



HAL
open science

The Challenge of Security Breaches in the Era of 5G Networking

Maria Belesioti, Jorge Carapinha, Rodoula Makri, Ioannis P. Chochliouros

► **To cite this version:**

Maria Belesioti, Jorge Carapinha, Rodoula Makri, Ioannis P. Chochliouros. The Challenge of Security Breaches in the Era of 5G Networking. 17th IFIP International Conference on Artificial Intelligence Applications and Innovations (AIAI), Jun 2021, Hersonissos, Crete, Greece. pp.106-117, 10.1007/978-3-030-79157-5_10 . hal-03789003

HAL Id: hal-03789003

<https://inria.hal.science/hal-03789003v1>

Submitted on 27 Sep 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License



This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

The Challenge of Security Breaches in the Era of 5G Networking

Maria Belesioti¹, Jorge Carapinha²,
Rodoula Makri³ and Ioannis P. Chochliouros^{1*} [0000-0002-4208-1676]

^{1*} Hellenic Telecommunications Organization (OTE) S.A.,
99 Kifissias Avenue, 15124 Maroussi-Athens, Greece

² Altice Labs, Aveiro, Portugal

³ Institute of Communication and Computer Systems (ICCS), Athens, Greece
mbelesioti@oteresearch.gr

Abstract. Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the Critical Infrastructures (CIs). 5G networks and future communications technologies radically transform the way we communicate, by introducing a vast array of new connections, capabilities and services in a multiplicity of sectors. In this scope, network function virtualization and end-to-end network slicing are two promising technologies empowering 5G networks for efficient and dynamic network/service deployment and management. Resilience of critical infrastructure systems and especially in telecommunication networks can be considered as “key factor” that can reduce vulnerability, minimize the consequences of threats as well as their cascade effects, accelerate mitigation and facilitate re-adaptation to a disruptive event. In this context, comprehensive knowledge of the complete surrounding environment and of the most important factors that affect and/or determine resilience, can evolve at a fundamental aspect concerning the case resilience of critical telecommunication. Based on this idea, the RESISTO project provides a holistic situation awareness for telecommunication infrastructures and simultaneously enhances resilience, while acting as an on top safety net boosting the faster and more reliable management enabling the digital transformation of our society and a variety of business processes. In this paper we specifically discuss the impact of the RESISTO platform when a security breach occurs in a 5G mobile network.

Keywords: 5G, Critical Infrastructure (CI), machine learning, resilience, security, threats, SDN, SDS, network virtualization.

1 Introduction

5G is a global network and services (r-)evolution that affects drastically a multiplicity of sectors in our modern societies and economies [1-2]. Through its main

technological enablers (such as cloud computing, Mobile Edge Computing (MEC), Software Defined Networking (SDN) and Network Function Virtualization (NFV)), 5G is expected to offer novel opportunities for growth and modify the features and capabilities of modern networking [3]. Among the actual challenges [4] are also those related to network and service security [5] where 5G is anticipated to change the landscape, especially as far as security of Critical Infrastructures (CIs) is concerned. To this respect, the ongoing EU-funded RESISTO [6] project will help Communications Infrastructures Operators, especially in the 5G era, to take the best countermeasures and reactive actions exploiting the combined use of risk and resilience preparatory analyses, detection and reaction technologies, applications and processes in the physical and cyber domain.

Many socioeconomic activities such as health domain, transport, telecommunications, electric energy, finance that are considered as “vital” for the proper function of the society and public safety are supported by many physical and cyber assets and systems one of which is telecommunication services. Serious disruptions of these services could cause as cascade effect, disruption in other dependent infrastructure causing major impact and discomfort in the continuity of everyday life of the society [7]. Critical Infrastructure Protection (CIP) means all activities aimed at ensuring the functionality, continuity and integrity of CIs in order to deter, mitigate and neutralise a threat, risk or vulnerability [8-9]. For this reason, an attack, either cyber or physical, in telecommunication systems may cause dangerous consequences in the physical world. Hence, resilience – together with security and reliability – are assessed as fundamental properties of both physical and cyber infrastructure aiming to ensure safety of people, of the environment and of the controlled physical processes [10]. In particular, with the actual exponential growth in wireless data traffic and demand for faster networks, network resilience is assessed as a critically important factor in emerging 5G networks [11-12]. The issue of network resilience is strongly linked to the 5G network architecture as well. In general, a convenient 5G network architecture will enable the creation of mobile networks upon virtualization platforms, by utilizing the cloud and will offer corresponding services.

