Mapping Cyber Threats in the 5G Supply Chain: Landscape, Vulnerabilities, and Risk Management

Moyan Lyu, Junaid Farooq, *Member, IEEE*, and Quanyan Zhu, *Senior Member, IEEE*

***Abstract*—Modern 5G systems are not standalone systems that come from a single vendor or supplier. In fact, it comprises an integration of complex software, hardware, and cloud services that are developed by specialist entities. Moreover, these components have a supply chain that may have linkages and relationships between different vendors. A mobile network operator relies on the functionality and integrity of all the constituent components and their suppliers to ensure the communication network's confidentiality, integrity, and availability. While the operator can employ cybersecurity best practices itself, it does not have control over the cybersecurity practices of its immediate vendors and the wider supply chain. Recently, attackers have exploited cyber vulnerabilities in the supplier network to launch large-scale breaches and attacks. Hence, the supply chain becomes a weak link in the overall cybersecurity of the 5G system. Hence, it is becoming crucial for operators to understand the cyber risk to their infrastructure, with a particular emphasis on the supply chain risk. In this paper, we systematically break down and analyze the 5G network architecture and its complex supply chains. We present an overview of the key challenges in the cybersecurity of 5G supply chains and propose a systemic cyber risk assessment methodology to help illuminate the risk sources and use it to manage and mitigate the risk. It will guide stakeholders in establishing a secure and resilient 5G network ecosystem, safeguarding the backbone of modern digital infrastructure against potential cybersecurity threats.**

***Index Terms*—5G networks, supply chain, cybersecurity, vendor risk management, bill-of-materials.**

I. Introduction

The advent of fifth-generation (5G) network technology heralds a new era in telecommunications, offering unprecedented speed, lower latency, and enhanced connectivity. One of the applications of 5G connectivity is to enhance the supply chain security of various industry verticals. However, the supply chain that underpins the 5G network infrastructure itself is susceptible to a wide range of cyber-physical threats. Unlike traditional telecommunications infrastructures, 5G networks are complex ecosystems, integrating a vast array of components like Radio Access Networks (RAN), Core Networks (CN), Multi-access Edge Computing (MEC), and extensive cloud services. These components are developed, managed, and supplied by a myriad of specialized entities globally, making the 5G supply chain a web of intricate interdependencies and relationships [1]. This complexity exposes the 5G networks to various cyber-physical threats, as seen in notorious supply chain attacks like SolarWinds, where vulnerabilities in the supply chain were exploited to execute large-scale cyber-attacks [2]. In recent years, there has been an increasing focus on cyber criminals in targeting and exploiting the most vulnerable components in the hardware and software supply chains, including virtual network functions (VNFs), programming libraries, software updates, etc. Such incidents underscore the imperative for mobile network operators to rigorously evaluate the cybersecurity practices of their supply chain, extending beyond immediate vendors to the entire network of suppliers.

While the network operators may have control over their own cybersecurity practices or *cyber-hygiene*, they may not have the awareness and direct control of the cybersecurity of their vendors in the extended supply chain. Consequently, it becomes imperative for them to thoroughly understand the provenance and security posture of the vendors that contribute to the 5G ecosystem, and to assess the risks they may introduce into the system operations [3]. The risk assessment involves fundamentally understanding how the network components are interconnected and how the cyber risk to the system can be amplified when components become part of a complex network. Furthermore, there is a need to understand the cybersecurity risk posed by every supply chain actor in the system, as well as the linkages and relationships among the vendors. From a mobile network operator's point-of-view, a supplier may have a very high cyber risk, but it may be related to a component that does not play a critical role in the system security. On the other hand, there may be a supplier with a low cyber risk, but it may be related to a highly critical component for system security. Similarly, an immediate component supplier may have a very low risk but may be owned or controlled by another entity with a low cybersecurity rating. Therefore, simply understanding the risk posture of suppliers is not enough, and we require system assessment to accurately characterize supply chain cyber risk.

Therefore, the cybersecurity of the 5G supply chain presents a complex risk landscape, wherein the diversity of components and suppliers contributes to a security environment that is only as strong as its weakest link. This necessitates continuous vigilance and comprehensive cybersecurity strategies to maintain the network's integrity and resilience [4]. This paper aims to dissect these issues, offering insights into the vulnerabilities inherent in the decentralized and multifaceted 5G supply chain and proposing measures to mitigate these

Moyan Lyu and Junaid Farooq are with the Department of Electrical & Computer Engineering, College of Engineering and Computer Science, University of Michigan-Dearborn, Dearborn, MI 48128 USA. E-mails: {moyanlyu, mjfarooq}@umich.edu.

Quanyan Zhu is with the Department of Electrical & Computer Engineering, NYU Tandon School of Engineering, Brooklyn, NY 11201 USA. Email: qz494@nyu.edu.

This work was supported in part by the National Science Foundation (NSF) under grants ITE-2226232 and ECCS-1847056.

