonomy. Public-private partnerships can be leveraged to develop de facto standards and promote best practices for 5G security implementation and 5G secure supply chains that other countries may come to adopt.

These efforts will benefit from government funding focused on realising: (i) standards-compliant network stacks for 5G and beyond that are open-source and secure by design to encourage the decoupling of the software and hardware ecosystems of 5G; these, in turn, will mitigate the threat posed by supply-chain attacks and promote 5G vendor diversification and market competition; (ii) innovation support for start-up companies; (iii) international collaboration and partnerships that create joint academic and research programmes centred on 5G; (iv) participation in standards bodies responsible for 5G and related technologies; and (v) exchange programs among leading research universities in NATO nations and its strategic partners such as South-Korea, Japan and Australia.

## 6. CONCLUSION

There is widespread awareness by governments and industry of the great potential for economic development that comes with 5G and of the new security vulnerabilities that come with it. More than in previous generations of mobile systems, there is also open discussion of the geopolitical factors in play. Specific concerns about security and privacy in the context of major Chinese 5G vendors have led to widely publicised discussions between US national security officials and their counterparts in allied nations.

The defence and national security apparatuses in many countries are grappling with how they can adopt 5G as part of their own critical communications infrastructure. In doing that, they face questions including military and civilian spectrum-sharing, adoption of open source implementation and securing the supply chain. It is appropriate, therefore, that NATO plays a role in

5G innovation and security by design, in sharing of 5G threat intelligence and in the certification of 5G security solutions.

We argue that increased cooperation among NATO nations and its strategic partners is vital to effectively face the new challenges brought by 5G. A role for NATO in serving as a forum for collaboration in 5G security across the Atlantic and expanding that collaboration through its diplomatic dialogues has also been recently advocated by others (Chivot and Jorge-Ricart, 2020). The development of a common 5G security strategy across the Atlantic would be the critical first step towards implementing the recommendations in this chapter. A common strategy, with buy-in from key stakeholders in government and industry, could lead to the creation of joint research programmes, harmonised spectrum allocation, a united front on the development of standards and incentives to accelerate intellectual property and innovation. 6G is already starting to be discussed: to regain the leadership in 5G and its successors, NATO nations will need to incentivise close collaboration between academic researchers, relevant NATO Centres of Excellence, NATO entities, private industry and regulators in NATO nations working together towards a common goal. Modest funding by the European Commission exists for international research collaboration in 5G, but this would need to be increased significantly with coordinated participation from funding agencies across the Atlantic to achieve the level of effect that we advocate in this article.

Such a joint strategy could also lead to more effective and coordinated participation by NATO nations and non-NATO EU member states in the standardisation of 5G and subsequent generations. It could also affect the adoption and success of new technologies, like open source initiatives for the 5G radio access network being championed by the O-RAN Alliance (2020) that can have a profound impact on the supply chain of these future networks.

## 7. REFERENCES


Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A., & Flinck, H. (2018) Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. *IEEE Communication Surveys and Tutorials.* 20 (3), 2429–2453.

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019) Security for 5G and beyond. *IEEE Communication Surveys and Tutorials.* 21 (4), 3682–3722.

Chivot, E., & Jorge-Ricart, R. (2020) *The EU's approach to 5G and the reshaping of transatlantic relations.* European Leadership Network. Available from: https://www.europeanleadershipnetwork.org/commentary/the-eus-approach-to-5g-and-the-reshaping-of-transatlantic-relations/ [Accessed 19th October 2020].

Corvus Insurance. (2020) Security Report. Available from: https://info.corvusinsurance.com/hubfs/Security%20Report%202.2%20-%20Health%20Care%20.pdf [Accessed 16th November 2020].

Cremers, C., & Dehnel-Wild, M. (2019) Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion. In Network and Distributed Systems Security Symposium (NDSS).

CTIA Certification. (2020) *IoT cybersecurity certification program management document* Available from: https://api.ctia.org/wp-content/uploads/2020/ 05/ CTIA-IoT-Cybersecurity-Program-Management-Document-Ver-1.2.pdf [Accessed: 4th August 2020].

Cybersecurity and Infrastructure Security Agency (CISA). (2019) *Overview of risks introduced by 5G adoption in the United States* (tech. rep.) Available from: https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf [Accessed 1st October 2020].