Telecom operators have SOC (Security Operation Centres) for the logical protection of their infrastructure and different systems (such as CCTV, access control, intrusion detection, biometrics, etc.) for the physical security management and, in some cases, a PSIM (Physical Security Information Management) which is a category of software platform for single monitoring, increased control, improved situation awareness and management reporting through one comprehensive user interface. In each domain the systems or platforms for the protection include specific modules for the correlation of information.

However, modern 5G architectures are designed to close security gaps from previous iterations of cellular networks [13]. The SDN architecture with its separation of data and control plane from network devices drastically simplifies configuration and management of security policies, with significant reduction of security risks associated to policy inconsistency. The key concept that underpins SDN is the logical centralization of network control functions by decoupling the control and packet forwarding functionality of the network. NFV complements this vision through the virtualization of these functionalities based on recent advances in general server and enterprise IT virtualization. Considering the technological maturity of the

technologies that 5G can leverage on, SDN is the one that is moving faster from development to production [14]. NFV and SDN along with network slicing [3, 15-16] offer mobile network providers the ability to support several 5G requirements and provide related services. In fact, 5G is claimed to satisfy the dramatically growing need of users and things for the imminent 2020 horizon and beyond. More specifically, in the 5G scope we identify (Fig.1) three major groups of use cases, namely [17]: (i) enhanced mobile broadband (eMBB) focusing on services with high requirements for bandwidth, such as streaming high definition (HD) videos, Virtual Reality (VR) and Augmented Reality (AR); (ii) ultra Reliable and Low-Latency Communications (uRLLC) aiming to support multiple advanced services for latency-sensitive connected devices (such as factory automation, autonomous driving and the PPDR use cases or robotic surgeries) and, finally; (iii) massive Machine-Type Communications (mMTC) are about services that include high requirements related to connectivity provision in huge numbers of devices (such as sensors that typically transmit and receive only small amount of data sporadically); an mMTC network is designed to support of up to 1 million devices per square km, which is 10 times the maximum amount currently possible with 4G LTE.

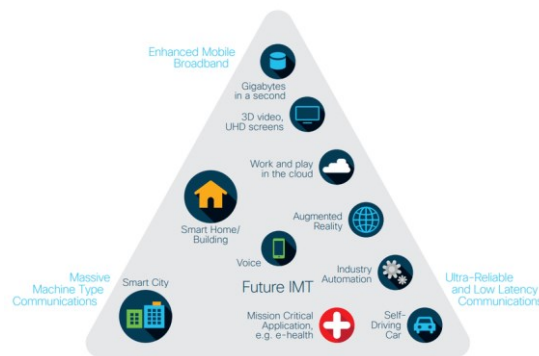


Fig. 1. 5G services and opportunities [18].

Each virtualized network slice consists of a number of Virtual Network Functions (VNFs) each one providing predefined services in its slice and all the VNFs of a slice collectively provide wireless network access to the Users' Equipment (UEs) attached to that slice. However, although SDN and virtualization bring significant innovation in the communication networks by expanding their services offering, they also open a wide window to new source of attacks [19-20]. At the same time, physical security continues to be an open challenge when it comes to the protection of the physical infrastructure's integrity as a whole, due to the increased complexity of the networks architecture further extended with pervasive use of IoT (Internet of Things).

Section 1 serves as an introduction to 5G opportunities, in parallel with the intended support of CIs; in particular we identify the importance of network resilience and security in modern network infrastructures such as those promoted by the 5G enabling technologies. Section 2 discusses the fundamental architecture proposed by the RESISTO project and further assesses the roles of the main entities composing the essential RESISTO platform. Section 3 attempts to briefly introduce several aspects

originating from the modern 5G threat landscape under a more generalised context, by focusing on selected use case about network response to a security breach. The work summarizes with some concluding remarks.