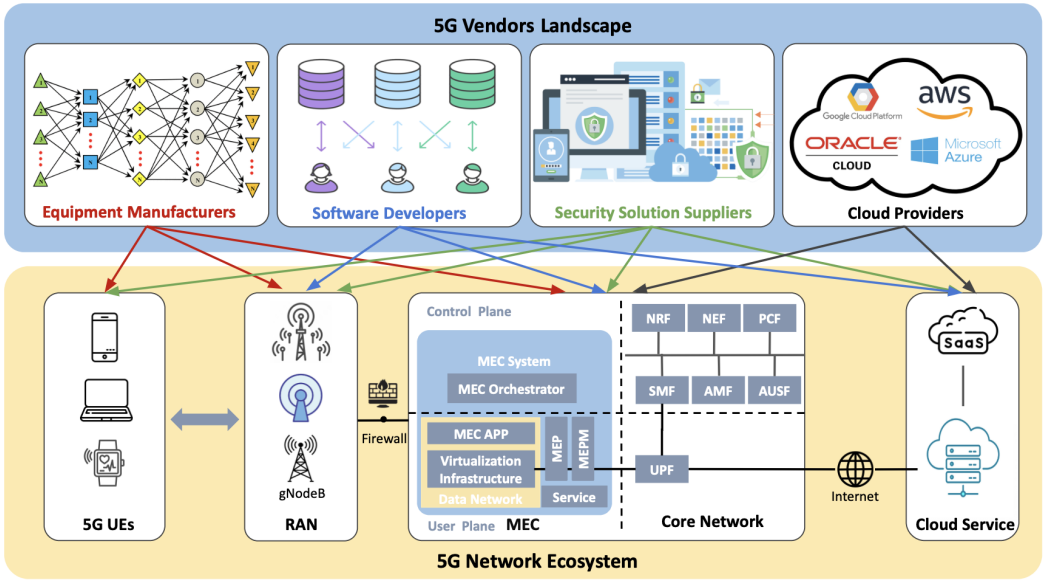

Fig. 1: An illustration of interactions between 5G components (UE, RAN, MEC, Core, Cloud), and the roles of different vendors in equipment manufacturing, software development, security, and cloud-based services.

evolving risks, thereby fortifying the network ecosystem.

The rest of the paper is organized as follows: Section II provides a detailed overview of the 5G supply chain, including its composition and the associated vendor ecosystem. Section III delves into the critical challenges of securing the cyber supply chain within the 5G framework. Section IV presents an overview of risk mitigation strategies for the 5G supply chain, and a case study on the systemic cyber risk assessment of 5G systems is showcased in Section V. Finally, the paper concludes with Section VI, exploring potential directions for future research.

II. The Supply Chain of 5G Networks

The architecture of 5G networks embodies a vast ecosystem, ranging from UEs to comprehensive cloud services, integrating a diverse array of vendors like equipment manufacturers, software developers, security solution providers, and cloud service providers. This section explores the key components of the 5G ecosystem and the associated vendor landscape.

A. Key Components Involved in the 5G Ecosystem

The 5G network ecosystem, as illustrated in Fig. 1, encompasses several critical components:

1) **User Equipment:** Positioned at network endpoints, UEs include devices like smartphones, tablets, and myriad Internet of Things (IoT) gadgets. These devices interface directly with the 5G network, connecting through the RAN to the CN and the internet. The UE segment is characterized by a vast array of manufacturers, each bringing unique designs and capabilities. This diversity, particularly in the more economically priced segments, often leads to variations in security features, potentially creating vulnerabilities within the network due to less sophisticated security protocols in cost-sensitive models.
2) **Radio Access Network Equipment:** Acting as the critical conduit between UEs and the CN, the RAN plays an indispensable role in the 5G ecosystem. The shift towards software-defined and open-source RAN systems, such as Open-RAN (O-RAN), brings a new dimension of security challenges. This change introduces a mix of components from different vendors, making it difficult to ensure uniform security standards across the network. Additionally, the RAN's inherent exposure to physical wireless signals opens it to risks of interception, where malicious entities within the supply chain could capture these signals, thus compromising data security and network integrity.
3) **Multi-Access Edge Computing and Core Network:** The core network, the backbone of the 5G infrastructure, handles critical operations such as routing, authentication, and data processing. It is increasingly becoming a target for cyber threats. Vulnerabilities within key network components, such as authentication servers or data management functions, can be exploited to gain unauthorized access, mimic legitimate users, or alter user data. The integration of MEC into the 5G framework adds another layer of complexity, placing processing capabilities closer to end-users and potentially increasing the risk of localized attacks and data breaches [5].
4) **Cloud Services and Software-as-a-Service Platforms:** The deployment of 5G networks over cloud infrastructures implicates inheriting the inherent cyber risks associated with these services. Vulnerabilities in cloud and software-as-a-service (SaaS) offerings, whether due to inadequate security measures or undisclosed backdoors, can significantly impact the security of the entire 5G network. The shared nature of cloud resources, especially in public clouds, necessitates rigorous isolation and protection protocols to prevent unauthorized access and data breaches. Private clouds, while offering more isolation,

