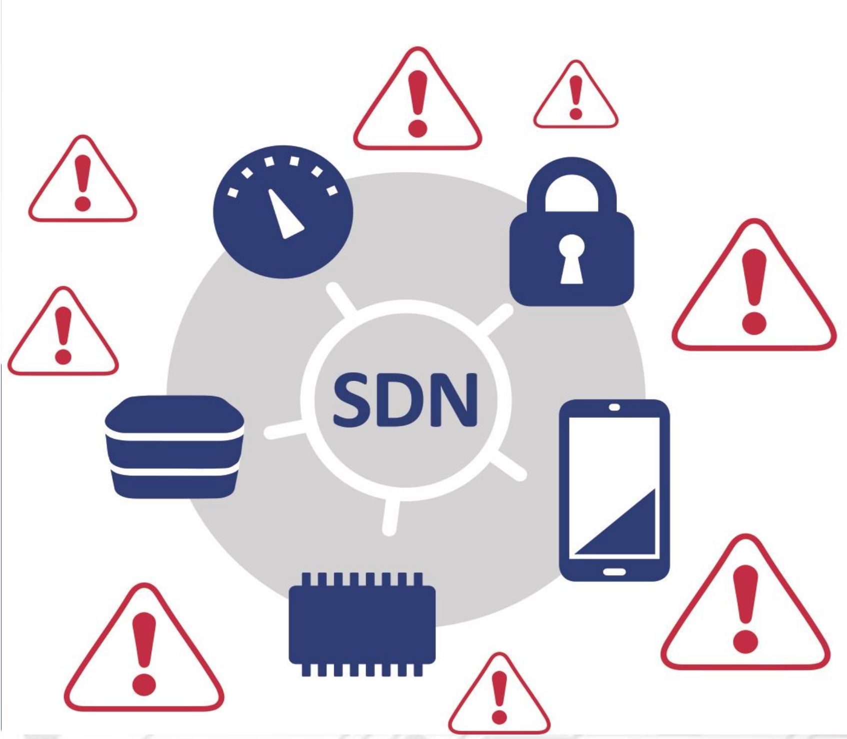

Threat Landscape and Good Practice Guide for Software Defined Networks/5G

DECEMBER 2015

www.enisa.europa.eu

European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Adrian Belmonte Martin (ENISA), **Louis Marinos** (ENISA), **Evangelos Rekleitis** (ENISA), **George Spanoudakis** (City University London), **Nikolaos Petroulakis** (City University London)

Editors

European Union Agency for Network and Information Security
ENISA responsible officer: **Adrián Belmonte Martín**
For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to express our gratitude to the following individuals for providing valuable comments as external reviewers of the report:
Lorenzo Di Gregorio (InnoRoute GmbH**), Giuseppe Bianchi** (CNIT / Univ. Roma Tor Vergata), **Eduardo Jacob** (University of the Basque Country)

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-161-8, DOI: 10.2824/67261

Table of Contents

Executive Summary

5G[1] represents the next major phase of mobile telecommunication systems and network architectures beyond the current 4G standards, aiming at extreme broadband and ultra-robust, low latency connectivity, to enable the programmable connectivity for the *Internet of Everything*[2]. Despite the significant debate on the technical specifications and the technological maturity of 5G, which are under discussion in various fora[3], 5G is expected to affect positively and significantly several industry sectors ranging from ICT to industry sectors such as car and other manufacturing, health and agriculture in the period up to and beyond 2020.

5G will be driven by the influence of software on network functions, known as *Software Defined Networking* (SDN) and *Network Function Virtualization* (NFV). 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.

To realize the business potential of SDN/5G, a number of technical issues related to the design and operation of Software Defined Networks need to be addressed. Amongst them, SDN/5G security is one of the key issues, that needs to be addressed comprehensively in order to avoid missing the business opportunities arising from SDN/5G.

In this report, we review threats and potential compromises related to the security of SDN/5G networks. More specifically, this report contains a review of the emerging threat landscape of 5G networks with particular focus on Software Defined Networking. It also considers security of NFV and radio network access. To provide a comprehensive account of the emerging threat SDN/5G landscape, this report has identified related network assets and the security threats, challenges and risks arising for these assets. Driven by the identified threats and risks, this report has also reviewed and identified existing security mechanisms and good practices for SDN/5G/NFV, and based on these it has analysed gaps and provided technical, policy and organizational recommendations for proactively enhancing the security of SDN/5G.

This report proposes 6 technical recommendations and 3 organizational recommendations:

- Technical Recommendations
  - Recommendation 1 (for Network providers): Mandate encryption and authentication in NBI, SBI and EWBI.
  - Recommendation 2 (for Network providers): Identify and monitor exposed functionalities of SDN controllers.
  - Recommendation 3 (for Network and Service providers): Control and monitor running application resources.
  - Recommendation 4 (for Network, Service providers and End users): Holistic Support for Security policies.
  - Recommendation 5 (for Administrators): Access control and Credentials enforcement
  - Recommendation 6 (for Developers): Application Isolation and Sandboxing.

[1] www.5g-ppp.eu/roadmaps
[2] http://ioeassessment.cisco.com/
[3] http://www.3gpp.org/news-events/3gpp-news/1734-ran_5g

- Organisational Recommendations
  - Recommendation 7 (for Service providers): Develop incident response capabilities and information sharing practices among telecom operators.
  - Recommendation 8 (for Administrators): Keep systems up to date
  - Recommendation 9 (for Network and Service providers): Use adequate security methods

1. Introduction

Software Defined Networking (SDN) is a new network paradigm moving rapidly from development to production environments. The key concept of the new paradigm is the decoupling of the control and packet forwarding functionality of the network. In classic networks, these two functionalities were the responsibility of the forwarding devices of the network. In SDN, these two functionalities have been separated into two functionality planes: the control plane and the data plane. The separation of these two functionality planes in SDNs has two significant consequences: (a) it reduces the difficulty in the configuration and alteration of the control functions of the network, as this functionality has no longer the responsibility of the forwarding devices of the network that tend to have proprietary implementations (e.g., operating systems), and (b) it enables the implementation of more consistent control policies through fewer and uniformly accessible controllers.

The concept of SDN has been around for many years having its roots in “active programmable networking” in academic research and the research literature[4]. In contrast to the early incarnations of SDN, the “modern” SDN realisation paradigm completely separates the Control and Data planes for increased functionality, control and programmability.

The potential benefits of SDN have attracted the interest of the wider IT community with many parties realigning the still “cloudy” concept of SDN, to fit their purposes. A large number of research and scientific reports, which are discussed in this report, have already been published reciting the architecture of SDN and the potentially benefits on simple and complex network Infrastructures. In summary, SDN is seen as a means of providing a more efficient, extremely flexible, cost effective, and potentially fully automated holistic network management and provisioning.

1.1 Policy Context

The value of threat analysis and emerging trends in cyber security is prioritized in the Cyber Security Strategy for the EU[5]. The ENISA Threat Landscape is aligned with this EU strategy and aims to contribute by identifying emerging trends in cyber-threats and analysing the evolution of cyber-crime (see ENISA’s report on Understanding the Importance of the Internet Infrastructure in Europe[6]).

Moreover, in the new ENISA regulation[7] the need of analysing current and emerging risks is highlighted. The new ENISA regulation stipulates that “the Agency, in cooperation with Member States and, as appropriate,

[4] Psounis, Konstantinos. "Active networks: Applications, security, safety, and architectures." Communications Surveys, IEEE 2.1 (1999): 2-16.

[5] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[6] ENISA, “Understanding the Importance of the Internet Infrastructure in Europe”, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/guidelines-for-enhancing-the-resilience-of-ecommunication-networks

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

with statistical bodies and others, collects relevant information". More specifically, it is stated that it should "enable effective responses to current and emerging network and information security risks and threats".

Therefore it is evident that the ENISA Threat Landscape makes a significant contribution to the EU Cyber Security Strategy, as it streamlines and consolidates available information on cyber-threats and their evolution.

This study on "Software Defined Networks Threat Landscape and Good Practice Guide" is one of the deliverables ("*WPK1.1-D2: Risk Assessment on two emerging technology/application areas*" that focuses on SDN/5G) foreseen in the ENISA Work Programme 2015[8], which aims to provide a contribution in the assessment of the exposure to cyber threats of the envisioned 5G networks with particular focus on their backbone networking technology represented by Software Defined Networking. As such, it contributes in the definition of the current state of the art as far as cyber security is concerned in this domain and it directly contributes to the cyber security assessment by addressing industry concerns in the area.

1.2 Scope

This report contributes to the definition of a threat landscape, which is an overview of current and emerging threats applicable to the SDN/5G technologies and their associated trends. Since 5G is a general term that integrates various networking technologies with different technological maturity, this study focuses on backbone network operation technologies, i.e., Software Defined Networking. Around these core technologies, other integral components of 5G, including radio access and NFV are also discussed. This discussion, however, is scoped by the relation of these other 5G components to SDN.

The goal is to identify threats and needs for enhancing the security of 5G networks with particular focus on SDN, and to provide good practices and recommendations for threats that are considered important.

1.3 Target Audience

This report can be useful to carry out detailed threat analyses and risk assessments for telecom operators and service providers according to their particular needs and mandate (e.g., protect specific based on asset impact analysis, respond to specific vulnerabilities with customized mitigation measures etc.). The threat exposure of SDN/5G that is presented in this study may be deepened by telecom operators through their own further threat analysis and risk assessment. Where this is necessary, the aim of this report is to provide a generic, yet comprehensive, set of asset and threat details that can serve as a starting point for further analysis. Deeper analysis may also be informed by the assessed threats, vulnerabilities, and impact statements of this report in as far as they are relevant to the concrete assets deployed by the particular telecom operators.

Moreover, the SDN/5G threat landscape presented in this report may be useful to policy-makers for understanding the current state of threats and respective mitigation practices and measures. The threat

[8] "ENISA Work Programme 2015", https://www.enisa.europa.eu/publications/programmes-reports/amending-work-programme-2015

landscape identified in this report may support policy actions in the areas of 5G networks, SDN, NFV, cyber security, critical infrastructure protection, Internet of Things[9] and Industrial Internet.

Furthermore, the SDN/5G security and threat research and technology reports collected and analysed by this study provide a comprehensive collection of information regarding related cyber security threats. To this end, this report targets also individual researchers, who might want to obtain access to these identified sources in order to use them for their own research purposes.

1.4 Structure of this document

The remainder of this report is organised as follows:

Chapter 2 gives insight into the methodology adopted for conducting this study.

Chapter 3 presents the architectural framework of SDN and describes the separation of control and forwarding functions, logically centralized network control elements and programmable interfaces at multiple levels.

Chapter 4 presents the SDN/5G asset types identified in our study by giving an overview of them and identifying their dependencies in the form of a mind map.

Chapter 5 presents a taxonomy of the threat types that our analysis has shown for the identified assets. Interrelated threats have been grouped to form a taxonomy that is presented as mind map.

Chapter 6 introduces the threat agents of SDN/5G.

Chapter 7 reviews existing and emerging (i.e., under development) practices for mitigating the identified threats. It also identifies and analyses the gaps identified in addressing current and emerging threats.

Chapter 8 provides technical and organisational recommendations arising in the context of our study.

Finally, Chapter 9 provides concluding remarks.

The report includes also three annexes, containing more detailed information on SDN/5G assets (Annex A) and their taxonomy (Annex B), and SDN/5G threats (Annex C). The provision of more detailed material as annexes was necessary in order to keep the size of the report within reasonable boundaries, and at the same time give to interested stakeholders access to more comprehensive lists of SDN/5G assets and threats.

A general note that is important to make prior to the rest of this report is that all material, which has been referenced by a URL in footnotes was last accessed on the day of publication of this study.

[9] Petroulakis, Nikolaos E., et al. "A privacy-level model of user-centric cyber-physical systems." Human Aspects of Information Security, Privacy, and Trust. Springer Berlin Heidelberg, 2013. 338-347.

2. Methodology

The methodology adopted in this study is in line with the methodology introduced in the ENISA's Cyber Threat Landscape.[10] According to this methodology, someone has first to identify valuable assets and then perform a risk assessment, which identifies the necessary protection levels for these assets. Subsequently, security measures that can achieve the required protection levels by mitigating fully or partly the assessed risks are identified. Any risks, which are not addressed by these measures, might be transferred or accepted. The elements of risk are graphically depicted in Figure 1.