2 Main Entities of the RESISTO Platform

A critical issue in service delivery in a 5G network is its resilience [21-22]. 5G provides preventative measures to limit the impact to known threats, but the adoption of new network technologies introduces potential new threats that telecom operators need to face [23]. In 5G, “build first and secure later” typical paradigm should be replaced by “security and resiliency by design” and “security and resiliency by operation”. Thus 5G networks should be designed in such a way that security and resilience are taken into account as a cornerstone feature in both design and operation stages [24]. The RESISTO concept [6] has been envisioned from the assumption that by combining physical and cyber security assessment and (up to real time) management within interacting operating tools, improved business and asset continuity can be further protected. RESISTO develops a cooperation framework that allows different parts of the overall Communication CI security personnel to exchange data and signals, to recognize complex attack patterns coming from different sources at different levels and, based on real time simulation of attack propagation within the CI and across interconnected CIs, to select and implement the best response and, in case of failure, the optimal mitigation strategy [25].

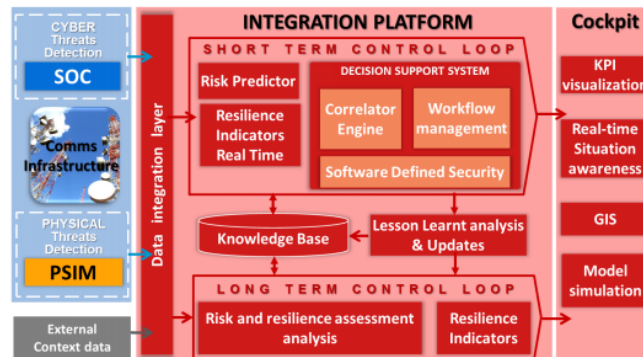


Fig. 2. RESISTO High level architecture.

The RESISTO project has thus developed an innovative architecture (as depicted in Fig.2) aiming to “face” the challenges posed by recent 5G advances [26-28]. The main element of this architecture is the RESISTO Cockpit which acts as the main user-interface providing the users real-time situation awareness of potential threats and alarms and related data, along with indicators to assess the resilience of the infrastructure. An additional important element is the model simulation for interdependency analysis that allowing to simulate the impact of the identified threats on the modelled infrastructure and to evaluate potential cascading effects. We also

have the Geo-referenced data representation on a map, derived from sensors warning about critical events and data processed from the integrated systems to enhance real-time knowledge of potential critical situation.

The Long-Term Control Loop is in charge of defining the configuration of the system, according to the security assessment and updating it on a periodic basis or when specific events take place (new threats or discovery of previously undetected vulnerabilities). It mainly consists of: (i) the “Risk and resilience assessment analysis” that identifies the context, analyses the interdependencies (physical, cyber, logical and geographic) and risks, assesses these risks and suggests the risk treatment, and; (ii) “Resilience Indicators” as summing up the resilience of CI communication in its operational phase.

Besides, RESISTO’S Short-Term Loop is another element of high importance into the related architecture. It is in charge of promptly responding to attacks and threats that may “impact” the operational life of the system. This element is essentially based on the following components:

- The “Risk Predictor” that evaluates the impacts of exploitations and countermeasures. In particular, this component gathers data on anomalies and security attacks from the physical domain (PSIM-C), the cyber domain (SOC), and the Correlator Engine, while it predicts the effects of countermeasures on the CI, accounting for interdependencies among virtual and physical domains. Moreover, it models the interdependencies of CI elements, with the simulation of the short-term effects of failure, both in terms of faults propagation and with respect to performance degradation.
- The “Resilience Indicators in Real-Time”, which are a real-time set of indicators that measure in the risk and resilience of the communication infrastructure derived as output of the “Risk and resilience assessment analysis”.
- The “Decision Support System” which consists of several distinct parts. One of them, the “Correlator Engine”, is maybe the most important part of the Short-Term Control Loop. This is a rule-based engine customized to detect threats, alarms, critical events defined by the “Risk and resilience assessment analysis” and the “Interdependency analysis” able to detect critical situations to manage. The correlator engine consists of two components namely: (i) an event stream processing module in order to identify threats and dangerous situations through the analysis of heterogeneous data sources in real-time by using several event correlation techniques, such as temporal correlation (based on event time) and logical – or causal – ones, and; (ii) the machine learning (ML) algorithms module in order to analyze the behavior of the RESISTO platform and the phenomena affecting the system, so that to make decisions, accordingly. The results of the application of ML algorithms can enhance the way the RESISTO platform detects dangerous situations by means of the correlation and definition of new rules and thresholds which trigger alarms. This module is also able to build intelligent defense models to prevent damages created by cyber-attacks. In this regard, the use of classification algorithms (e.g. Artificial Neural Networks) for analyzing the network traffic, inspecting the system logs and correlating these data with the monitoring of resource utilization of the systems, can lead to significant improvements in detecting anomalies and attacks, occurring over the communications network. The Correlator is a logically centralized entity.