Department of Defense (DoD). (2020) *Department of Defense 5G strategy* (tech. rep.). Available from: https://www.cto.mil/wp-content/uploads/2020/05/ DoD_5G_Strategy_May_2020.pdf [Accessed 1st October 2020].

ENISA. (2018) *Information Sharing and Analysis Centers (ISACs): Cooperative models* Available from: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models [Accessed 3rd August 2020].

European Union. (2019) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/213 (Cybersecurity Act). Available from: https://eur-lex.europa.eu/legal-content/EN/ TXT/PDF/?uri=CELEX:32019R0881&from=EN [Accessed 1st October 2020].

Frost & Sullivan. (2020) 5G and Cybersecurity Implications for Enterprises. Technical Report.

GSMA. (2020) *5G spectrum: GSMA public policy position*. Available from: https://www.gsma.com/spectrum/wp-content/uploads/2020/03/5G-Spectrum- Positions.pdf [Accessed 1st October 2020].

Hussain, S. R. et al. (2019) 5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol. In ACM SIGSAC Conference on Computer and Communications Security (CCS), 669-684.

IBM. (2018) *Blockchain for multinational information sharing.* Available from: https://www.ibm.com/blogs/blockchain/2018/06/blockchain-for-multinational-information-sharing/ [Accessed 11th September 2020].

Iplytics. (2019) *Who is leading the 5G patent race?* Available from: https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race 2019.pdf [Accessed 30th July 2020].

ITU-T. (2019) X.1215: *Use cases for structured threat information expression* Available from: file:///Users/connect_user/Downloads/T-REC-X.1215-201901-I!!PDF-E.pdf [Accessed 21st September 2020].

Jover, R., & Marojevic, V. (2019) Security and protocol exploit analysis of the 5G specifications. IEEE Access 7, 24956-24963.

Kaska, K., Beckvard, H., & Minárik, T. (2019) *Huawei, 5G and China as a security threat* Available from: https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/ [Accessed 16th November 2020].

Kim, H., Kwon, H., & Kim, K. K. (2019) Modified cyber kill chain model for multimedia service environments. *Multimedia Tools and Applications*. 78 (3), 3153–3170.

Liu, M., Mao, Y., Leng, S., & Mao, S. (2018) Full-duplex aided user virtualization for mobile edge computing in 5G networks. *IEEE Access*. 6, 2996–3007.

Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017) A survey on mobile edge computing: The communication perspective. *IEEE Communication Surveys and Tutorials*. 19 (4), 2322–2358.

MITRE. (2020) ATT&CK *Matrix for Enterprise.* Available from: https:// attack.mitre.org/ [Accessed 4th August 2020].

NIS Cooperation Group. (2019) EU coordinated risk assessment of the cybersecurity of 5G networks. Technical Report.

NIS Cooperation Group. (2020) *Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures*. Available from: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating- measures [Accessed 3rd August 2020].

Office of the Inspector General of the Intelligence Community. (2019) *Unclassified joint report on the implementation of the Cybersecurity Information Sharing Act of 2015.* Available from: https://www.oversight.gov/sites/default/files/oig-reports/Unclassified%2020191219_AUD-2019-005-U_Joint%20Report.pdf [Accessed 21st September 2020].

O-RAN Alliance. (2020) Operator Defined Next Generation RAN *Architecture and Interfaces*. Available from: https://www.o-ran.org/ [Accessed 1st October 2020].

Riaz, H., & Tahir, M. A. (2018) Analysis of VMware virtual machine in forensics and anti-forensics paradigm, In International Symposium on Digital Forensic and Security (ISDFS).

Sexton, C., Kaminski, N., Marquez-Barja, J., Marchetti, N., & DaSilva, L. (2017) 5G: Adaptable Networks Enabled by Versatile Radio Access Technologies. *IEEE Communications Surveys and Tutorials*. 19 (2), 688-720.

Sharevski, F. (2018. Towards 5G cellular network forensics. EURASIP Journal on Information Security. 8.

Tank, D., Aggarwal, A., & Chaubey, N. (2019) Virtualization vulnerabilities, security issues, and solutions: A critical study and comparison. International Journal of Information Technology.

US Congress. (2015) Cybersecurity Information Sharing Act of 2015. Available from: https://www.congress.gov/bill/114th-congress/senate-bill/754 [Accessed 1st October 2020].

White House. (2020) National strategy to secure 5G of the United States of America. Technical Report.