Threats have a key role in defining the risk assessment especially when considering the components of risks. ISO 27005, the widely adopted standard in the area defines that risks emerge when: "Threats abuse vulnerabilities of assets to generate harm for the organization".

Following this methodology, we have identified assets, threats, existing and emerging security measures for SDN/5G. These constitute the core of the SDN Threat Landscape and Good Practice Guide (STL) presented in this report. Based on this core, we have also identified gaps that originate from non-mitigated threats and provided relevant recommendations. An additional key element of our methodology is that identification and analysis has been based on a study of the related literature, without attempting any experimental or other form of validation of the claims made within this literature.

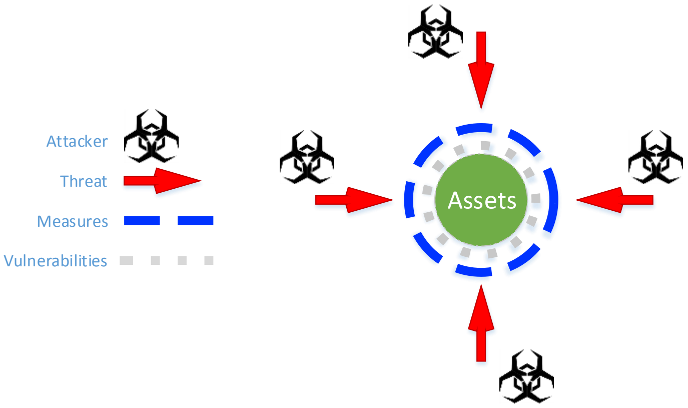

Figure 1 - Elements of risks

Furthermore, this study does not consider the use of any specific SDN equipment or the operational processes and services. Thus, it has not been possible to make a detailed and quantitative assessment of the impact and vulnerabilities of assets. Such activities could only be performed by asset owners and would probably require supporting tools for carrying out more comprehensive risk assessments in complex environments.

[10] "ENISA Threat Landscape 2014", https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

3. SDN/5G Architecture

3.1 SDN Architecture

The main principle that underpins an SDN's architecture can be summarized as the separation of control and forwarding functions, logically centralized network control elements and programmable interfaces at multiple levels.

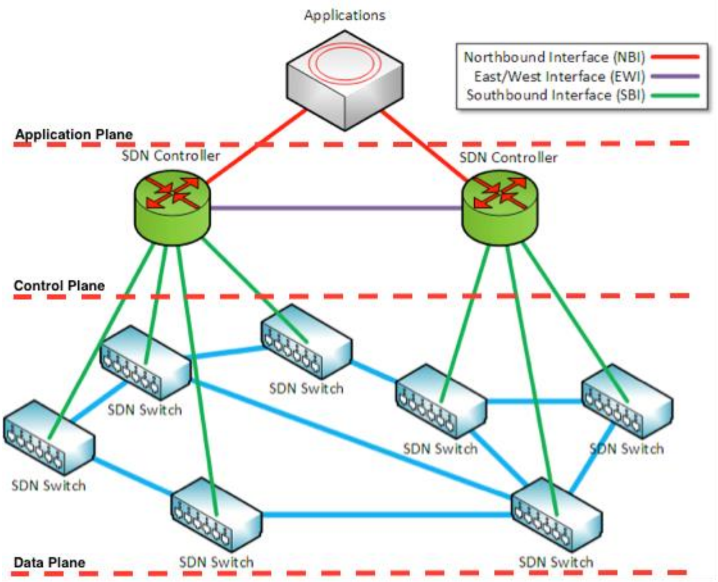

Figure 2 - Typical SDN Architecture Topology

The typical architecture of SDNs according to the Open Networking Foundation[11] is shown in Figure 2. As shown in the figure, this architecture involves three separate functionality planes:

- The *Data Plane* – i.e., the plane responsible for the data forwarding functionality of the network. The functionality of this plane is realized through a set of physical network devices (network elements).
- The *Control Plane* – i.e., the plane responsible for the control functionality of the network. The functionality of this plane is realized through a set of controllers and devices that facilitate the creation and destruction of network flows and paths. In an SDN, different controllers have control responsibility over disjoint subsets of forwarding devices. Through these forwarding devices, they

[11] Open Networking Foundation, https://www.opennetworking.org/

control different parts of the SDN. Typical SDN Controllers include OpenDaylight[12], NSX[13], Nuage[14], OpenContrail[15], ONOS[16], Beacon[17], Floodlight[18], NOX[19], ONIX[20], POX[21] and Maestro[22].

- The *Application Plane* – i.e., the plane responsible for generic network management auditing, and reporting functionalities (e.g., SDN management, monitoring and security). The functionality of this plane is realized through different network management applications (e.g. Network visualization).

The SDN architecture defines also the key interfaces between the different components in it. These interfaces are:

- The *East/West bound API* – This interface is implemented by the different controllers of the SDN and is used to facilitate communications between them. Representative examples of such APIs are ALTO[23] and Hyperflow[24].
- The *Southbound API* – This interface is implemented by the different forwarding devices in the SDN to enable the communication between these devices and the controllers of the network. Representative examples of such APIs are OpenFlow[25], ForCES[26], PCEP[27], NetConf[28] and IRS[29].

[12] OpenDaylight: open platform for programmable networks, https://www.opendaylight.org/

[13] NSX: Vmware network virtualization platform, http://www.vmware.com/products/nsx

[14] Nuage: Nuage Networks network virtualization platform, http://www.nuagenetworks.net/products/virtualized-services-platform/

[15] OpenContrail: open source network virtualization platform for the cloud, http://www.opencontrail.org/

[16] ONOS: open carrier-grade SDN network operating system designed, http://onosproject.org/

[17] Beacon: cross-platform and modular Java-based OpenFlow controller, https://openflow.stanford.edu/display/Beacon/Home

[18] Floodlight: open enterprise-class SDN controller, http://www.projectfloodlight.org/floodlight/

[19] NOX: open c++ based SDN development controller platform, http://www.noxrepo.org/

[20] Koponen, Teemu, et al. "Onix: A Distributed Control Platform for Large-scale Production Networks." OSDI. Vol. 10. 2010., http://static.usenix.org/events/osdi10/tech/full_papers/Koponen.pdf

[21] POX: open python based SDN development controller platform, http://www.noxrepo.org/pox/about-pox/

[22] Cai, Zheng. "Using and Programming in Maestro.", http://maestro-platform.googlecode.com/files/programming.pdf

[23] ALTO: Application Layer Traffic Optimization for distributed topologies, https://tools.ietf.org/html/rfc7285

[24] Tootoonchian, Amin, and Yashar Ganjali. "HyperFlow: A distributed control plane for OpenFlow." Proceedings of the 2010 internet network management conference on Research on enterprise networking. USENIX Association, 2010., https://www.usenix.org/legacy/event/inmwren10/tech/full_papers/Tootoonchian.pdf

[25] OpenFlow: communications protocol providing access to the data plane, https://en.wikipedia.org/wiki/OpenFlow

[26] Yang, Lily, et al. Forwarding and control element separation (ForCES) framework. No. RFC 3746. 2004., http://www.rfc-editor.org/info/rfc3746

[27] Vasseur, J. P., and J. L. Le Roux. "Path computation element (PCE) communication protocol (PCEP)." (2009)., http://tools.ietf.org/html/rfc5440_1

[28] Zhou, Lei, Ligang Dong, and Rong lin. "Research on ForCES Configuration Management Based on NETCONF." Information Technology Journal 13.5 (2014): 904-911., http://docsdrive.com/pdfs/ansinet/itj/0000/56356-56356.pdf

[29] IRS: interface to the Routing System, routing protocol, https://tools.ietf.org/html/draft-ward-irs-framework-00

- The *Northbound API* – This interface is implemented by the controllers of the SDN and is used to facilitate the communication between controllers and the network management applications. Representative examples of such APIs are FML[30], Procera[31], Frenetic[32], Maple[33] and RESTful[34]**.**

The final purpose of separating the network's control and forwarding planes is to provide various benefits; as simplified administration, automated reconfiguration and performance improvements, however it can also introduces some significant challenges in network security. In addition this approach reduces the CAPital EXpenditure (CAPEX), the initial money investment of a company as well as the OPerating EXpenditure (OPEX) that is the ongoing cost of the investment. In the following, we identify the key assets in an SDN that may become the source of security risks for it.

3.2 5G Design Principles

The fifth generation of mobile technology known as 5G is positioned to address the demands and business of the future internet. Whether the need is to download multimedia content, provide content for robots and autonomous cars or enable distant healthcare, 5G will be the technology behind the scenes and will be on the forefront of all consumer and business applications. Experts speculate that 5G will be in place by the end of the decade.

At the time of writing this report, there is no standardized architecture for 5G access. An illustration of the 5G architecture as envisioned by the Next Generation Mobile Networks (NGMN)[35] alliance is depicted in Figure 3.

[30] Katta, Naga Praveen, Jennifer Rexford, and David Walker. "Logic programming for software-defined networks." Workshop on Cross-Model Design and Validation (XLDI). Vol. 412. 2012., http://www.cs.princeton.edu/~jrex/papers/xldi12.pdf

[31] Voellmy, Andreas, Hyojoon Kim, and Nick Feamster. "Procera: a language for high-level reactive network control." Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012., http://dl.acm.org/citation.cfm?id=2342451

[32] Frenetic: high-level domain-specific SDN programming language, https://en.wikipedia.org/wiki/Frenetic_(programming_language)

[33] Voellmy, Andreas, et al. "Maple: Simplifying SDN programming using algorithmic policies." ACM SIGCOMM Computer Communication Review. Vol. 43. No. 4. ACM, 2013., http://dl.acm.org/citation.cfm?id=2486030

[34] Sezer, Sakir, et al. "Are we ready for SDN? Implementation challenges for software-defined networks." Communications Magazine, IEEE 51.7 (2013): 36-43., http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6553676

[35] Next Generation Mobile Networks NGMN

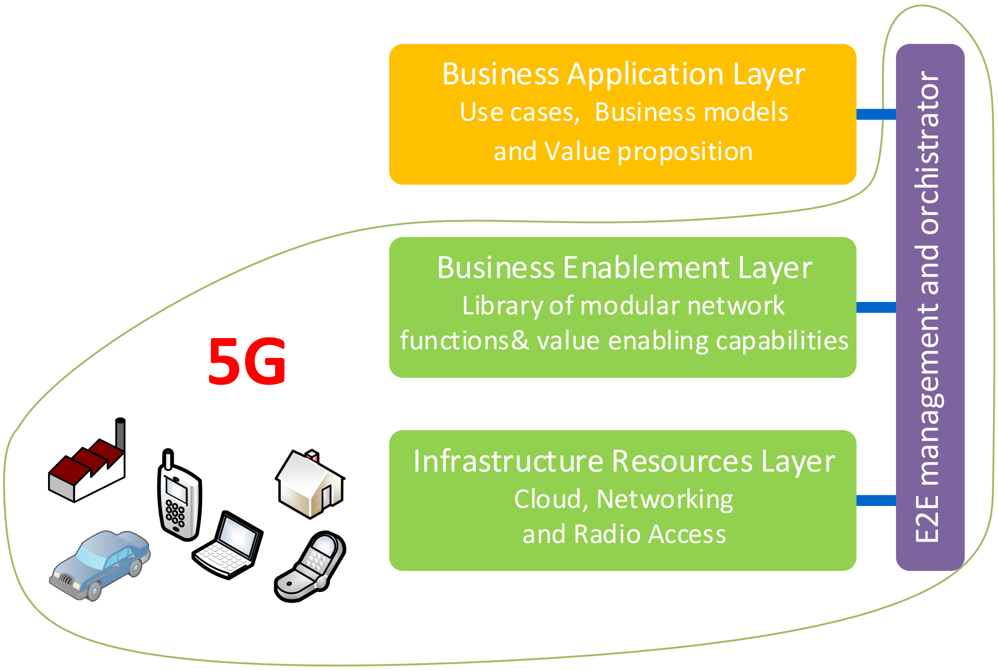
Business Application Layer
Use cases, Business models and Value proposition
Business Enablement Layer
Library of modular network functions& value enabling capabilities
Infrastructure Resources Layer
Cloud, Networking and Radio Access
E2E management and orchestrator
5G

Figure 3 - 5G architecture

“NGMN envisions an architecture that leverages the structural separation of hardware and software, as well as the programmability offered by SDN and NFV. As such, the 5G architecture is a native SDN/ NFV architecture covering aspects ranging from devices, (mobile/ fixed) infrastructure, network functions, value enabling capabilities and all the management functions to orchestrate the 5G system. The architecture comprises three layers and an E2E management and orchestration entity.”[36]

The **infrastructure resource layer** contains any physical device including mobile devices, Internet of Things (IoT) devices etc. (5G devices), as well as fixed networking devices (networking nodes, cloud nodes, access nodes etc.). This layer utilizes the SDN/NFV programmability as well as the configurability of 5G devices in order to meet the 5G design specifications (e.g. bandwidth, capacity latency).