However, it can take advantage of the NFV and SDN of the underlying communication network to enable seamless distribution of detection and analysis functions among several geographical dispersed points of presence (such as data centers), creating the means to implement fog/-computing topologies.

The Correlator also triggers the Workflow Management software engine in charge to guide the operator during the reaction phase. On the basis of the alarm type, the most appropriate workflow is selected and executed. A workflow is a conditional sequence of steps and each separate step can specify a procedural action, drive a physical actuator, carry out a complex action on the communication network, isolate a faulty or attacked component, reconfigure a part of the network, disable a 5G slice, etc.

Another important part is the Software Defined Security (SDS), which is a sort of a reaction/resilience mechanism that performs a dynamic, flexible reconfiguration of security/resilience mechanisms and relocation (virtualization) of security functions, in a way similar to what currently done in SDN. SDS integrates mitigation and resiliency functionalities into a unique framework able to dynamically and proactively react to the evolving threats by enforcing the most appropriate security policies in each CI node. Such framework is fed by an appropriate Decision Support System (DSS) taking the data stored into the Knowledge Base as valuable input parameters.

Based on an Integrated Risk and Resilience analysis management and improvement process [29-30] availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative DSS to protect communication infrastructures from combined cyber-physical threats exploiting the SDS model on a suite of state-of-the-art cyber/physical security components (i.e.: blockchain, machine learning, IoT security, airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. The involvement of communications operators in the RESISTO framework will allow the implementation of a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences and cascading effects, in particular by bouncing efficiently back to original and forward to operational states of operation.

3 The 5G Threat Landscape

The 5G era has already arrived, bringing faster speeds and lower latency thus enabling a complete new business sector and also offering innovative applications. Although the 5th generation of communications is more robust than its predecessors, when it comes to security the high complexity of 5G infrastructures as well as the overarching nature of 5G, make it not easy to manage [31-32]. The lack of information since existing deployments are still evolving and the large number of potential stakeholders involved makes the assessment of cyber threats a hard task. On the other hand, the involvement of several stakeholders which play different roles in

the 5G ecosystem, will foster the effort for security assurance of the network at different levels and separate layers [24, 33].

According to the 5G-PPP White Paper on the 5G architecture [34], the list of stakeholder roles in the 5G ecosystem is the following: (i) Service customers (SCs); (ii) Service Providers (SPs); (iii) Mobile Network Operators (MNOs) also known as Network Operators (NOPs); (iv) Virtualization Infrastructure Service Providers (VISPs), and; (v) Data Centre Providers (DCPs). Complementary to stakeholders, 5G spans in many vectors through which adversaries can attack. One of the most important concerns regarding threats are posed by telecommunication operators as critical infrastructure operators, which are evolving their networks using 5G technology for critical services. 5G will utilize more ICT components and services while, at the same time, people, companies and organizations will “build” their everyday activities on 5G services potentially increasing network vulnerabilities. In addition it is a fact that as 5G will be deployed based upon 3G and 4G LTE already deployed mobile networks, deployment actions are carrying part of legacy vulnerabilities in terms of security [33, 35-36].

3.1 5G Network Response to a Security Breach

The complexity added by 5G requires traditional (i.e. preconfigured) security solutions to be supplemented and reinforced with dynamic mechanisms, instantiated and deployed by AI-based systems [37]. Thus, early and integrated threat detection is a key requirement and strongly affects both 5G network deployment and behaviour. Complex mechanisms based on a combination of big data and ML can be used to identify threats not spotted by conventional solutions supported by basic filters.