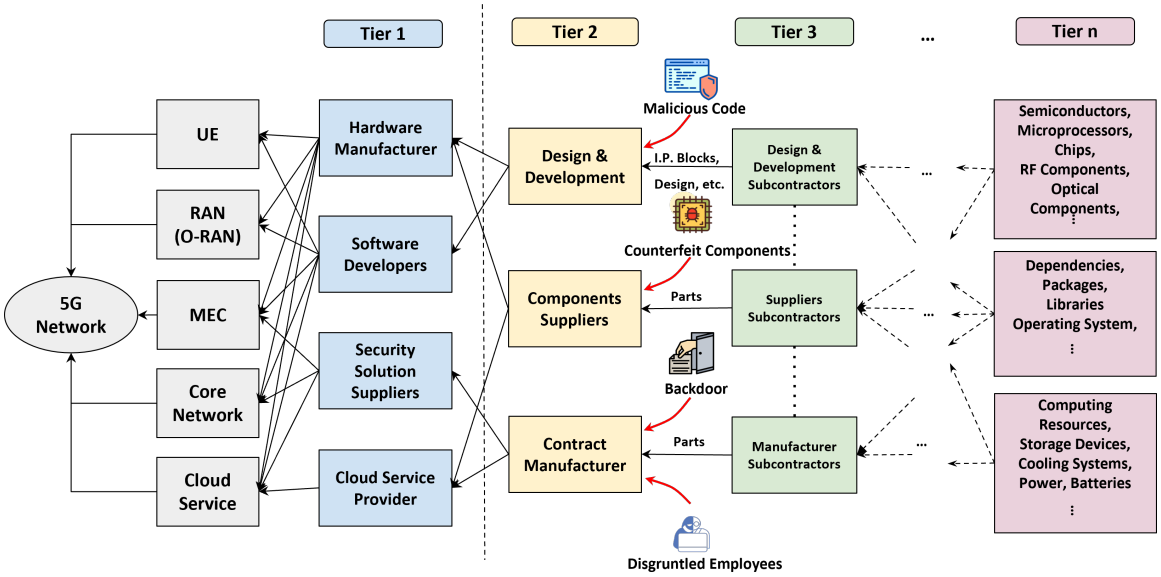

Fig. 2: A high-level representation of the 5G network supply chain ecosystem, illustrating a multi-tiered vendor structure from core hardware manufacturers to peripheral component suppliers and highlighting potential security vulnerabilities at each level, including the risks of malicious code, counterfeit components, and insider threats.

are still dependent on the security measures implemented by the service providers.

B. Vendor Landscape of 5G Networks

The vendor ecosystem in the 5G network, as illustrated in Figure 1, encompasses a broad spectrum of component categories and services. These include hardware elements, software layers, security mechanisms, and cloud-based resources. The analysis below focuses on these categories, specifically addressing the potential security risks and their sources:

1) **Hardware Manufacturers:** At the core of the 5G infrastructure are the computing hardware platforms that host various network functions, such as access and mobility management function (AMF), session management function (SMF) and user plane function (UPF). These platforms comprise servers, storage systems, and specialized network appliances designed to support the high throughput and low-latency requirements of 5G networks. Provided by third-party vendors, these hardware components form the bedrock upon which network capabilities are built and thus represent a vector through which vulnerabilities may be introduced into the system [6]. The provenance of this computing hardware is global, with manufacturers often situated in regions with differing geopolitical interests, which raises concerns about the potential for foreign influence or control over the hardware manufacturers, which could lead to the introduction of backdoors or other security weaknesses [7]. Moreover, Fig. 2 indicates that each tier presents potential vulnerabilities that could be exploited, such as introducing malicious code and counterfeit components. The concerns associated with this tiered supply structure extend beyond mere operational dependencies; they encompass potential vulnerabilities that could be weaponized, allowing for the introduction of backdoors or other security compromises. This global and multifaceted supply chain, with its geopolitical entanglements and extensive reach, demands rigorous scrutiny and robust security protocols to safeguard the integrity of 5G infrastructures against threats that may emerge at any tier.
2) **Software Developers:** This group is responsible for developing operating systems, management software, and the various applications that run on the 5G infrastructure. They work on the Control Plane, manage UPF services, and contribute to the development of cloud services. The software supply chain is depicted in Fig. 3, where the continuous integration (CI) and continuous deployment (CD) pipelines illustrate the journey from code development to production. The paths show how an attacker can infiltrate a CI/CD pipeline to compromise a 5G software development system. Malicious code injection into a system by third-party malware can occur in various ways, such as compromised software packages, managers, services, or even human operators [8]. During the deployment phase, threat actors may insert additional malware into code repositories, causing infected test tools to jeopardize software deployment. Also, during updates, malicious code could be inserted into collaborative platforms such as GitHub and then introduced into the update mechanism of a running program, thereby compromising the integrity of the entire 5G system by updating the application.
3) **Security Solution Providers**: These vendors offer a range of security products and services designed to protect the 5G network from cyber threats. They provide firewalls, intrusion detection systems, and advanced threat prevention tools. In the 5G context, these providers must adapt traditional security solutions to meet the unique requirements of the high-speed, low-latency network.