The **business enablement layer** contains all the necessary functions for the 5G converged network in the form of modular architecture building blocks. These blocks along with configuration parameters can be evoked from a common repository upon request depending on the use case.

The **E2E management and orchestration entity** has access to manage and orchestrate the above mentioned architectural blocks. In addition, it defines network slices for each use case, interconnects the relevant functions of the network, assigns the proper configuration to meet E2E specifications and maps all these to the network entities of the infrastructure resource layer.

The **business application layer contains applications** and services of the 5G network operators or other enterprises that use the network. An interface to the E2E management and orchestration entity can be used to map an application to existing network slices, or to create new slices for the applications.

[36] “NGMN 5G white paper”, https://www.ngmn.org/5g-white-paper/5g-white-paper.html

4. SDN/5G Assets

4.1 Methodological conventions

As commonly defined, in our study, an *asset* is anything that has value and therefore requires protection. Due to their value, assets become the targets of *threat agents*. Threat agents are human or software agents, which may wish to abuse, compromise and/or damage assets. Threat agents may perform *attacks*, which create *threats* that pose *risks* to assets.

In a typical ICT system, assets can be: (a) hardware, software and communication components; (b) communication links between them; (c) data that control the function of the system, are produced and/or consumed by it, or flow within it; (d) the physical and organizational infrastructure within which the ICT system is deployed, and (e) the human agents who interact with the system and may affect its operation (e.g., users, system administrators etc.).

In the overview of SDN assets that we provide in the remainder of this report, we have categorized assets into the above categories. Furthermore, we have grouped assets according to their position within the typical SDN architecture, i.e., into data plane, control plane and application plane assets.

Another important consideration has been the inter-domain multi-operator landscape, which refers to the interconnection of several network operators through specific SLAs. In the current, non-SDN-based network model, a network operator is only capable to request network resources from a neighbouring network operator based on static and agreed SLAs. This is not flexible and requires high negotiation efforts to facilitate end-to-end QoS through multiple operator networks. Moreover, in contemporary multi-operator ecosystems, QoS provisioning, as required by industrial applications is not manageable due to different QoS levels that operators are able to provide[37]. SDN technology addresses these issues, by providing mechanisms that enable and allow to access the network infrastructure in different operator domains and provide path-level QoS across different operator domains.

It should be noted that, due to the emerging nature of SDNs, there is no commonly accepted detailed architecture of data and software components below the 3 architectural layers indicated in Figure 2. Hence, to provide a thorough asset analysis, we have identified the different types of functionalities, which have been suggested in the literature for each of the different SDN architecture layers, and mapped them onto logical functional SDN components, which we, subsequently, refer to as assets. Clearly, these “logical” software assets may be realized through different groups of actual software components in different SDN implementations. Nevertheless, we believe that, as a first step towards a security threats analysis, the reference to “logical” software assets is sufficient.

[37] ETICS White paper (2013), https://www.ict-etics.eu/fileadmin/documents/news/ETICS_white_paper_final.pdf

4.2 Categories of SDN Assets

In this part valuable assets of an SDN network infrastructure are presented that are commonly found in the literature in a hierarchical manner. Based on a single first top layer classification these SDN assets are distinguished into:

- **Data Plane Assets:** This asset group includes all assets of the SDN network deployments that include the physical instances of the network such as switching devices (Switches/Routers) and the communication medium (wired or wireless). Data plane assets include both hardware and software (e.g. Firmware, or a more or less full-fledged operating system and software switch) of the so called network elements.
- **Control plane Assets:** This asset group includes any SDN assets related to the control plane of the SDN. Such assets include both the hardware (e.g. controllers and Interfaces) and software used to realize SDN control (e.g. protocols for the controller communication), along with system configuration and control data.
- **Application plane Assets:** This asset group includes software applications that are used to implement any network explicitly, directly. Applications can communicate their network requirements and desired network behaviour to the SDN Controllers via APIs. Application plane assets include also hardware that is used to run these applications (e.g. Servers)
- **SDN Users:** This asset group includes any User that is using equipment attached to the Data plane of an SDN deployment. Service-level agreements and regulations can be considered as SDN user assets as well.
- **Service provider IT Infrastructure Assets:** This asset group includes any component of an IT infrastructure that is used by or belong to any service provider in the SDN from a billing system to stored data of an end user in a cloud.
- **Network service provider physical infrastructure Assets:** This asset group includes physical assets of the network service providers including every construction (e.g. Buildings, data centres etc.), machinery as well as the power supply networks
- **Human Assets:** This asset group includes any human in the SDN ecosystem from system and network administrators to simple end users.

A mind map presenting the above taxonomy is shown in Figure 4. A more detailed taxonomy of assets categorised in deeper taxonomic levels is also provided in Annex A.Annex A:

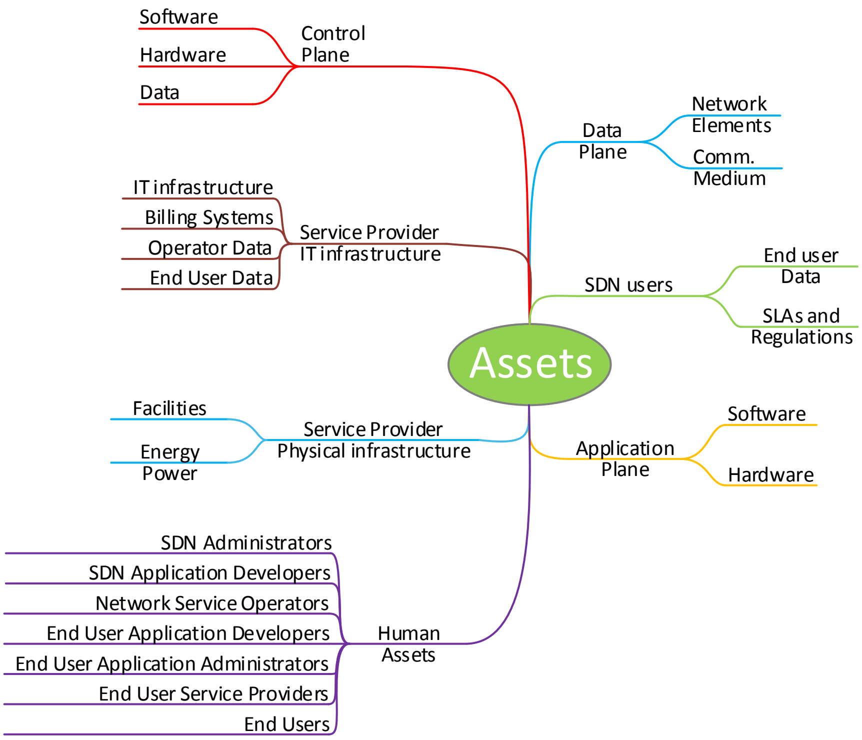

Figure 4 - SDN assets threat landscape

It should be noted that the SDN network infrastructure and its respective components/assets, assumed by our analysis, may belong either to a single network operator (intra-domain case) or to multiple network operators (inter-domain case).

5. SDN Threats

SDN brings significant innovation to networking. Key concepts associated with SDN such as Logically Centralized Intelligence, Programmability and Network Abstraction establish a basis for future communications. While significant improvements may be achieved in network security by centralization and programmability, these two concepts can also attract a new level of threats and attacks.

Security within the SDN paradigm is a challenge, as all layers, sub-layers and components need to communicate according to strict security policies. In this report, we have attempted to increase awareness by identifying key valuable assets of the SDN infrastructure that are needed in order to ensure proper network function and interoperability. As these assets may, however, become the target of attacks, they become naturally the main driver of threat analysis aimed at securing SDNs.

5.1 Taxonomy of SDN/5G Threats

The identification of SDN/5G threats has been based on a study of the related literature, which indicates not only SDN threats but also generic taxonomies that could be used for classifying them.

One of these taxonomies has been documented in the ENISA report "ENISA Threat Landscape 2014"[38] (ETL14). Although this taxonomy has not been developed for SDN/5G threats, our view is that it is generic enough to be used for classification of such threats. This is because of the similarity of the respective landscapes, i.e., the Internet Infrastructure and the SDN/5G landscape, which renders the taxonomic classification presented in ELT14 broadly applicable to the SDN/5G landscape. Furthermore, the adoption of this taxonomy can make the understanding of the SDN/5G threat landscape easier for the reader.

Based on ETL14, the general categories of threats for the SDN/5G landscape are:

- *Nefarious activity/abuse (NAA)*: This threat category is defined as "intended actions that target ICT systems, infrastructure, and/or networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target"[34]
- *Eavesdropping/Interception/* Hijacking *(EIH)*: This threat category is defined as "actions aiming to listen, interrupt, or seize control of a third party communication without consent"[34]
- *Physical attacks (PA)*: This threat category is defined as "actions which aim to destroy, expose, alter, disable, steal or gain unauthorised access to physical assets such as infrastructure, hardware, or interconnection"[34]
- *Damage (DAM)*: This threat category is defined as intentional actions aimed at causing " destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness"[34]
- *Unintentional Damage (UD):* This threat category is defined as unintentional actions aimed at causing " destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness "[34]

[38] ENISA Threat Landscape 2013, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

- *Failures or malfunctions (FM):* This threat category is defined as "insufficient functioning of an (Internet infrastructure) asset"[34]. In the case of SDN/5G the assets include those defined in the asset list.
- *Outages (OUT):* This threat category is defined as "unexpected disruptions of service or decrease in quality falling below a required level "[34]
- *Disaster (DIS):* This threat category is defined as "serious disruption of the functioning of a society"[34]
- *Legal (LEG)*: This threat category is defined as "legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law" [34]

In addition to the above general taxonomy, we also categorise threats depending on whether their source is an SDN element, a 5G element or a generic network element. Based on this criterion, threats can be further categorised into:

- *SDN specific threats*[39]: These are threats related to the elements of the SDN architecture. These threats fall under the categories "Nefarious activity/abuse" and "Eavesdropping/Interception/ Hijacking". SDN specific threats are described in detail in Sect. 5.2.
- *Network Virtualisation threats*: These are threats related to the underlying IT infrastructure used for virtualising network operations. Network Virtualisation specific threats are described in more detail in Sect. 5.3.
- *5G/Radio access threats*[40]**:** These are threats related to the 5G landscape but not specific to the SDN infrastructure. 5G specific threats include threats related to the wireless medium, the virtualisation of functions and the multi-operator environment. Threats of the wireless medium are mostly related to "Eavesdropping/Interception/Hijacking"; threats on virtualisation are related to "Nefarious activity/abuse" and "Eavesdropping/Interception/ Hijacking". 5G specific threats are described in more detail in Sect. 5.4.
- *Generic network infrastructure threats:* These are threats that any network infrastructure faces without reference to the 5G and/or SDN landscape. Generic network infrastructure threats fall under the categories "Physical attacks", "Damage or loss of equipment", "Equipment failures or malfunctions", "Outages", "Disaster" and "Legal and business". Generic network infrastructure threats are described in more detail in Sect. 5.5.

5.2 SDN specific Threats

In the following, we present types of threats that are specific to SDN. Such threats may relate to different assets in the reference SDN architecture, as shown in Figure 5. For the listed threats, we also identify the layer of the reference SDN architecture that these threats are primarily related to according to the literature if relevant.