In addition, prompt reaction is also a key requirement. 5G provides a number of tools to avoid or mitigate the effects of security and resilience threats, which are mainly related to the capability to detach network functions from the infrastructure and flexibly control the lifecycle of network services. The independence between network and infrastructure, which strictly speaking is not enabled by 5G, but rather the virtualization of network resources, paves the way to the definition of innovative security use cases [32, 33]. Network slicing is the main enabler and catalyst to properly deliver those use cases. The combination of AI-based detection tools with network slicing provides new possibilities to prevent or mitigate many of the security and resilience threats in telco infrastructures, especially for 5G, and is likely to represent a relevant research topics in the next few years [21, 24]. The use case described in this section hopefully illustrates the synergies that can be obtained through the combination of these two technological trends.

The proposed use case [38] aims to showcase the vulnerabilities of 5G Communication Networks considered as Critical Infrastructures and how the RESISTO platform aims to deal with these challenges. The increasing complexity of the 5G architecture and the extensive use of programmable platforms are the key elements of high concern, in the proposed scope.

Network slicing is an important tool to provide isolated networks, each optimized for specific types of traffic characteristics. One such characteristic could be related to security and safety requirements – by means of slicing, it will be possible to

dynamically confine the impact of security requirements to single slices, rather than the whole network. In addition, new recovery mechanisms are enabled by network slicing, especially the capability to establish network resources on-demand. This use case [38] comprises a mission-critical (MC) scenario based on a 5G telecommunication mobile network in which the probability of an ongoing cyber/physical attack or equipment failure is assessed by continuous analysis of specific parameters (e.g. temperature) or abnormal behaviour, making use of machine learning techniques. The use case definition is based on the execution of different actions depending on the perceived probability of equipment failure.

We consider a SP that builds and operates a network slice based on own resources – core network, core DC (hosting the majority of the 5G Core components), coloured black in Fig.3, as well as resources leased from an independent Network Slice Subnet Provider (NSSP A) – C-RAN and edge components, coloured green in Fig.3. For the purposes of the use case, a second NSSP (NSSP-B) having a business relationship with the SP, is also able to provide C-RAN and edge components if/when needed (e.g. for reasons of malfunction or quick traffic growth), but not active by default.

Phase 1 (preparation): The use case is triggered when the probability of service loss affecting resources run by NSSP-A goes above a certain threshold, e.g. 35% (possible cause – temperature rising in Edge Point-of-Presence (PoP)). The event may be accidental, caused by a natural event or by a malicious action. At this stage, the risk is classified as low to medium. The preparation of a smooth transition from NSSP-A to NSSP-B is started through the creation of a slice subnet (C-RAN, Edge, x-haul) dimensioned according to the number of users. Recovery mechanisms (e.g. equipment restart) if available and feasible, are attempted. The SP requests NSSP-B to instantiate an edge slice subnet, in case a relocation of resources from NSSP-A proves to be necessary as a result of the identified issue.

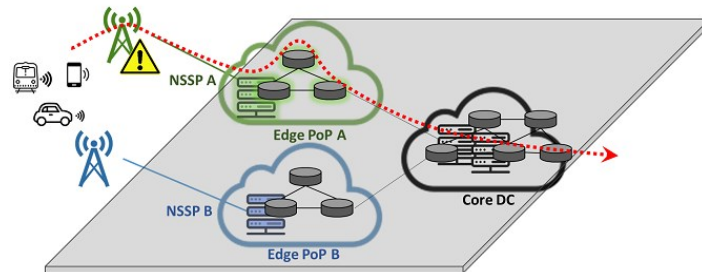


Fig. 3. 5G Network Response to a Security Breach – Activation phase.

Phase 2 (activation): When the service loss probability goes above a second threshold (e.g. 50%), the risk is classified as high. The slice subnet that had been instantiated in the previous step is activated at this point (colored blue in Fig.3). This includes the activation of all Virtual Machines (VMs)/containers, as well as the virtual links. At the same time, non-essential resources are shutdown.

Phase 3 (migration): When a third service loss probability threshold (e.g. 65%) is exceeded then actuation/mitigation and is triggered. The affected C-RAN and edge

components are relocated from NSSP A to NSSP B; however, the service interruption should not be noticed from the customers. This is illustrated in Fig.4, below.