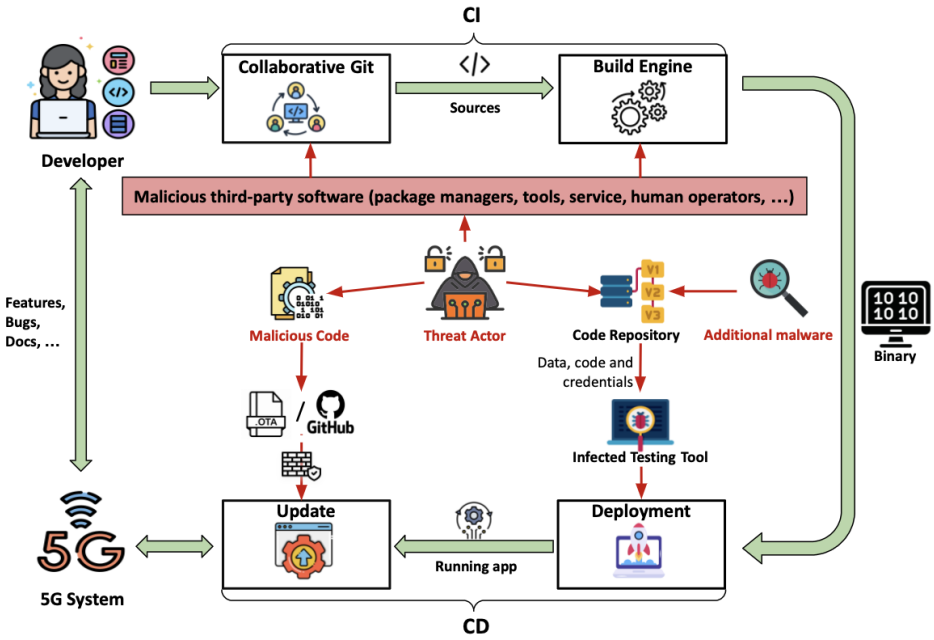

Fig. 3: Overview of software vulnerabilities in 5G networks highlighting potential security breaches from code development to deployment, including risks from malicious third-party software and threat actors targeting repositories and updates.

They must also ensure that their solutions are scalable and flexible enough to accommodate the dynamic nature of 5G services. However, relying on these third-party providers for critical security infrastructure introduces trust and dependency challenges.

4) **Cloud Service Providers:** The 5G network increasingly leverages cloud infrastructure to enhance flexibility and scalability. Cloud service providers offer infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and SaaS that 5G networks utilize for various purposes, including hosting RAN, MEC, and CN components. Major players in this sector, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, are typically known for robust security measures. However, smaller cloud providers might offer different levels of security, thus becoming potential weak points in the 5G supply chain. Issues such as multi-tenancy, data sovereignty, and API security are critical challenges that cloud service providers must address to ensure the security and reliability of 5G services.

III. Key Challenges in Cybersecurity of The 5G Supply Chain

The 5G supply chain faces complex challenges due to its layered technological components and extensive network of global vendors and service providers. Some of the key technological challenges in 5G network supply chain security are described in the following subsections.

A. Complex, Hidden, Multi-tier Interdependencies

Fig. 2 provides a glimpse into the complex structure of the 5G network supply chain, from the fundamental network constituents to the intricate web of suppliers and subcontractors. The 5G ecosystem is built upon countless software libraries, VNFs, and cutting-edge hardware. Each of these components might be sourced from different vendors, potentially across the globe. For instance, a single 5G base station might incorporate a chipset from one manufacturer, software libraries from another, and specific firmware developed by yet another vendor, exemplifying the complex and multi-tiered relationships that are characteristic of these supply chains. A 5G operator, while typically familiar with their immediate suppliers, may not have visibility into the deeper layers of the supply chain, where the "suppliers of their suppliers" operate. This opaqueness becomes particularly pronounced in the context of international trade, where a piece of equipment's journey from manufacture to deployment may span several continents [9]. For example, a European operator might obtain its hardware from a company based in North America, but this hardware may integrate firmware developed in Asia, with each regional link in the chain subject to different regulations and security standards.

B. Vetting of Hardware and Software Vendors

On the hardware front, 5G employs a plethora of new components, from base stations to specialized routers, which were sourced and assembled across diverse global regions, standing at multiple junctures ripe for compromise. From the possibility of counterfeit components slipping into the mix to the risk of unauthorized modifications, the vetting process needs to ensure the integrity of each piece. Moreover, the dynamic and evolving landscape of hardware designs necessitates a one-time vetting and a continuous re-evaluation to ensure that innovations do not inadvertently introduce security loopholes.

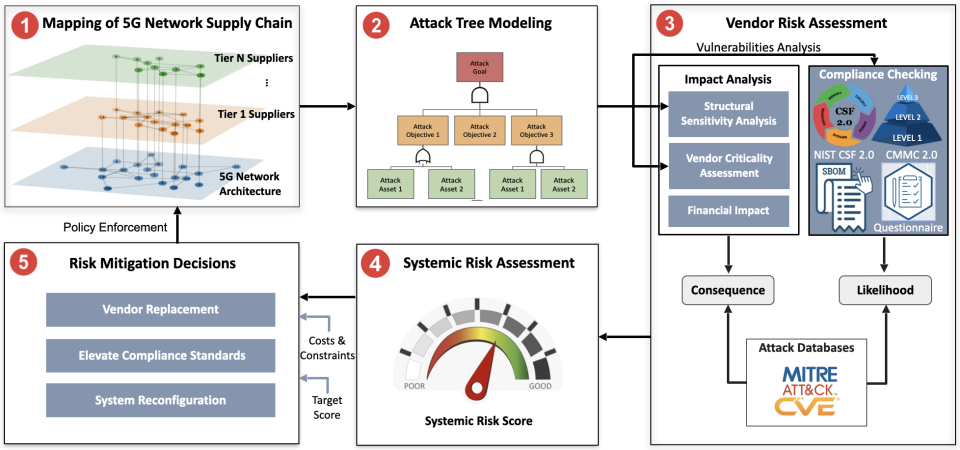

Fig. 4: An integrated cybersecurity framework for 5G networks, utilizing attack tree modeling and compliance monitoring to inform strategic risk mitigation decisions based on systemic threat assessment.

Another layer of complexity is the covert nature of specific threats. Detecting vulnerabilities intentionally designed to remain hidden, such as covert data extraction channels or concealed functionalities, presents a formidable challenge. Additionally, vendors' security practices might fluctuate over time, demanding that vetting is not just a one-off task but a consistent monitoring activity [10].