Data forging: This threat involves compromising an SDN element (e.g., controller, router, switch) in order to forge network data and launch other attacks (e.g., DOS). Whilst data forging may, in principle, relate to data

[39] SDNSecurity.org, "An Overview of Misuse / Attack Cases", http://sdnsecurity.org/project_SDN-Security-Vulnerbility-attack-list.html

[40] Ericsson White paper, "5G Security", Uen 284 23-3269 | June 2015, http://www.ericsson.com/res/docs/whitepapers/wp-5g-security.pdf

held by any component of an SDN (e.g., network switches, controllers and/or SDN applications), a threat specific to SDN consists in forging requests from accessible low level SDN controllers to upper level ones, in order to drive their decisions on how to redefine large parts of the network. In the literature it has been identified as a threat related to components in the data plane and the controller plane.

Traffic diversion: This threat involves compromising a network element in order to divert traffic flows and to enable eavesdropping. Traffic diversion is a threat relating to network elements of the data plane. A specific kind of traffic diversion that is available in virtualized networks is network slice trespassing. This occurs when the mandatory isolation between slices is compromised in any active node or when the enforcing access to a slice in the edge equipment is either bypassed or misconfigured. This ends with alien traffic circulating on a given slice.

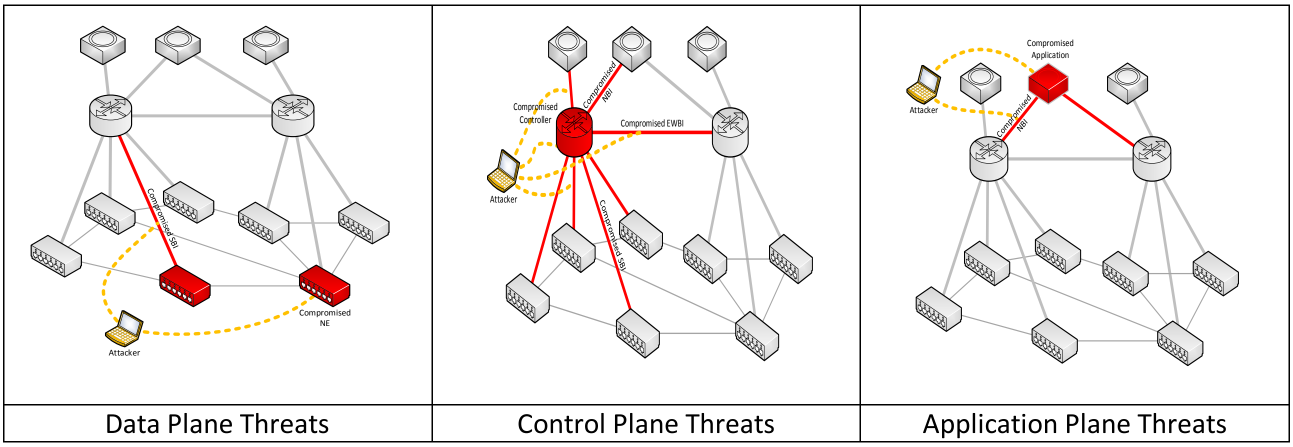

Figure 5 - Threats of SDN reference architecture

Side channel attack: This threat involves extracting information on existing flow rules that are used by network elements. The threat can be realised by exploiting patterns of network operations (e.g. exploiting the time required for establishing a network connection). Side channel attacks is a threat relating to network elements of the data plane.

Flooding attack: Flooding attacks involve compromising a SDN component in order to make it flood other components, which it interacts with. Flooding occurs through the transmission of data that can exhaust component resources and lead to a reduction or complete shutdown of the service provided by the component. Flooding attacks occur primarily for network components of the data plane. In such cases, the threat involves compromising a network component in order to make it flood its controller with network messages, and overload and eventually exhaust the controller's resources. Flooding attacks can also occur at the control plane. In such cases, a controller is flooded with messages from other (malicious) controllers that can exhaust its resources causing a reduction or complete shutdown of the controller's service. Specific to SDN are amplification flooding attacks where a small stream of requests with a faked sender elicits a flooding large stream of response. While protection from such attacks have been devised for many known network protocol, the exposure of several network functions (NFV) by SDN controllers presents a whole new landscape of threats.

Software/firmware exploits: This threat involves exploiting vulnerabilities of the software/firmware in order to cause some malfunction, reduction or disruption of service, eavesdrop data or destroy/compromise data. Software/firmware exploits may occur in all layers of the SDN reference architecture, and depending on the layer that they relate to they have been distinguished into **network element software/firmware exploits**, **controller software/firmware exploits**, and **SDN applications software/firmware exploits**. Software/firmware exploits of network elements and controllers cause the malfunction or even their termination of operation. In the case of switches, for example, the exploited switches can drop, slow down, clone or deviate network traffic. Exploited switches software/firmware can also create forged traffic in order to exhaust other switches and/or the controllers the switches are connected to.

Denial of Service (DoS): This threat relates to attacks aimed at causing reduction or disruption of the SDN service. DoS threats may occur in all layers of the SDN reference architecture. At the data plane, DoS can be caused by attackers, which flood the bandwidth or resources of network elements. This arrack type in many occasions originate by multiple compromised systems, such as botnets, which are flooding the targeted SDN with traffic. At the control plane, a DoS can be caused by congesting controllers through a large number of forged flow arrivals, causing network performance degradation and interruption. Traditional DoS defences' approaches focus on protecting the data plane, and are therefore ineffective in the cases of SDN control plane DoS attacks. DoS attacks may also appear at the application plane affecting, for example, network management applications.

Identity spoofing: Identity spoofing is a threat where a threat agent successfully determines the identity of a legitimate entity and then masquerades this entity in order to launch further attacks. Identity spoofing is a threat that can affect any type of software component or human agents. In the case of SDN, identify spoofing has been identified as an attack affecting mainly SDN controllers (**SDN controller identity spoofing**). In this attack, the attacker spoofs the identity of a legitimate controller and interacts with the network elements controlled by the legitimate controller (i.e., elements of the data plane) in order to trigger several other types of attacks (e.g., instantiate network flows, divert traffic etc.).

API exploitation: This threat involves exploiting the API of a software component in order to launch different types of further attacks such as the unauthorised disclosure, compromise of integrity and/or destruction of information, or the unauthorised destruction/degradation of service. In SDN, API exploitation may relate to all the different types of APIs that may be found in an SDN. These include: (a) the Northbound API (**Northbound API exploitation**) that facilitates the communication between SDN controllers and SDN applications; (b) the Southbound API that facilitates the communication between SDN network elements and SDN controllers (i.e., **Southbound API exploitation**), and (c) the Eastbound/Westbound API that facilitates the communication between SDN controllers (i.e., **Eastbound/Westbound API exploitation**).

Memory scraping: This threat arises when an attacker scans the physical memory of a software component in order to extract sensitive information that is it not authorised to have. Whilst in SDN, memory scrapping can affect components of any layer, this type of threat has been primarily identified for SDN application servers[41]. While the memory scrapping threat is exclusive to SDN, a core dump (e.g. as the result of malicious software) can be used to exploit private data. Furthermore SDN reconfiguration may require reboots that an attacker could use in order to attack the boot procedure. Once successfully performed, memory scrapping can be used to extract sensitive SDN data (e.g., flow rules at the Northbound API).

[41] J. Hizver, Taxonomic Modeling of Security Threats in Software Defined Networking, BlackHat Conference, August 5-6, 2015, available from: https://www.blackhat.com/docs/us-15/materials/us-15-Hizver-Taxonomic-Modeling-Of-Security-Threats-In-Software-Defined-Networking-wp.pdf

Remote application exploitation: In this threat, an attacker gains access or obtains higher access privileges to an SDN application by exploiting software vulnerabilities of it. This can then be used to execute operations illegitimately.

Traffic sniffing: Traffic sniffing involves tapping data flows within a network. In SDN, traffic sniffing has been identified primarily as an attack upon the communication link between an application at the SDN application plane and a controller at the control plane in order to gain access to important controller configuration data or application-level credentials. Traffic sniffing can be enabled by the use of weak or no encryption in the relevant communication link. It should be noted that traffic sniffing might also be used for legitimate reasons (e.g., for network monitoring and administration) and if used in this manner it should not be regarded as an attack.

5.3 Network Virtualisation Threats

Network virtualisation threats[42,43,44,45] are threats related to the underlying IT infrastructure used for virtualising network operations. Such threats can be distinguished into:

Threats related to servers running virtualised network functions (virtualised host abuse): Virtualisation of functions and their operation on virtual machines (e.g., a server that can be used as a network switch) is a common practice in SDN. Therefore traditional security threats for servers running virtualised network operations such as network monitoring, access control, network management etc. should be considered.[46]

Threats to data centres hosting SDN operations (Data centre threats): Many SDN systems are deployed within data centres. Hence, security threats of data centres should be considered, similarly to the server case. Moreover, data servers are using Data Centre Interconnect (DCI) protocols, which may lack authentication and encryption to secure the packet contents. Thus an attacker could create spoofed traffic in such a way that it traverses the DCI links or to create a DoS attack of the DCI connections.

Threats related to virtualization mechanism: (Network Virtualization bypassing): The use of the network between different tenants need to assure that only legitimated traffic enters or leaves a network slice, but also that any switching element checks and enforces the traffic isolation by installing legitimate flow rules preventing slice trespassing.

[42] Drutskoy, Dmitry, Eric Keller, and Jennifer Rexford. "Scalable network virtualization in software-defined networks." Internet Computing, IEEE 17.2 (2013): 20-27., http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6362137

[43] Pearce, Michael, Sherali Zeadally, and Ray Hunt. "Virtualization: Issues, security threats, and solutions." ACM Computing Surveys (CSUR) 45.2 (2013): 17., http://dl.acm.org/citation.cfm?id=2431216

[44] ETSI GS NFV-SEC 001 V1.1.1 (2014-10): Network Functions Virtualisation (NFV);NFV Security;Problem Statement, http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/001/01.01.01_60/gs_NFV-SEC001v010101p.pdf

[45] ETSI GS NFV-SEC 003 V1.1.1 (2014-12): Network Functions Virtualisation (NFV);NFV Security;Security and Trust Guidance, http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/003/01.01.01_60/gs_NFV-SEC003v010101p.pdf

[46] Network Functions Virtualisation (NFV);NFV Security; Problem Statement, http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/001/01.01.01_60/gs_NFV-SEC001v010101p.pdf

In reference to the taxonomy of threats outlined in Sect. 2, wireless medium threats fall under the general category of "Eavesdropping/Interception/ Hijacking".

5.4 5G radio access threats

In SDNs there can also be threats arising due to the use of 5G technology[47,48]; in particular the use of wireless communication in 5G. Such threats, as described in[49] can be distinguished into:

User emulation: The wireless medium can be exploited by adversaries that mimic incumbent signals. Nodes launching such attacks can be (i) **Greedy mobile nodes** that by transmitting fake incumbent signals force all other users to vacate a specific band (spectrum hole) in order to acquire its exclusive use and (ii) **Malicious mobile nodes** (adversaries) that mimic incumbent signals in order to cause Denial of Service (DoS) attacks. Malicious nodes can cooperate and transmit fake incumbent signals in more than one band, thus causing extensive DoS attacks making a radio hop from band to band, severely disrupting its operation.

Spectrum sensing data falsification: The received signal power may enforced to become lower compared to what path loss models have predicted due to transmission features such as signal fading, multi-path propagation, etc., [50]. This may lead to harmful interference due to undetected primary signals.

MAC layer attack: This category of attacks includes (i) MAC spoofing, where attackers send spurious messages aiming to disrupt the operation of network(e.g. channel negotiation), (ii) Congestion attacks, where attackers flood Common Control Channel in order to cause an extended DoS attack and (iii) Jamming attacks, where attackers cause DoS attacks at this layer by creating interference.

In reference to the taxonomy of threats outlined in Sect. 2, Network Function Virtualization (NFV)[51] threats can be seen as threats under the "Nefarious Activity/Abuse" and "Eavesdropping/Interception/ Hijacking" categories.