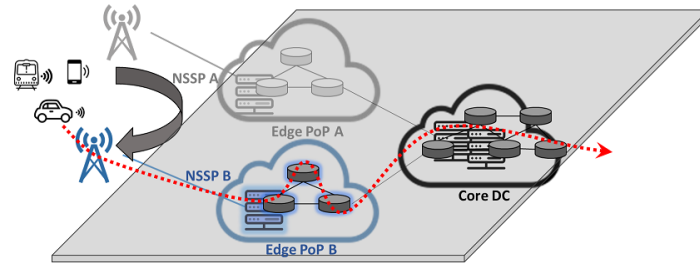


Fig. 4. 5G Network Response to a Security Breach – Mitigation phase.

In a 5G environment, the actuation phase takes advantage of network slicing and the capability to deploy network services on demand. In this case, the affected resources (i.e. those provided by NSSP A) should be deactivated and replaced by different resources in such a way that service continuity can be guaranteed.

In this use case, the assets affected are the NSSPs and, as a consequence, the SP. The SP has a key role and provides communication services to end-users, supported by network slices. The SP is also supposed to provision of the network, thus it is also able to perform the role of Network Slice Provider (NSP). A network slice can be composed of multiple network slice subnets (e.g. core, edge). Each slice subnet may be owned and operated by the SP, or by an independent NSSP (Network Slice Subnet Provider). The security threat vectors in 5G will be multi-dimensional, as 5G networks will connect infrastructures, interconnect societies and industries, providing anything-as-a-service, and integrate new models of service delivery. Since 5G has higher flexibility and agility, NFV and SDN play a vital role in 5G [39].

The virtualization of network resources, and especially network slicing, enable the definition of new business models based on new stakeholders and roles. In this context, the definition of any 5G use case should be understood under a specific business ecosystem, where different players are responsible for playing different roles [40]. The use case described above is based on novel 5G business models enabled by Network as a Service (NaaS) and the separation of service providers and (virtual) infrastructure providers. In addition, the possibility of sharing mobile access/edge network resources among competitor operators under certain circumstances (e.g. natural events such as forest fires affecting the availability of the mobile network in a certain zone) has been suggested for possible implementation as a way to avoid loss of communication, which is often a cause for aggravation of the related effects.

The discussed use case demonstrates how the RESISTO platform can be used to mitigate the following risks, among others: (i) Service delivery failure in a geographical area, as a result of intentional malicious actions (e.g. cyber-physical attacks, motivated either by terrorism and economic sabotage), equipment malfunctions or natural events (e.g. forest fire, potentially endangering significant components of the network infrastructure physically located on that zone); (ii) financial losses, both to operators (loss of income, customer churn) and end users

(especially businesses for which communication is a critical requirement); (iii) damages caused by network disruptions, especially in emergency scenarios, potentially exposing human lives to risk. The most significant contribution of RESISTO is on the decision-making process.

The innovations of the use case are mainly related to the combined use of two types of tools for security threat detection and mitigation, respectively: (i) Artificial Intelligence (AI) / ML-based detection mechanisms for early detection of security threats, and; (ii) network automation and programmability, enabled by 5G cornerstones such as network virtualization, software defined networking and network slicing. This use case is expected to evaluate and demonstrate the preparedness of the RESISTO platform to handle the specific challenges of 5G and the ability to exploit the 5G features mentioned above in scenarios of cyber-physical attacks or natural events.

4 Discussion

5G will provide super-high data rates, better quality of service and very low latency through dense base station deployments. Communities will rely on 5G far more than ever compared to previous communications systems. Factories, businesses and critical infrastructure will all rely on 5G data connectivity, and this technology will transform business. The diffusion of Software Defined Network (SDN), slicing and virtualization techniques, the use of programmable platforms will become pervasive. However, although SDN brings significant innovation in terms of adaptability, new source of attacks appear in the horizon. At the same time physical security represents an open challenge when it comes to protection of physical infrastructure integrity as a whole due to the increased complexity of the 5G architecture.