C. Analyzing Vendor-Induced Impact

The architectural complexity of 5G networks is intensified by the multitude of vendors contributing essential hardware, software, and services. Each vendor, with their distinct cybersecurity practices, introduces a unique profile of potential vulnerabilities to the system. A critical concern is the difficulty quantifying the ramifications of individual vendor contributions to the holistic security of the 5G network. While primary components such as the RAN, CN, and UEs form the backbone of the network, the intertwined dependencies on various vendors' hardware and firmware mean that a vulnerability in one can have cascading effects on the entire system. The challenge lies not just in identifying these vulnerabilities but in evaluating the magnitude and reach of their potential impact. As the 5G ecosystem expands, incorporating diverse vendors from different regions with varying security standards and practices, the task of uniformly assessing their individual implications becomes increasingly daunting. The confluence of multiple vendors' practices makes it arduous to predict how a security lapse in one entity can reverberate throughout the system. The lack of a standardized evaluative framework further exacerbates this challenge, underscoring the pressing need for rigorous methodologies to analyze the systemic risk posed by individual vendors.

D. Trust Quantification Due to Insufficient Data

In the intricate ecosystem of 5G supply chains, a major hurdle is the scarcity of comprehensive data on the cybersecurity measures, practices, and vulnerabilities of the involved entities. This gap hinders the ability to fully assess and understand each supplier's security posture and potential risks. The interconnected nature of the 5G supply chain, where each link is crucial for the overall system's security, exacerbates the challenge. The difficulty in evaluating the broader system impact of a single supplier's compromise is a critical concern. The lack of detailed and transparent data from vendors about their security practices creates an opaque environment, making it challenging for primary operators to conduct a thorough risk assessment and devise effective mitigation strategies [11]. This opacity not only obstructs risk analysis but also complicates the development of a comprehensive and proactive security framework. Moreover, it hinders empirical validation of the risk models due to the lack of ground truth. Therefore, enhancing data transparency and availability becomes essential to enable more informed decision-making and trust-building in the 5G supply chain security realm.

IV. Mitigation Strategies for 5G Network Supply Chain Security

The security of the 5G network supply chain is paramount for the integrity of the telecommunications infrastructure. This section delineates a holistic approach to risk assessment and the implementation of potent mitigation strategies to safeguard the 5G network supply chain.

A. Comprehensive Mapping of the 5G Network Supply Chain

The foundational step in fortifying 5G network security involves an exhaustive mapping of the network's infrastructure. This entails delineating the network topology and identifying all pertinent supplier tiers—from direct Tier 1 suppliers to the nuanced web of subcontractors [12]. Through visual mapping, the interconnections and dependencies within the 5G supply chain are made transparent, which is crucial for pinpointing potential vulnerabilities and gauging the ramifications of any disruptions in network operations. This is shown as step 1 in Fig. 4.

Following the comprehensive mapping, the next critical step is attack tree modeling. As illustrated in step 2, this

methodical modeling serves as a strategic assessment tool, charting potential threat vectors in a hierarchical structure. Beginning with the primary attack goal, it dissects the multiple objectives an adversary might pursue and the specific network assets that could be compromised. This analytical framework is pivotal in preempting security breaches, allowing for the identification of key assets within the supply chain that require fortified protection against potential attack scenarios.

B. Rigorous Vendor Risk Assessment

A pivotal component in mitigating risks across the 5G system is a thorough risk assessment of each vendor within the supply chain. The risk assessment framework proposed herein integrates established cybersecurity frameworks and employs advanced tools to evaluate the likelihood and consequences of potential security breaches.

1) Compliance Analysis: The initial phase of vendor risk assessment necessitates a meticulous examination of each vendor's adherence to cybersecurity standards and best practices. Employing an amalgamation of criteria, including the Cybersecurity Maturity Model Certification (CMMC) 2.0 and the NIST Cybersecurity Framework (CSF) 2.0, we can appraise a vendor's cybersecurity stature and the probability of cyber incursions. A Software Bill of Materials (SBOM), which details the provenance and status of software components, is scrutinized to ensure the use of secure and up-to-date elements.

2) Vulnerability Evaluation: In conjunction with compliance, the evaluation of known vulnerabilities and attack patterns is paramount. Utilizing comprehensive databases such as the MITRE ATT&CK framework and Common Vulnerabilities and Exposures (CVE) data, we can assess prevalent threats and tailor our defense mechanisms accordingly [13]. For instance, a vendor's non-conformity to CSF controls, coupled with known CVE listings, may escalate the estimated probability of a successful attack.

3) Consequence Assessment: The repercussions of cyberattacks are assessed through a multifaceted analytical approach. By constructing an attack tree model, we visualize potential attack vectors, enabling us to discern the network's structural vulnerabilities. Coupled with structural sensitivity analysis, we ascertain which segments of the network and which vendors are most susceptible to breaches. The criticality of each vendor is evaluated based on their indispensability to network operations, and a financial impact assessment quantifies the potential economic losses resulting from a vendor's compromise.