5.5 Generic network infrastructure threats

Besides the pure telecommunication infrastructures, in SDN/5G there are interdependencies with other computing infrastructures such as the cloud that may be used for network virtualisation. Such

[47] Mantas, Georgios, et al. "Security for 5G Communications." Fundamentals of 5G Mobile Networks (2015): 207-220., http://onlinelibrary.wiley.com/doi/10.1002/9781118867464.ch9/summary

[48] Demestichas, Panagiotis, et al. "5G on the horizon: key challenges for the radio-access network." Vehicular *Technology Magazine, IEEE* 8.3 (2013): 47-53., http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6568922

[49] Fragkiadakis, Alexandros G., Elias Z. Tragos, and Ioannis G. Askoxylakis. "A survey on security threats and detection techniques in cognitive radio networks." Communications Surveys & Tutorials, IEEE 15.1 (2013): 428-445.

[50] R. Chen, J. Park, T. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," IEEE Magazine, vol. 46, pp. 50–55, 2008., http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4481340

[51] ETSI, "Network Functions Virtualisation – Introductory White Paper", 2012, https://portal.etsi.org/NFV/NFV_White_Paper.pdf

interdependencies can introduce additional generic infrastructure threats, which may lead to SDN/5G failures, misconfiguration and errors. ENISA has produced an extensive and comprehensive report for this area[52]. In the following, we highlight the generic network infrastructure threats that should be considered in addition to the SDN specific threats and the 5G specific threats.

Physical threats: This type of attack refers to actions (attacks) aimed at destroying, disabling, altering or stealing physical ICT infrastructure assets. This type of threat applies to any network and computing infrastructure, including SDN/5G infrastructures. Physical threats are very important due to the virtualisation of networking functions, which may result in deploying such functions in remote servers and data centres. Despite the existence of physical protection mechanisms (e.g., physical surveillance and surveillance cameras, security locks, security guards), physical breaches and insider threat attacks still occur[53]. Examples of such attacks include fraud, sabotage vandalism, theft, information leakage/sharing, unauthorised physical access and terrorist attacks.

Damage/loss: This type of threats refers to intentional or unintentional destruction of ICT infrastructure. It may be physical as for example the destruction of a server or take the form of a cyber damage as, for example, mixing-up information in a data centre due to maintenance errors or erroneous system administration.

Failures/malfunctions: This type of threats refers to failures or insufficient functioning of network and infrastructure subsystems. Examples of this threat type include failure or malfunctioning of devices including network elements, controllers and network management applications, disruption of the communication links, and/or failure of service providers.

Outages: This type of threats refers to the interruption or failure in the supply of a service. In the case of SDN/5G networks, it includes interruption of support services such as Internet and electricity, the loss of network connectivity either due to cable errors or the loss of (part of) a wireless network, or loss of human (e.g. strike of employees of a network operator) or physical resources.

Disaster: A disaster is a sudden incident that interrupts the daily activities of the society. It can be categorised in disasters caused by the intervention of human (environmental) or natural disasters such as floods, earthquakes etc.

Legal: Since the 5G landscape is of multi-operator nature, where all operators will be interconnected to each other, multi-operator related threats are very important. In this landscape, operators of the SDN infrastructure that will not honestly stick to business agreements (SLAs) should be considered. Moreover, measures for non-repudiation of SLAs between different operators should be considered.

5.6 Lists of SDN/NFV/5G and Generic Network Threats

[52] Enisa, “Annual Incident Reports”, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

[53] Kelly Jackson Higgins, “Five Ways To (Physically) Hack A Data Center” Available: http://www.darkreading.com/five-waysto-(physically)-hack-a-data-center/d/d-id/1133615

In the following, we present two tables of SDN related threats. These tables list SDN/NFV/5G specific threats (Table 1 - SDN/5G Specific threats and assetsTable 1), and generic network threats (Table 2), respectively. For each threat, the tables provide:

(a) A brief description of the threat (see "Threat" column), the main type of the threat in reference to the taxonomy described in the ENISA report on "Threat Landscape and Good Practice Guide for Internet Infrastructure"[54] that has been overviewed in Sect. 2 of this report. In cases where a threat falls under more than one categories in the ENISA taxonomy, the additional categories are identified in the description of the threat.

(b) The assets that the threat affects (see column "Asset types"). This description refers to the asset listing produced earlier as part of the project.

(c) The potential effect of the threat described in terms of the basic security properties that a threat can compromise, i.e., confidentiality, integrity or availability (see column "Potential Effect").

[54] Enisa, "Threat Landscape and Good Practice Guide for Internet Infrastructure", https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure

Threat types	Threats	Potential Effect	Asset types
Nefarious Activity/Abuse	Manipulation of Information / Data forging • Routing table manipulations • DNS manipulations • Falsifications of configurations	• Information integrity • Information destruction • Service availability	• Data plane data • Control plane data, • Application plane data
	Software/firmware exploits • Controller ○ Kernel flaws (can also be seen as FM threats) ○ Buffer overflows (can also be seen as FM threats) ○ SQL injection (can also be seen as FM threats) ○ XSS (can also be seen as FM threats) • Network element ○ Kernel flaws (can also be seen as FM threats) ○ Buffer overflows (can also be seen as FM threats)	• Information integrity • Information destruction • Outage • Service availability	• Data plane software • Control plane software
	Denial of Service (DoS) (can also be seen as OUT threats) • Flooding attack • Amplification attack	• Service availability	• Data plane • Control plane • Application plane • Service Provider IT infrastructure • SDN users
	Remote SDN application exploitation • Network visualisation exploitation • Network management • Mobility management • Service provisioning exploitation • Traffic engineering exploitation • Virtual Cloud networking exploitation	• Information integrity • Information destruction • Service availability	• Application plane

	SDN API exploitation • NBI exploitation • EWBI exploitation • SBI exploitation	• Information integrity • Information destruction • Service availability	• Data plane • Control plane • Application plane
	Malicious Software • Virus • Malware • Worms • Trojan • Botnet • Greyware	• Information integrity • Information destruction • Other software asset integrity • Other software asset destruction • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • SDN users • Human agents
	Unauthorised activities • Unauthorised access • Unauthorised installation of software • Unauthorised use of software • Unauthorised administration of devices and systems	• Information integrity • Information destruction • Other software asset integrity • Other software asset destruction • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • SDN user • Human agents
	Virtualisation threats • Virtualised hosts abuse ○ Denial or Loss of service (can also be seen as OUT threats) ○ Degradation of service (can also be seen as OUT threats) • Data Center threats ○ Resource contention (can also be seen as FM and OUT threats) ○ Abuse of unencrypted data	• Information integrity • Information destruction • Other software asset integrity • Other software asset destruction • Service availability	• Data plane • Control plane, • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
Eavesdropping/Interception/ Hijacking	Traffic diversion	• Information confidentiality • Service availability	• Data plane • Control plane • SDN user

	Side channel attack	• Information confidentiality • Service availability	• Data plane • Control plane • SDN user
	Identity spoofing • SDN ○ Controller ○ Network element • Network administrators • Network operators	• Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • SDN user • Human agents
	Software/firmware exploits • Controller • Network element	• Information confidentiality • Service availability	• Data plane • Control plane
	Memory scraping (can also be seen as NAA threat)	• Information confidentiality • Service availability	• Data plane • Control plane • Application plane
	Virtualisation threats • Virtualised hosts abuse ○ Unauthorised access ○ Loss of control of virtualised function • Data Center threats ○ DC Traffic spoofing ○ Inter VM attack • Network Virtualization bypass ○ Unlawful network slice ingress and egress ○ Slice trespassing.	• Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Human agents
	Traffic sniffing	• Information confidentiality	• Data plane • Control plane • Application plane • SDN user
	Mobile 5G user interception • User Emulation	• Information integrity • Information destruction • Information confidentiality	• Data plane • SDN user (when wireless communication is used)

	• Spectrum sensing data falsification (can also be seen as NAA threat) • MAC attack	• Service availability	
	Man in the middle • In NBI • In EWBI • In SBI	• Information confidentiality	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Human agents
	Interception of Information • Espionage ○ Nation State ○ Corporate • Rogue Hardware • S/W Interceptions	• Information confidentiality	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Human agents

Table 1 - SDN/5G Specific threats and assets

Threat types	Threats	Potential effect	Asset types
Physical attacks	Fraud	• Information integrity • Information destruction • Information confidentiality	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
	Sabotage	• Information integrity • Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
	Vandalism	• Information integrity • Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
	Theft (of devices, storage media and documents)	• Information integrity • Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
	Information leakage/sharing	• Information integrity • Information destruction • Information confidentiality	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents

	Unauthorised physical access / Unauthorised entry to premises	• Information integrity • Information destruction • Information confidentiality	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
	Terrorists attack	• Information integrity • Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
Damage	Information leakage/sharing due to human error	• Information integrity • Information destruction • Information confidentiality	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
	Erroneous use or administration of devices and systems	• Information integrity • Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
	Maintenance mix-up	• Information integrity • Information destruction Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • Human agents
	Data loss	• Information integrity • Information destruction	

	• Unintentional change of data in an information system • Loss of information in the cloud • Loss of data integrity	• Information confidentiality	
Failures or malfunctions	Failure of devices or systems	• Information integrity • Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure
	Failure or disruption of communication links	• Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure
	Failure or disruption of main supply	• Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure
	Failure or disruption of service providers (supply chain)	• Information integrity • Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure
	Malfunction of equipment (devices or systems)	• Information integrity • Information destruction • Information confidentiality • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure
Outages	Loss of resources • Human resources	• Service availability	• Data plane • Control plane

	• Physical resources		• Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • SDN user • Human agents
	Support services • Internet provider • Electricity provider	• Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • SDN user • Human agents
	Network connectivity • Cable Networks Service availability • Wireless Networks • Mobile Networks	• Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • SDN user • Human agents
Disasters	Natural disasters	• Information destruction • Human agent loss • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • SDN user • Human agents
	Environmental disaster	• Information destruction • Human agent loss • Service availability	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • SDN user • Human agents

Legal and business	Breach of SLAs	• Information integrity • Information destruction • Information confidentiality • Service availability	• Application plane • SDN user • Service provider IT Infrastructure • Human agents
	Breach of legislation	• Information integrity • Information destruction • Information confidentiality • Service availability	• Application plane • SDN user • Service provider IT Infrastructure • Human agents
	Judiciary decisions/court orders	• Information integrity • Information destruction • Information confidentiality • Service availability	• Application plane • SDN user • Service provider IT Infrastructure • Human agents
	Abuse of personal data	• Information integrity • Information destruction • Information confidentiality	• Application plane • SDN user • Service provider IT Infrastructure • Human agents
	Illicit competition	• Information integrity; • Information destruction • Information confidentiality • Service availability	• Application plane • SDN user • Service provider IT Infrastructure • Human agents

Table 2 - Generic network infrastructure threats and assets

Figure 6 shows the higher part of the threat taxonomies (i.e., up to second third level of classification) listed in Table 1 and Table 2 in the form of a mind map. A more detailed mind map showing up to two more levels of taxonomic classification can be found in Annex C:.