The management of security and resilience of critical infrastructures based on 5G will constitute one of the most important challenges of the years to come, as both of these network features can strongly influence design and operation of the corresponding infrastructure. In particular, the dynamicity and the softwarized environment in which the future infrastructure will be deployed will need intelligent prevention and mitigation strategies that RESISTO platform can sufficiently offer on top of telco operators' security systems. This platform also fits for the support of 5G modern deployments and behaviour as explained for a selected use case of 5G network response to a security breach.

Acknowledgments. The paper has been based on the context of the “RESISTO” (“RESilience enhancement and risk control platform for communication infrastructure Operators”) Project, funded by the EC under the Grant Agreement (GA) No.786409.

References

1. Rost, P., Banchs, A., Berberana, I., Reitbach, M., Doll, M., et al.: Mobile Network Architecture Evolution toward 5G. *IEEE Communications Magazine* **54**(5), 84-91 (2016)
2. Agiwal, M., Roy, A., et al.: Next Generation 5G Wireless Networks: A Comprehensive Survey. *IEEE Communications Surveys Tutorials* **18**(3), 1617--1655 (2016)
3. Chochliouros, I.P., et al.: Enhancing Network Management via NFV, MEC, Cloud Computing and Cognitive Features: The “5G ESSENCE” Modern Architectural Approach”. In: *Proceedings of AIAI-2018, AICT 520*, pp.1--12. Springer, Cham (2018)
4. Next Generation Mobile Networks (NGMN) Alliance: NGMN 5G White Paper. NGMN Alliance (2015)
5. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., et al.: 5G: Security analysis of threats and solutions. In: *Proceedings of CSCN-2017*, pp.193--199. IEEE (2017)
6. RESISTO (“RESilience enhancement and risk control platform for communication infraStructure Operators”) H2020 Project (Grant Agreement No.786409). <http://www.resistoproject.eu/>
7. Setola, R., Luijff, E., and Theocharidou, M.: Critical Infrastructures, Protection and Resilience. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds.), *Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control*, vol.90, pp.1--18. Springer, Cham (2018)
8. European Commission: Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, SWD(2013) 318 final, 28.08.2013. <http://ec.europa.eu/transparency/regdoc/rep/10102/2013/EN/10102-2013-318-EN-F1-1.PDF>.
9. Council of the European Union: Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal L345, pp.75--82 (2008)
10. Aziz, F.M., et al.: Resilience of LTE Networks against Smart Jamming Attacks: Wideband Model. In: *Proceedings of the IEEE PIMRC 2015*, pp. 1344--1348. IEEE (2015)
11. Abhishek, R., Tipper, D., and Medhi, D.: Network Virtualization and Survivability of 5G Networks: Framework, Optimization Model, and Performance. In: *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps)*, pp. 1--6. IEEE (2018)
12. Abhishek, R.: Resilience and Survivability of 5G Networks. Ph.D. Thesis, University of Missouri-Kansas City, USA. Proquest LLC (2020, May)
13. 5GAmericas: Security Considerations for the 5G Era - A 5GAmericas' White Paper (2020, July)
14. European Union Agency for Cybersecurity (ENISA): Threat Landscape for 5G Networks. ENISA (2020, December)
15. Nguyen, V.-G., Brunstrom, A., Grinnemo, K.-J., and Taheri, J.: SDN/NFV-based mobile packet core network architectures: A survey. *IEEE Communications Surveys and Tutorials* **19**(3), 1567--1602 (2017)
16. Olimid, R.F., and Nencioni, G.: 5G Network Slicing: A Security Overview. *IEEE Access* **8**, pp. 99999-100009 (2020)
17. International Telecommunication Union – Radiocommunications Sector (ITU-R): Recommendation ITU-R M.2083-0 (09-2015): “*IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*”. ITU-R (2015)
18. Geller, M., and Nair, P.: 5G Security Innovation with Cisco – White Paper (2018)
19. GSM Association (GSMA): Migration from Physical to Virtual Network Functions – Best Practices and Lessons Learned Version 0.1. GSMA (2018, October)
20. The 3rd Generation Partnership Project: 3GPP TR 33.848 V0.5.0 (2019-11): Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and