C. Systemic Risk Assessment

Systemic risk encompasses both upstream risks emanating from the intricate web of vendor relationships and interdependencies, as well as downstream risks due to the interconnections in the system architecture [14]. The upstream analysis focuses on assessing the intricate web of relationships, hierarchies, and dependencies among vendors, including mergers, acquisitions, and geopolitical factors that shape their operations. This involves an examination of vendor alliances, inter-dependencies, and the potential cascading effects of cybersecurity incidents or disruptions across the complex network of suppliers. By understanding these intricate vendor dynamics, organizations can gauge the systemic risks propagated through the supply chain and implement mitigation strategies. Conversely, the downstream analysis delves into the inherent risks within the system architecture and topology itself, encompassing the inherent risks associated with individual components. This includes evaluating the security implications of design choices, such as network segmentation, access control mechanisms, and component inter-connectivity. Additionally, it involves assessing the potential impact of vulnerabilities or compromises within individual components on the overall system's integrity and resilience. This holistic perspective ensures a comprehensive evaluation of the entire supply chain, from the intricate web of vendor dynamics to the security implications of architectural design choices.

D. Decisive Risk Mitigation Actions

1) System Reconfiguration: System reconfiguration for risk mitigation in the 5G supply chain involves adopting a comprehensive strategy. Network segmentation could be employed, delineating critical network sections to contain potential security breaches [15]. Enhanced access controls should ensure the least privilege principle, supplemented by robust authentication systems. Establishing failover mechanisms and redundancy for critical components could bolster system resilience against disruptions. Encryption of data, both at rest and in transit, is vital for protection against unauthorized access while bolstering system monitoring and logging to detect and respond to security incidents promptly.

2) Vendor Replacement Protocols: When vendor replacement becomes necessary, a meticulous vetting process is indispensable. Potential new vendors should be evaluated not only for service quality and cost but also for their cybersecurity track records and adherence to rigorous security standards. Utilizing third-party security ratings can provide an objective evaluation of a vendor's security posture. Trial implementations or proofs of concept can help corroborate vendor claims. Including stringent security clauses in contracts, such as audit rights and vulnerability remediation commitments, ensures ongoing vendor compliance. Diversifying the vendor pool can mitigate risks associated with over-reliance on a single supplier.

3) Elevation of Compliance Standards: Elevating compliance standards entails enforcing adherence to recognized cybersecurity standards, such as ISO/IEC 27001, and regularly conducting comprehensive audits. It also involves a commitment to continuous improvement, with regular updates and advancements in cybersecurity practices. Continuous training for vendor personnel in security protocols and compliance requirements is critical to maintain heightened security awareness and readiness. Mandating vendors to secure and sustain relevant cybersecurity certifications adds an extra layer of assurance, reinforcing a robust framework for risk mitigation throughout the 5G supply chain.

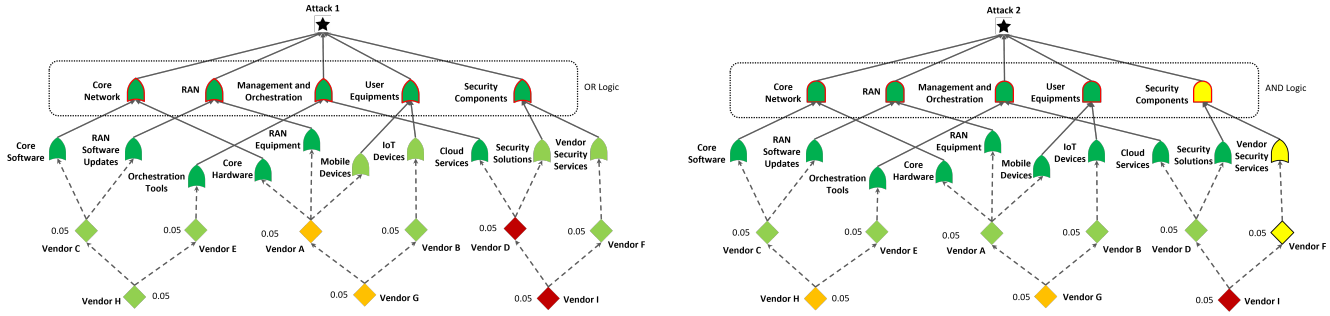

Fig. 5: Attack tree for two different attack types, where top-level components have either an OR logical connection (Attack 1) or an AND logical connection (Attack 2). Node colors indicate the relative sensitivity of system risk to the corresponding node.

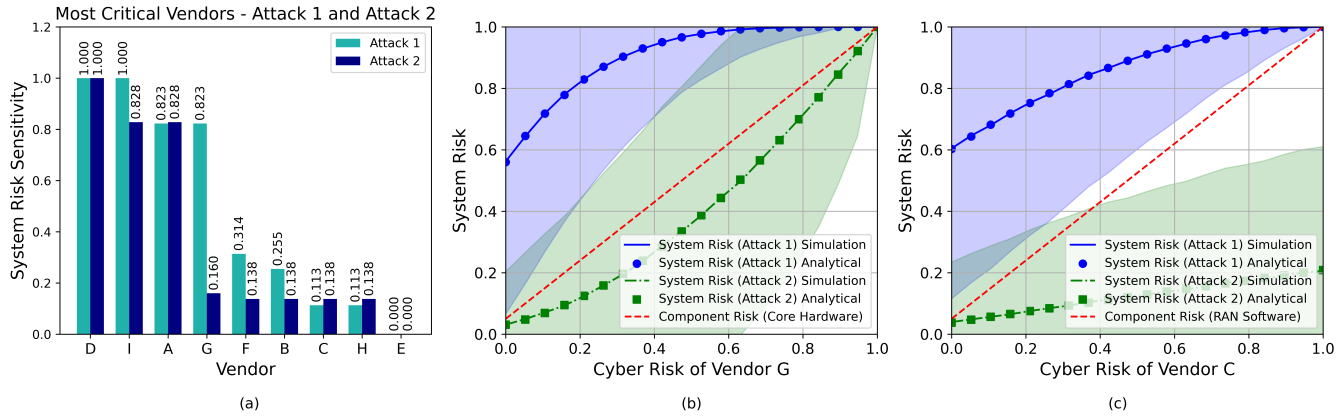

Fig. 6: Risk assessment of the system for different attack types in response to varying cyber risks of vendors G in (b) and vendor C in (c). The corresponding component risk is also plotted for reference in each case.