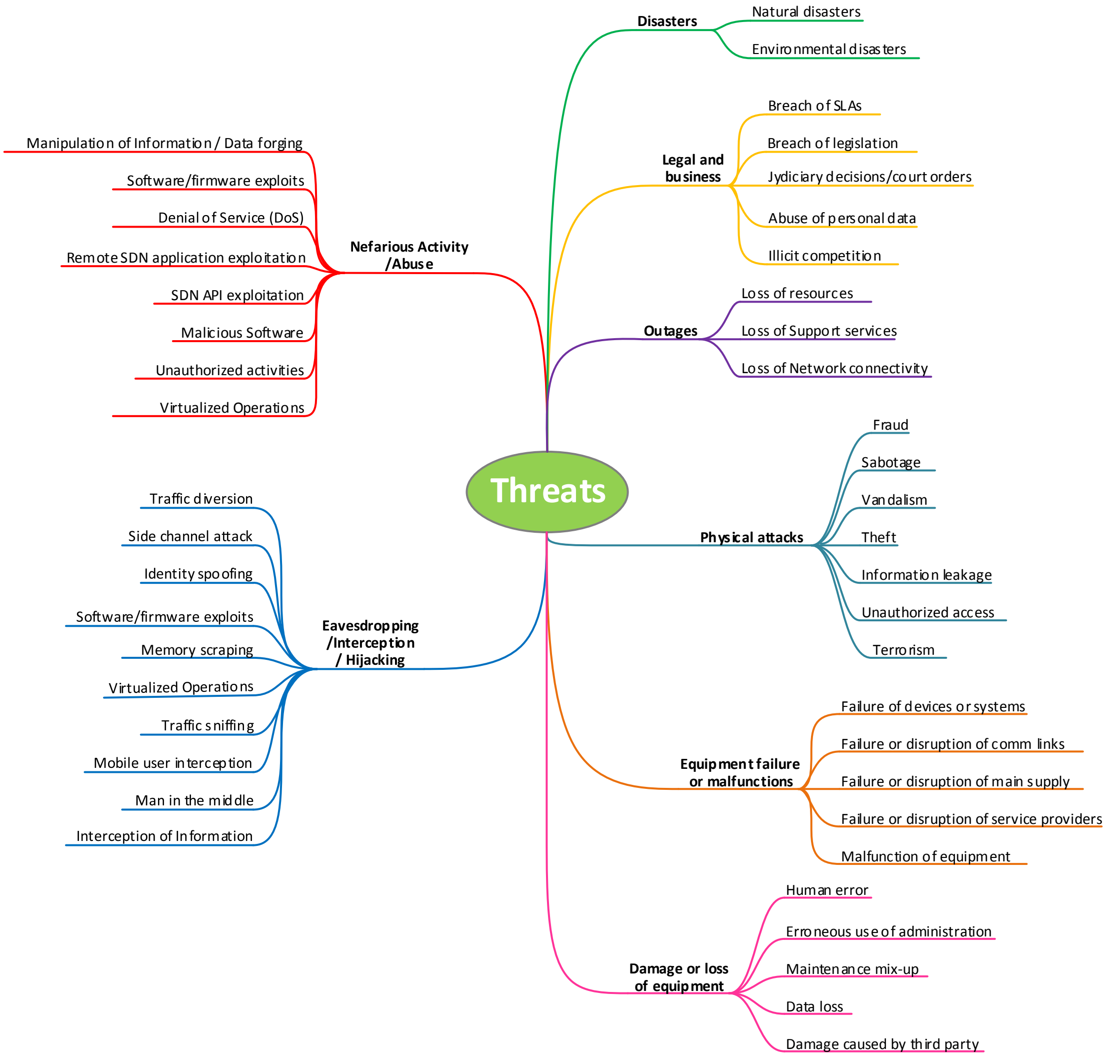

Figure 6 - Top level threats taxonomy

6. Threat Agents

According to ELT14[55], a threat agent is "*someone or something with decent capabilities, a clear intention to manifest a threat and a record of past activities in this regard*". ELT14 categorizes thread agents as follows:

- Corporations
- Hacktivists
- Cyber criminals
- Cyber terrorists
- Script kiddies
- Online social hackers
- Employees
- Nation states

Another categorization of threat agents in the case of SDN may be based on whether or not an agent has legitimate access to the resources/assets of a network. According to this criterion, and similarly to [56] attackers may be distinguished into:

- **External attackers:** These are attackers with no legitimate access to the SDN network and its services, but they own appropriate network tools and in some occasions infrastructure that enable then to interfere with the operation of the SDN network. In addition, these attackers may have unsupervised access to servers that run virtualised SDN application and they have the ability to modify the behaviour of these servers by installing rogue software on them. This is a broad category of attackers including cybercriminals, hacktivists, terrorists, corporations and Nation States.
- **Internal attackers**: These category refers to people that have inside access to the network operator resources. They can be employees (staff) of the network operator and contractors.
    - **Dishonest customers:** These can be misbehaving end-users that have legitimate/subscribed access to the SDN network and its services and take advantage of their access to the network in order to interfere with its operation or to gain illegal access to its services (e.g., by impersonating another customer).
    - **Dishonest operators:** These are telecom operators or service providers that their network infrastructure is based on SDN, which attempt to gain competitive advantage over their competing operators by not honestly sticking to their agreed business agreements (SLAs).

For the SDN landscape, it is crucial for asset owners to be aware of which threats can emerge from different threat agent groups. The following table (Table 3) presents an overview of this based on the threat agent categorization of ELT14.

[55] "ENISA Threat Landscape 2014", https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

[56] Askoxylakis, I., et al. "Securing multi ‐ operator ‐ based QoS ‐ aware mesh networks: requirements and design options." Wireless Communications and Mobile Computing 10.5 (2010): 622-646.

	Corporations	Hacktivists	Cyber Criminals	Cyber Terrorists	Script Kiddies	Online-Social Hackers	Employees	Nation States
Nefarious activity/Abuse	●	●	●	●	●	●	●	●
Eavesdropping/ Interception/ Hijacking	●		●	●	●	●	●	●
Physical attacks		●	●	●			●	
Damage	●	●	●	●	●	●	●	●
Unintentional Damage						●	●	●
Failures/ malfunctions			●	●	●		●	●
Outages	●	●	●	●	●	●	●	●
Disaster								
Legal	●							●

Table 3 - Involvement of threat agents in threats

7. Good Practices

This section provides a review of existing techniques, tools and practices for threat mitigation in SDN/5G that have been identified through literature search and discussion with an expert group convened by ENISA for this purpose.

The underlying search that resulted in the identification of threat mitigation practices has also considered established research programmes and large scale collaborative research and innovation projects, which have already delivered or are expected to deliver techniques, tools and practices for SDN/5G security threat mitigation, according to their work programme. To support and enhance the outcomes in this direction, the expert group that was convened by ENISA involved representatives from Phase 1 of the funded projects of 5G Infrastructure Public Private Partnership[57] (in short 5G PPP)[58]. 5G PPP was initiated by the EU Commission and industry manufacturers, telecommunications operators, service providers, SMEs and researchers with the aim of delivering solutions, architectures, technologies and standards for global next generation communication infrastructures.

In the following, we first present threat mitigation practices arising from already developed SDN protection technologies (Sect.7.1) and then mitigation practices, which are currently under development (Sect.7.2).

7.1 Existing threat mitigation practices

Existing threat mitigation practices have identified through a review of SDN protection techniques that have been suggested in the literature and/or implemented in existing SDN tools. The tools that were considered for this purpose are discussed next.

7.1.1 Overview of tools/techniques

Secure Architecture for the Networked Enterprise (SANE[59]): SANE is an architecture developed to protect enterprise networks. SANE includes one logical controller for all packet forwarding rule decisions. This controller is the only trusted component in the network and assigns an encrypted channel to every permitted request. SANE supports natural policies (e.g. allow everyone in group accounting to connect to the web server hosting documentation) that are autonomous of network topology and the used equipment.

Ethane[60]: Ethane is an architecture proposed for enterprise networks to provide strong security guarantees. It is based in a Central Domain Controller (DC) that implements secure bindings by authenticating users, hosts, services etc. DC contains the global security policy of the network and checks every new flow request

[57] https://5g-ppp.eu/5g-ppp-phase-1-projects/

[58] https://5g-ppp.eu/

[59] M. Casado, T. Garfinkel, A. Akella, M. J. Freedman, D. Boneh, N. McKeown, and S. Shenker. SANE: A Protection Architecture for Enterprise Networks. In Proceedings of the 15th USENIX Security Symposium (SS), volume 15, 2006.

[60] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker. Ethane: Taking Control of the Enterprise. ACM SIGCOMM Computer Communication Review (CCR), 37(4):1–12, 2007.

against this policy. (*Note: Ethane is no longer maintained, however, due to the importance in the evolution of SDN has been included*)

FlowNAC[61]: FlowNAC is network access control solution, based on flows, that permits granting the users rights to access the network following a target service use request. Each set of flows functions as a service that can be independently requested. Multiple services can be authorized at the same time. SDN offers the granularity that is necessary for identifying services at the data plane as a set of flows, in order to enforce suitable policy. This is done in a dynamic fashion.

Panopticon[62]: An architecture proposal to realize incrementally deployment of SDN. Panopticon results in a Hybrid SDN deployment. It introduces a mechanism called Solitary Confinement Tree, which using VLAN functionality ensure that inbound traffic to switch ports of legacy devices passes through at least one SDN switch. This topology is sufficient to ensure end-to-end network policy.

DefenceFlow[63]: DefenceFlow is a commercial application that detects and resolves DDoS attacks. Its operation is based on pattern matching of traffic statistics of SND forwarding devices. In case of DDoS detection it redirects traffic to the nearest mitigation device. A mitigation device devices can be placed in any location in the network

HP Sentinel Security[64]: An SDN application that monitors the flow creation process in the network. As a flow is identified, it is compared to a reputation database for IP Address and DNS names. If the lookup is positive, traffic is dropped on the forwarding devices.

NOX[65] : The NOX SDN controller has focussed on implementing traffic anomaly detection algorithms.

Rosemary[66]: Rosemary is an SDN controller that is based on the approach of spawning SDN applications in an isolated pseudo network operating system. The result is network application containment and resilience strategy.

FRESCO[67]: FRESCO is a security application development framework that is designed to enable rapid design of detection and mitigation modules in the context of OpenFlow. FRESCO provides a scripting API enabling the coding of security monitoring and threat detection logic as modular libraries.

FlowChecker[68]: FlowChecker is a tool that can identify intra switch misconfigurations. This tool can used to: (a) verify the consistency of different switches and controllers across different SDN infrastructures using OpenFLow, (b) validate the correctness of the FlowTable configurations of new deployed protocols and

[61] J. Matias, J .Garay, A. Mendiola, N. Toledo, E.; Jacob. FlowNAC: Flow-based Network Access Control. In proceedings of Third European Workshop on the Software Defined Networks (EWSDN), 2014

[62] D. Levin, et al. Toward Transitional SDN Deployment in Enterprise Networks. In Proceedings of the Open Networking Summit (ONS), 2013.

[63] http://www.radware.com/Products/DefenseFlow/

[64] http://h17007.www1.hp.com/docs/interopny/4aa4-3871enw.pdf

[65] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker. NOX: Towards an Operating System for Networks. ACM SIGCOMM Computer Communication Review, 38(3):105–110, 2008.

[66] S. Shin, et al. "Rosemary: A robust, secure, and high-performance network operating system." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014.

[67] S. Shin, et al. "FRESCO: Modular Composable Security Services for Software-Defined Networks." NDSS. 2013.

[68] Al-Shaer, Ehab, and Saeed Al-Haj. "FlowChecker: Configuration analysis and verification of federated OpenFlow infrastructures." Proceedings of the 3rd ACM workshop on Assurable and usable security configuration. ACM, 2010.

services, (c) provide debugging information regarding reachability and security problems, and (d) analyse the impact of new configurations (”what-if” analysis).

NICE[69]: NICE is a tool that can automate the testing of OpenFlow applications through a combination of symbolic execution and model checking. NICE utilises model checking techniques and symbolic execution for generating network traffic, which can be used to systematically explore the state space of the entire SDN deployment (switches, controllers, hosts).

Veriflow[70]: Veriflow is a network troubleshooting tool that can be used to find erroneous forwarding rules in an SDN deployment. In addition it can be utilised to prevent misbehaviour caused by such rules to the network. Veriflow provides a layer between SDN controllers and switches that examines network-wide invariant violations in real time as rule are inserted, deleted or modified in a switch.

FortNOX[71]: FortNOX is an extension of the NOX OpenFlow controller specializing in providing role-based authorization and enforcing security constraints on the controller. FortNOX consists of a mediation service that performs verification of OpenFlow Application rules against a set of network flow constraints that have been defined by administrators or OpenFlow security applications. This mediation service cannot be bypassed.

FLOVER[72]: FLOVER is a model checking system, which can be used to verify that flow policies deployed by an OpenFlow application do not violate network security policies.

Se-Floodlight[73]: Security Enhanced (Se) Floodlight is an implementation of an OpenFlow security mediation service for enforcing network security. It is similar to FRESCO except there is more functionality due to the extensions set by the new OpenFlow specification.

FatTire[74]: FatTire is a programming language designed for writing fault resilient network application programs. It utilizes n-regular expressions that allow programmers to exclusively specify sets of legal paths through the network and fault resilient requirements for those paths.

AVANT-GUARD[75]: AVANT-GUARD is a data plane extension consisting of an actuating triggers and a Connection migration module. AVANT-GUARD is designed to make SDN security applications more scalable and consequently capable of tackling a dynamic range of network threats. The connection migration module provides shielding to the control plane from saturation attacks to the interface between control and data plane (SBI API). The actuating triggers module enables the data plane to asynchronously report network

[69] M. Canini, et al. "A NICE Way to Test OpenFlow Applications." NSDI. Vol. 12. 2012.