- System Aspects; Security Aspects; Study on Security Impacts of Virtualisation (Release 16). 3GPP (2019)
21. Taleb, T., Ksentini, A., et al.: On Service Resilience in Cloud-native 5G Mobile Systems. *IEEE Journal on Selected Areas in Communications (JSAC)* **34**(3), 483--496 (2016)
 22. Sterbenz, J.P.G., Çetinkaya, E.K., Hameed, M.A., Jabbar, A., et al.: Evaluation of Network Resilience Survivability and Disruption Tolerance: Analysis Topology Generation Simulation and Experimentation. *Telecommunications Systems* **52**, 705--736 (2013)
 23. Xie, L., et al.: Network survivability under disaster propagation: Modeling and analysis. In: *Proceedings of the IEEE WCNC-2013*, pp. 473--4735. IEEE (2013)
 24. Arfaoui, G., et al.: Security and Resilience in 5G: Current Challenges and Future Directions. In: *2017 IEEE Trustcom/BigDataSE/ICSS*, pp. 1--8. IEEE (2017)
 25. Yusta, J.M., Correa, G.J., and Lacal-Arantequi, R.: Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy*, **39**(10), 6100--6119 (2011)
 26. Belesioti, M., Chochliouros, I.P., et al.: Enhancing Critical Infrastructure Protection: The RESISTO Concept. In: *Proceedings of EuCNC 2018*, pp. 591--592. IEEE (2018)
 27. Belesioti, M., Makri, R., Fehling-Kaschek, M., Carli, et al.: A New Security Approach in Telecom Infrastructures: The RESISTO Concept. In: *Proceedings of the DCOSS-2019/SecRIoT-2019 Workshop*, pp. 212--218. IEEE Computer Society (2019)
 28. RESISTO Project: Deliverable 2.7: "RESISTO Platform and Tools Reference Architecture-final" (2019, December)
 29. Häring, I., Sansavini, G. Bellini, E., Martyn, N., Kovalenko, T., et al.: Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures and Case Studies. In: I. Linkov and J.M. Palma-Oliveira (eds.), *Resilience and Risk: Methods and Applications in Environment, Cyber and Social Domains*, pp. 21--80. NATO Science for Peace and Security Series C: Environmental Security, Springer, Dordrecht (2017)
 30. Bellini, E., and Ferreira, P.: Managing interdependencies in critical infrastructures - A cornerstone for system resilience. In: S. Haugen, A. Barros et al. (eds.), *Safety and Reliability – Safe Societies in a Changing World*, 2687--2692. CRC Press (2018)
 31. Dutta, A., and Hammad, E.: 5G Security Challenges and Opportunities: A System Approach. In: *Proceedings of the 2020 IEEE 3rd 5G World Forum (5GWF)*, pp. 109--114. IEEE (2020)
 32. Fang, D., Qian, Y., and Hu, R.Q.: Security for 5G Mobile Wireless Networks. *IEEE Access* **6**, 4850--4874 (2017)
 33. Cao, J., Ma, M. Li, H., Ma, R., Sun, Y., et al.: A Survey on Security Aspects for 3GPP 5G Networks. *IEEE Communications Surveys & Tutorials* **22**(1), 170--195 (2020)
 34. 5G Public Private Partnership (5G-PPP): View on 5G Architecture – White Paper, Version 3.0. 5G-PPP (2019, June)
 35. Khan, R., Kumar, P., Jayakody, D.N.K., and Liyanage, M.: A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future directions. *IEEE Communications Surveys and Tutorials* **22**(1), 19--248 (2019)
 36. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., et al.: Overview of 5G Security Challenges and Solutions. *IEEE Communications Standards Magazine* **2**(1), 36--43 (2018)
 37. 5GAmericas: The Evolution of Security in 5G - White Paper (2019, July),
 38. RESISTO Project: Deliverable 2.8: "Table-Top Read Teaming Results of RESISTO Architecture, Scenarios and Use Cases Tabular Report" (2020, January)
 39. Liyanage, M., Ahmad, I. Bux Abro, A., Gurtov, A., and Ylianttila, M.: *Comprehensive Guide to 5G Security*. Wiley (2018)
 40. The 3rd Generation Partnership Project: 3GPP TR 28.801 v15.1.0: "Technical Report Technical Specification Group Services and System Aspects; Telecommunication management; Study on management and orchestration of network slicing for next generation network (Release 15)". 3GPP (2018)