V. Case Study

In this section, we provide a case study to illustrate the concept of supply chain risk assessment over an example 5G network architecture with the help of attack tree models. We analyze the overall system risk in response to a change in cyber risk of one of the vendors. Our findings have been validated with the help of Monte Carlo simulations.

A. Example 5G Network and Attack Tree Models

We consider the example of a private 5G system with UEs, RAN, CN, management and orchestration tools, and security components. These components have underlying software and hardware components that are potential attack surfaces. Fig. 5 illustrates the logical interconnection between the components of two different types of attacks[1]. Attack 1 assumes an OR logic for the component compromise, e.g., the CN is compromised if either the core software or core hardware is compromised. On the other hand, Attack 2 assumes AND logic for the component compromise, e.g., the CN is considered compromised if both the core software and core hardware are compromised. Furthermore, the vendors and their hierarchy are illustrated in Fig. 5. Vendors A through G are component suppliers, while vendors G through I are top-level suppliers that own other vendors. For instance, vendor G owns or controls vendors A and B. For this case study, we assume that all components and sub-components are risk-free[2] while the only risk in the system emanates from the vendors. For simplicity, we assume a 5% chance of a breach for all vendors A through I. Based on these settings, we analyze the systemic risk, i.e., the probability of system compromise, using attack tree synthesis and determining the relative contributions of the components and vendors to that risk, providing a more accurate quantification. The node colors indicate the relative sensitivity of the node to the overall system risk, which is indicated by a range of colors from green (low sensitivity) to red (high sensitivity). A ranking of the vendors in terms of their sensitivity to the system risk is provided in Fig. 6(a) for both types of attacks considered in the case study. This analysis is particularly useful while prioritizing cybersecurity investments or taking risk mitigation actions, as outlined in Section IV-D.

[1]We focus on two extreme types of attacks for simplicity of analysis. While any arbitrary combination of logical interconnection of components is possible for attack propagation, the impact would be somewhere in between the two extremes.

[2]This assumption has been made to isolate and evaluate the impact of supply chain risks without the additional variable of component-related risks.

B. Analysis & Insights

Based on the sensitivity analysis of the example in our case study, we can see that in the case of Attack 1, vendors I and D are considered highly critical (highlighted in red), while vendors G and A are moderately critical (highlighted in yellow). However, in the case of attack 2, only vendor I is considered highly critical, while the top-level vendors G and I are considered moderately critical. Moreover, we see that the branch of Security Components through Vendor F presents significant criticality. Note that systemic risk analysis has illuminated the potential risk pathways and can be used to prioritize the scrutiny and protection of those attached paths. To investigate and further analyze the behavior of the systemic risk to individual risk of vendors, we have varied the cyber risk of Vendors G and C under both attack types while keeping the risk of the other vendors constant. Fig. 6 (b) and (c) plot the system risk with respect to the cyber risk of vendor G and C respectively. It can be observed that while the risk of the respective components affected (i.e., Core Hardware in Fig. 6(b) and RAN Software in Fig. 6(c) increases linearly as the vendor cyber risk changes, the systemic risk under different attack types can be significantly different and nonlinear. For instance, under attack 1, the system risk is significantly higher than under attack 2. Moreover, in the case of attack 2, the system risk is much lower than the component risk, while for attack 1, the system risk is higher than the component risk. To validate the analytical findings based on probabilistic computations over the attack tree, we also perform Monte Carlo simulation with 10^4 iterations. Each iteration considers a realization of attack state of the vendors, i.e., compromised or un-compromised. Based on the attack tree, the overall system state is determined and averaged over all iterations. Fig. 6 shows that the simulation results validate our analysis and also shows the standard deviation of the risk using the shaded region. Notice that the variance generally decreases as the attack or system failure event becomes more certain. This evaluation can assist in strategic planning for cybersecurity resources, particularly in larger systems with complex supply chains and a high number of vendors. For instance, in certain attack scenarios, a vendor may have a much more critical role and may need more stringent monitoring for cyber threats compared to other threats and vice versa.

VI. Open Challenges and Future Directions

The evolving landscape of 5G supply chain security presents several open problems and avenues for future research, which are critical to enhancing the resilience and integrity of telecommunications infrastructure.

A. Adaptive Security Architectures

Current security solutions often struggle to keep pace with the dynamic nature of 5G technologies and their associated cyber threats. Future research should focus on the development of adaptive security architectures that can automatically adjust to new threats as they emerge. This includes the use of AI-driven security systems that learn from ongoing network activity and threat patterns to predict and mitigate potential breaches before they occur.

B. Holistic Risk Management Frameworks

The inter-connectivity of the 5G supply chain necessitates a holistic approach to risk management that encompasses not just technical solutions but also organizational and operational changes. Future directions should include the creation of comprehensive risk management frameworks that integrate cybersecurity with physical security, personnel security, and supply chain logistics. These frameworks should be capable of assessing risks from multiple dimensions and providing actionable insights for risk mitigation.