[70] A. Khurshid, W. Zhou, M. Caesar, and P. B. Godfrey. VeriFlow: Verifying Network-wide Invariants in Real Time. In Proceedings of the First ACM Workshop on Hot Topics in Software Defined Networks, pages 49–54, 2012

[71] Al-A Porras, Philip, et al. "A security enforcement kernel for OpenFlow networks." Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012, http://www.openflowsec.org/FortNOX_Sigcomm_HotSDN_2012.pdf

[72] Son, Seuk, et al. "Model checking invariant security properties in OpenFlow." Communications (ICC), 2013 IEEE International Conference on. IEEE, 2013.

[73] Reitblatt, Mark, et al. "Fattire: Declarative fault tolerance for software-defined networks." Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013.

[74] Reitblatt, Mark, et al. "Fattire: Declarative fault tolerance for software-defined networks." Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013.

[75] Shin, Seungwon, et al. "Avant-guard: Scalable and vigilant switch flow management in software-defined networks." Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013.

state to the control plane and provides the ability to activate a flow rules under some predefined conditions. In this way it helps the control plane to manage network flows without delay.

PermOF[76]: PermOF is a highly tuneable permission system that incorporates an as-needed customized permission set and an advanced thread-based isolation mechanism. It can be used to define permissions to control access of OpenFLow controllers from the application layer. Hence, effectively it provides an isolation layer between the application and the control layer in the reference SDN architecture. Network operators can use PermOF to define application permission policies at run time.

7.1.2 Mitigated SDN threats

Our initial analysis has shown that the techniques/tools overviewed above address some of the threats that have been identified for SDN.

The following table (Table 4) shows, which SDN threats are addressed by each of the above techniques/tools. PA in the table indicates that a technique/tool partially addresses the threat. An empty cell in the table indicates that a threat is not addressed according to the initial analysis. It should be noted that the information provided in Table 4 is based only on a review of the documentation of the reviewed tool and has resulted from any form of tool/technique usage or testing.

[76] Wen, Xitao, et al. "Towards a secure controller platform for openflow applications." Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013.

Threat types	Threats	SANE	Ethane	FlowNAC	Panopticon	DefenceFlow	HP Sentinel	Rosemary	FRESCO	FlowChecker	NICE	Veriflow	FortNOX	FLOVER	FatTire	AVANT-GUARD	PermOF
Nefarious Activity / Abuse	Manipulation of Information / Data forging	PA	PA							PA		PA	PA	PA	PA		
	• Routing table manipulations									PA		PA	PA	PA	PA		
	• DNS manipulations																
	• Falsifications of configurations									PA		PA	PA				
	Software/firmware exploits							PA									
	• Controller ○ Kernel flaws (can also be seen as FM threats) ○ Buffer overflows (can also be seen as FM threats) ○ SQL injection (can also be seen as FM threats) ○ XSS (can also be seen as FM threats)							PA									
	• Network element ○ Kernel flaws (can also be seen as FM threats) ○ Buffer overflows (can also be seen as FM threats)																
	Denial of Service (DoS) (can also be seen as OUT threats)	PA	PA		PA	PA					PA			PA	PA	PA	
	• Flooding attack										PA			PA		PA	
	• Amplification attack															PA	

	Remote SDN application exploitation	PA	PA	PA				PA					PA				PA
	• Network visualisation exploitation																
	• Network management																
	• Mobility management																
	• Service provisioning exploitation			PA													
	• Traffic engineering exploitation												PA				
	• Virtual Cloud networking exploitation																
	SDN API exploitation								PA								
	• NBI exploitation																
	• EWBI exploitation																
	• SBI exploitation								PA								
	Malicious Software						PA										PA
	• Virus																PA
	• Malware						PA										PA
	• Worm																PA
	• Trojan																PA
	• Botnet																PA
	• Greyware																PA
	Unauthorised activities	PA	PA	PA				PA	PA	PA			PA				
	• Unauthorised access	PA	PA	PA					PA								
	• Unauthorised installation of software								PA								
	• Unauthorised use of software								PA								

	- Unauthorised administration of devices and systems	PA	PA	PA					PA	PA			PA				
	Virtualisation threats						PA										
	- Virtualised hosts abuse o Denial or Loss of service (can also be seen as OUT threats) o Degradation of service (can also be seen as OUT threats)																
	- Data Center threats o Resource contention (can also be seen as FM and OUT threats) o Abuse of unencrypted data							PA									
	- Network Virtualization Bypass o Unlawful network slice ingress and egress o Slice trespassing			PA													
	Traffic diversion	PA	PA				NC	PA	PA	PA	PA		PA	PA	PA		
	Side channel attack																
	Identity spoofing	PA	PA	PA					PA	PA			PA				
	- SDN o Controller o Network element	PA	PA	PA					PA	PA			PA				
	- Network administrators			PA					NC								
	- Network operators			PA					NC								

	Software/firmware exploits							PA	PA								PA
	• Controller							PA	PA								PA
	• Network element																
	Memory scraping (can also be seen as NAA threat)						PA										PA

Threat types	Threats	SANE	Ethane	FlowNAC	Panopticon	DefenceFlow	HP Sentinel	Rosemary	FRESCO	FlowChecker	NICE	Veriflow	FortNOX	FLOVER	FatTire	AVANT-GUARD	PermOF
Eavesdropping / Interception / Hijacking	Virtualisation threats						PA										
	Virtualised hosts abuse • Unauthorised access • Loss of control of virtualised function																
	Data Center threats • DC Traffic spoofing • Inter VM attack																
	Network Virtualization by-pass • Unlawful network slice ingress and egress • Slice trespassing			PA													
	Traffic sniffing						PA	PA	PA	PA	PA		PA	PA			
	Mobile 5G user interception																
	• User Emulation																

	• Spectrum sensing data falsification (can also be seen as NAA threat)																
	• MAC attack																
	Man in the middle	PA	PA														PA
	• In NBI	PA	PA														PA
	• In EWBI																
	• In SBI	PA	PA														
	Interception of Information						PA										
	• Espionage ○ Nation State ○ Corporate																
	• Rogue Hardware																
	• S/W Interceptions						PA										

Table 4 - SDN threats addressed by different techniques/tools

An overview of the way in which each tool/technique addresses specific threats is given below:

SANE provides mitigations for the following threats:

- *Manipulation of Information / Data forging:* The network is based on a domain controller that provides an authentication service to every node on the network. A Network Service Directory (NSD) replaces classical DNS in SANE based deployments. NSD maintains an access control list for every service.
- *Denial of Service (DoS):* SANE includes capabilities for DDoS prevention. SANE hosts do not exchange information with network elements but receive the so called “capabilities” for the domain controller, which are constructed on–route.
- *Remote SDN application exploitation:* SANE based networks require authentication of all principals (hosts, switches etc.) using symmetric key encryption in order to ensure secure communication.
- *Unauthorized access, unauthorized administration of devices and systems*: SANE addresses unauthorized activities using the Access Control List (ACL) that it incorporates. To access network resources in SANE, a host has to be authorized and have the required policies in the ACL that permit requesting the so called network capabilities. In addition, encryption is used for the distribution of network capabilities.
- *Traffic diversion*: Routing in SANE is done by the domain controller that encrypts route information (next hop) in a SANE header in every packet. In SANE, only the domain controller records and maintains a complete view of the network topology.
- *Identity spoofing*: SANE networks implement authorization and symmetric key encryption and an access control list for every network node (host, switches etc.)
- *Man in the middle in NBI and SBI*: SANE networks implement authorization and symmetric key encryption and access control list for every network node (host, switches etc.)

Ethane provides mitigations for the following threats:

- *Manipulation of Information / Data forging*: Ethane networks are based on a central controller. Computes route information for the permitted flows by having knowledge of the network topology. Ethane does not allow any communication between end hosts without explicit permission.
- *Denial of Service (DoS)*: Ethane networks allow initial data exchange only to the controller in order to grant network access. Unauthorized packets are dropped by the switching elements.
- *Remote SDN application exploitation*: Ethane establishes that a misbehaving node cannot masquerade as the controller or a network element (switch or router) by utilizing authentication with preconfigured credentials. Communication between the controller and the network element is established only after authentication is successful. This communication is done via an encrypted connection and it facilitates all communications between the controller and the network element.
- *Unauthorized access, unauthorized administration of devices and systems*: Ethane establishes that a misbehaving node cannot masquerade as the controller or a network element (switch or router) by utilizing authentication with preconfigured credentials. Communication between the controller and the network element is established only after authentication is successful. This communication is done via an encrypted connection and it facilitates all communications between the controller and the network element.
- *Traffic diversion*: Routing is performed by the controller which has all the topology information of the network. Only the controller can alter data flows by controlling the switching elements trough encrypted links.
- *Identity spoofing*: Authentication is mandatory to access network resources.
- *Man in the middle in NBI and SBI*: Communications are encrypted with predefined keys.

FlowNAC provides mitigations for the following threats:

- *Service provisioning exploitation*: There is an authorization mechanism that checks every service requested by a user.

- *Unauthorized activities*: Users have to be authenticated and authorized for each individual service. All frames coming from the user are individually evaluated and categorized in services. Afterwards, an allow or deny judgment is enforced for each of these frames conditional on whether the associated service is permitted or not.

- *Identity spoofing:* Identity of every applicant that asks for a service is checked. This can be done on the first access and periodically. This covers user and administration access.

- *Network Virtualization bypass, Unlawful network slice ingress and egress*: No authenticated service (or corresponding flow) is allowed to enter, or even leave, a slice.

Panopticon provides mitigations for the following threats:

- *Denial of Service (DoS)*: Panopticon proposes hybrid SDN – non SDN network architecture. As an abstraction layer, Panopticon is responsible for hiding the legacy devices and acts as a “network hypervisor” that maps the logical SDN abstraction to the underlying hardware, being able to prevent or mitigate this kind of attacks.

DefenseFlow provides mitigations for the following threats:

- *Denial of Service (DoS)*: DefenseFlow incorporates a patented behavioural fuzzy logic detection algorithm which is able to detect different types of network DDoS attacks.

HP Sentinel security provides mitigations for the following threats:

- *Malicious software – Malware*: HP Sentinel security incorporates detection capabilities for about 700,000 malicious malware, spyware, and botnet threats.
- *Virtualization threats*: HP Sentinel security provides support for the Threat Protection System (see below) in virtual environments. HP provide the Sentinel security application for HP Virtual Application Networks SDN Controller.
- *Traffic sniffing*: In an HP Sentinel security environment an SDN controller forwards new IP connection requests to a Threat Protection System (TPS). TPS uses a reputation database to check the requests and replies with a pass/fail request to the controller.
- *Interception of information – S/W interceptions, Memory Scrapping*: HP Sentinel security provides real-time threat detection and security policy enforcement at the edge of the deployed network.

Rosemary provides mitigations for the following threats:

- *Remote SDN application exploitation*: Network applications are isolated from the core of the Rosemary operating system. In addition, Rosemary utilizes sandboxing functionality to protect the network operation system.
- *Unauthorized activities*: Rosemary establishes whether an application has rights to access or modify a data structure. If an application can not access the data structure, it will not be able to get the necessary capability.

- *Traffic diversion*: To alter flow tables in a Rosemary Environment, an application has to gain access permission from the NOS.
- *Software/firmware exploits - Controller*: As discussed for the case of remote SDN application exploitation, in Rosemary network applications are isolated from the core of the Rosemary operating system. In addition, Rosemary utilizes sandboxing functionality to protect the network operation system.
- *Traffic sniffing*: To alter flow tables in a Rosemary Environment, an application has to gain access permission from the NOS.

FRESCO provides mitigations for the following threats:

- *SBI exploitation*: Fresco controllers must be authorized and use encryption to communicate with the network switching elements.
- *Unauthorized activities, Memory scraping*: Fresco uses a Security Enforcement Kernel (SEK).
- *Traffic diversion*: When a conflict appears, the FRESCO Security Enforcement Kernel applies a hierarchical authority model that provides the capability to replace an existing flow rule with a candidate rule, if the digital signature of the source of the candidate rule possesses more authority than the source of the existing rule.
- *Identity spoofing*: FRESCO applications (aka modules) are created using a scripting language. FRESCO incorporates a script-to-module translator, which automatically translates the scripts to modules, creates instances of the modules, and validates and registers the modules using a registration API. This API allows only authorized administrators to create FRESCO modules.
- *Controller firmware/software exploits*: Applications in FRESCO access the SDN controller through the Security Enforcement Kernel.
- *Traffic sniffing*: The FRESCO Security Enforcement Kernel utilizes a trust model that empowers FRESCO modules to digitally sign each candidate flow rule. This permits SEK to conclude whether a candidate flow rule was produced by a FRESCO security module, an OpenFlow application, or a network administrator.