C. Standardization of Security Practices

As 5G technology continues to be adopted globally, there is a pressing need for the standardization of security practices across different regions and sectors. Future research should aim to develop global standards that address the unique vulnerabilities of the 5G supply chain. This includes standardized protocols for the assessment, auditing, and certification of security practices among all stakeholders in the supply chain.

D. AI and LLMs in Cybersecurity Compliance and Risk Assessment

Exploring the integration of artificial intelligence, especially large language models (LLMs), offers a transformative avenue for enhancing cybersecurity compliance and risk assessment in 5G supply chains. LLMs have the potential to automate the intricate analysis of cybersecurity frameworks and extensive vendor documentation. This capability enables rapid assessments of compliance against diverse standards, significantly accelerating the evaluation process that is traditionally manual and time-consuming.

VII. Conclusion

The deployment of 5G technology marks a significant milestone in the telecommunications industry, ushering in a new era of connectivity and innovation. However, the vast and globalized supply chain underpinning this technology has become a focal point for cybersecurity concerns. This paper has delved into the complexities of the 5G supply chain, revealing the multifaceted cybersecurity risks inherent within its extensive network of vendors and suppliers. Our examination of the supply chain's structure, identification of key vulnerabilities, and assessment of the risk landscape emphasizes the need for a meticulous and comprehensive approach to secure the 5G supply chain. We have proposed a tailored systematic framework aimed at effectively mitigating these risks. At the core of this strategy is the thorough assessment of vendor risks, the adoption of robust mitigation measures, and the continuous monitoring of supply chain dynamics to preempt potential cyber threats. We have created a case study demonstrating a systematic approach to evaluating cybersecurity risks within the 5G supply chain, highlighting the critical role of vendor risk management and the systemic impact of potential vulnerabilities. By simulating different attack scenarios, we illustrated the potential pathways through which threats can propagate across the network, underscoring the necessity for strategic and informed countermeasures to safeguard the 5G ecosystem.

REFERENCES

[1] J. Boyens, C. Paulsen, N. Bartol, K. Winkler, and J. Gimbi, "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry," National Institute of Standards and Technology (NIST), Tech. Rep. NIST IR 8276, Feb. 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

[2] S. Peisert, B. Schneier, H. Okhravi, F. Massacci, T. Benzel, C. Landwehr, M. Mannan, J. Mirkovic, A. Prakash, and J. B. Michael, "Perspectives on the SolarWinds incident," *IEEE Security & Privacy*, vol. 19, no. 2, pp. 7–13, 2021.

[3] E. S. R. Board, "Mitigating systemic cyber risk," Tech. Rep., 2022. [Online]. Available: https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemiCyberRisk.220127~b6655fa027.en.pdf

[4] K. Zheng and L. A. Albert, "A robust approach for mitigating risks in cyber supply chains," *Risk Analysis*, vol. 39, no. 9, pp. 2076–2092, 2019.

[5] T. W. Nowak, M. Sepczuk, Z. Kotulski, W. Niewolski, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "Verticals in 5G MEC-use cases and security challenges," *IEEE Access*, vol. 9, pp. 87 251–87 298, 2021.

[6] W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, "An overview of hardware security and trust: Threats, countermeasures, and design tools," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 6, pp. 1010–1038, 2021.

[7] J. C. Booth, M. L. Dowell, A. D. Feldman, P. D. Hale, M. M. Midzor, and N. D. Orloff, "5G hardware supply chain security through physical measurements," National Institute of Standards and Technology, Tech. Rep. NIST.SP.1278, 2022. [Online]. Available: https://doi.org/10.6028/NIST.SP.1278

[8] W. Enck and L. Williams, "Top five challenges in software supply chain security: Observations from 30 industry and government organizations," *IEEE Security & Privacy*, vol. 20, no. 2, pp. 96–100, 2022.

[9] T. Omitola and G. Wills, "Towards mapping the security challenges of the Internet of things (IoT) supply chain," *Procedia Computer Science*, vol. 126, pp. 441–450, 2018.

[10] C. Clancy, J. Ferraro, R. Martin, A. Pennington, C. Sledjeski, and C. Wiener, "Deliver uncompromised: Securing critical software supply chains," *MITRE Technical Papers*, vol. 24, p. 01, 2021.

[11] L. Williams, "Trusting trust: Humans in the software supply chain loop," *IEEE Security & Privacy*, vol. 20, no. 5, pp. 7–10, 2022.

[12] T. Kieras, J. Farooq, and Q. Zhu, "I-SCRAM: A framework for IoT supply chain risk analysis and mitigation decisions," *IEEE Access*, vol. 9, pp. 29 827–29 840, 2021.

[13] R. Al-Shaer, J. M. Spring, and E. Christou, "Learning the associations of MITRE ATT&CK adversarial techniques," in *IEEE Conference on Communications and Network Security (CNS)*, 2020, pp. 1–9.

[14] J. M. Batalla, E. Andrukiewicz, G. P. Gomez, P. Sapiecha, C. X. Mavromoustakis, G. Mastorakis, J. Zurek, and M. Imran, "Security risk assessment for 5G networks: National perspective," *IEEE Wireless communications*, vol. 27, no. 4, pp. 16–22, 2020.

[15] H. Chen, H. Cam, and S. Xu, "Quantifying cybersecurity effectiveness of dynamic network diversity," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 6, pp. 3804–3821, 2022.