FlowChecker provides mitigations for the following threats:

- *Routing table manipulations, Falsifications of configurations, Traffic diversion, Traffic sniffing*: Flow checker is able to validate the correctness of the flow tables and configuration of the SDN switching devices.
- *Unauthorized administration of devices and systems*: FlowChecker uses SSL to communicate with the SDN controllers in the network.
- *SDN Identity spoofing*: A controller has to subscribe to the FlowChecker (called master controller). In addition there is the possibility that flow tables are stored in a Database with role based access control.

NICE provides mitigations for the following threats:

- *Flooding attack*: NICE is capable of checking for generic correctness properties such as no forwarding loops or no black holes, and when required write additional application-specific correctness properties. Python code snippets that make assertions about the global system state, can be utilized.
- *Traffic diversion, Traffic sniffing*: NICE outputs property violations along with their traces so that they can be deterministically reproduced.

VeriFlow provides mitigations for the following threats:

- *Routing table manipulations, DNS manipulations*: VeriFlow resides between the SDN applications and SDN devices in order to capture and check every flow rule entering the network.
- *Falsifications of configurations*: VeriFlow search for erroneous rules issued by SDN applications, and when required, prevents them from reaching the SDN network and causing irregular network behaviour or even damage.

FortNOX provides mitigations for the following threats:

- *Routing table manipulations:* FortNOX has the ability to enforce network flow rules produced by OF-enabled security applications that request to reprogram switches in response to potential runtime operational threats.
- *Falsifications of configurations*
- *Traffic engineering exploitation*: FortNOX uses a rule conflict resolution for the flow rules with authorization levels (rolls)
- *Unauthorised administration of devices and systems*: FortNOX incorporates an authentication mechanism.
- *Traffic diversion, Traffic Sniffing*: Digital signature validation is performed for each flow rule insertion request via a role-based source authentication module. This may lead to assignment of appropriate priority to a candidate flow rule, or even the lowest priority in the event that no signature is provided.
- *SDN Identity spoofing*: FortNOX supports digital signatures for each flow rule inserted in the SDN switching devices.

FLOVER provides mitigations for the following threats:

- *Routing table manipulations*: Flow tables are sent to the switching elements over an encrypted network link.
- *Flooding attack*: FLOVER ensures consistency with the current network security policy for the flow rules inserted in a switch's flow table(s).
- *Traffic sniffing and Traffic diversion*: FLOVER decomposes network security policies in sets of assertions referred to as non-bypass properties. Non-bypass properties specify whether a certain packet/flow matching a set of conditions should be forwarded to its destination or otherwise dropped. Yices, a Satisfiability Modulo Theories solver, is used to check for non-bypass property violations.

FatTire provides mitigations for the following threats:

- *Routing table manipulations*: FatTire features logic that facilitates reasoning about the behaviour of the system during periods of failure recovery. This enables verification of network-wide invariants.
- *Denial of Service*: FatTire incorporates modules (outcome) that on OF switches and can take advantage of in-network fast-failover mechanisms.
- *Traffic diversion*: The FatTire compiler generates rule tables and group tables that enable fault-tolerance while at the same time guaranteeing that traffic flows along the paths specified by the program.

AVANT-GUARD provides mitigations for the following threats:

- *Falsifications of configurations*: Intelligence empowered connection mitigation, differentiates sources that will complete TCP connections from sources that will not, at the data plane level.
- *Denial of Service*: A classification stage performs connection mitigation which shields the control plane from failed connection floods on the client-side. Such connections may be the product of DoS attacks or reconnaissance activities.
- *Traffic diversion*: AVANT-GUARD employs triggers that introduce conditional flow rule activation. Security applications can predefine a set of actions and strategies for handling flows that appear as a product certain network operating conditions that can be expressed through switch statistics.

PERMOF provides mitigations for the following threats:

- *Malicious Software*: PermOF introduces a shim layer that is configured and controlled by the controller kernel. This ensures isolation of and achieves zero interaction between the applications and the OS. This feature is a product of modifying the dynamic library of the programming language or the OS itself.
- *Remote SDN application exploitation*: to ensure the application authenticity and integrity, PKI-based authentication may be enforced.
- *Controller Software/firmware exploits, Memory scraping*: An Isolation mechanism, including a system permission set, is introduced by PERMOF. With PERMOF Third party SDN applications are operating under minimized privileges
- *Man in the middle in NBI*: When an API call is received from the application, a thread class encapsulates the function call and passes it to kernel. This is done by utilizing the built-in inter-thread communication facility. As the caller's identity is attached on the API calls, the controller's kernel can easily perform permission control, based on a pre-configured policy.

7.2 Threat mitigation practices under development

In the following, we present practices for threat mitigation in SDN/5G that are under development. Several good practices may relate and address more than one threat. In the context of this report all 5G-PPP Phase 1 projects, that consist of fifteen Research and Innovation action projects and three Innovation action projects of HORIZON 2020 in the area of Information and Communication Technologies[77] have been asked to provide their input.

7.2.1 Related 5G-PPP HORIZON 2020 projects

VirtuWind[78] is aimed at developing an open, modular and secure framework to support intra-domain and inter-domain scenarios in real wind parks based on SDN and NFV. The choice of the domain reflects the emergence of wind energy as a mainstream form of sustainable energy generation. VirtuWind adopts a security-by-design approach for the SDN and NFV ecosystem. This appears to be necessary as introducing

[77] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/information-and-communication-technologies

[78] http://virtuwind.eu/

revolutionary concepts like SDN and NFV for critical infrastructures requires a careful investigation of new security risks, which have not been relevant in legacy systems. In this context, VirtuWind has the objective of: (i) establishing a comprehensive threat and risk framework for industry-level SDN networks, (ii) defining security mechanisms for north-/southbound and inter-controller interfaces, securing the controller (e.g., prevent DoS), (iii) developing mechanisms for network monitoring and intrusion detection for SDN networks, (iv) developing Signed Virtual Network Functions, (v) developing accountability mechanisms for SDN networks, and (vi) developing inter-domain incident detection mechanisms.

SUPERFLUIDITY[79] is working on security verification of virtualized network functions, using symbolic execution techniques. This is a technique (from SW compilers) which permits to automatically and systematically explore paths, so as to verify what the security and policy implications are when running certain (composition of) functionalities. In the past such techniques have been successfully applied to specific middlebox functions[80] (for instance, middleboxes that rely on the composition of standard Click elements). The work in progress in SuperFluidity focuses on generalizing and extending these techniques to a wider heterogeneous set of VNF (which in turns means a dedicated work devised to characterize the I/O relation of such VNFs); cloud enabled VNFs; and support for heterogeneous/multi-operated settings.

CHARISMA[81] As indicated in the project's website[77], CHARISMA proposes "an intelligent hierarchical routing and paravirtualised architecture that unites two important concepts: devolved offload with shortest path nearest to end-users and an end-to-end security service chain via virtualized open access physical layer security (PLS)." The use of a cloud infrastructure in CHARISMA is aimed at achieving low-latency ("<1ms" according to the project consortium) and the security required for future 5G networking in which wireless/wired communications converge. The project aims to deliver enhanced performance targeting a "1000-fold increased in mobile data volume, 10-100 times higher data rates, 10-100 times more connected devices" and 5-fold reduction of latency.

5G NORMA[82] is aimed at developing a novel, adaptive mobile network architecture, capable of accommodating 5G. The focus of this architecture will be to support network customisability whilst ensuring high performance and security, and meeting specific cost and energy requirements. 5G NORMA is also aimed at offering openness based on appropriate APIs.

5G ENSURE[83] focuses on the development of a security architecture for 5G that would be acceptable to and shareable by different 5G stakeholders. To realise this vision, 5G ENSURE has the goal of developing security enablers for 5G and making them available in a shared testbed. The project aims to develop these enablers driven by security use cases and scenarios in the areas of cybersecurity and aerospace.

CogNet[84] aims to develop support for intelligent 5G Network Management whilst increasing dramatically the extent of connected devices (the aim is to achieve connectivity of trillions of devices). This requires the creation of highly optimised networks, are capable of making maximum use of available radio spectrum and bandwidth. The same need arises due to the need to meet other QoS properties for such networks. To achieve these requirements CogNet also aims to develop self-managed networks, based on machine learning techniques that can address relevant organisation, configuration, security, and optimization

[79] http://superfluidity.eu/
[80] http://nets.cs.pub.ro/~costin/files/symnet.pdf
[81] https://5g-ppp.eu/charisma/
[82] https://5gnorma.5g-ppp.eu/
[83] http://www.5gensure.eu/
[84] http://www.cognet.5g-ppp.eu/

issues. Additional elements of CogNet's vision are the use virtualisation (as a means for meet changing resource demands) and energy efficiency.

7.2.2 Other related EU funded projects

BEBA[85] project aims to entail platform-agnostic programming of stateful flow/traffic processing logic directly within network nodes, thus rescinding the today's necessary reliance on external (slowpath) controllers. Moreover, BEBA will provide the programmers with the ability to control, via the above stateful behavioural descriptions, an extended set of actions and primitives specifically devised for the monitoring and network security domain, so as to permit platform-agnostic programming of middle box-type network functions. In terms of security, BEBA project aims to mitigate DoS/latency attacks to the control-data plane communication channel (concretely, the communication channel between centralized controller and remote SDN devices).

NetIDE[86] aims at delivering an integrated development environment that aims to support the whole software development lifecycle of SDN applications in a vendor- and controller-independent fashion. The NetIDE framework should represent a single point of entry to SDN software development and offer a unified development environment following the 'write once, execute anywhere' paradigm. The project has already delivered a first open source release of the framework which includes: (i) the NetIDE Development Environment, an Eclipse-based integrated environment for developers; (ii) the NetIDE Network Engine, a controller-agnostic environment where SDN applications for different controllers can be deployed on top of the same infrastructure; (iii) a set of NetIDE Tools enabling developers to systematically test, profile, and tune their network applications (logger, debugger, a wireshark dissector and many others). These tools are designed to offer considerable benefits when troubleshooting in a productive environment after application deployment.

FP7 UNIFY[87] project considers that every Service Graph (SG) or Network Function - Function Graph (NF-FG) deployment started by a Resource Orchestrator needs to be enforced in relation to a policy. This approach assures not only that services are deployed only by principals according to a policy, but also that resources (computing and network) are consumed in a policy compliant way. This eliminates resource starvation attacks.

FLAMINGO[88] is a European (ICT-FP7) Network of Excellence (NoE) investigating Network and Service Management. As a NoE, FLAMINGO is based on a joint program of integrated research activities, whose objective has been to investigate and address three challenges deemed important for the Future Internet (FI). FLAMINGO identified these challenges as: (a) the development of scalable monitoring systems that can effectively support the sharing of monitoring data the "knowledge plane" and decision algorithms of the Future Internet; (b) the development of automated and self-management frameworks for managing networks and their interconnected objects in a fully distributed and autonomic manner, and (c) the investigation of "economic, legal, and regulative constraints" that arise in border management systems and can affect FI.

In Table 5 below we give a summary of measures related to the SDN threat landscape that the 5G PPP H2020 and the other EU funded projects reviewed above have aimed to develop.

[85] http://www.beba-project.eu/

[86] http://www.netide.eu/

[87] https://www.fp7-unify.eu/

[88] http://www.fp7-flamingo.eu/

Measures to be developed by Research and innovation Projects	Related 5G-PPP Projects							Other EU funded projects		
	VirtuWind	SUPERFLUIDITY	CHARISMA	5G Norma	5G ENSURE	CogNet	BEBA	NetIDE	FP7 UNIFY	FLAMINGO
Threat analysis/assessment to be conducted	x									
Cryptographic and/or key management mechanisms	x									
Authentication/Access control mechanisms	x								x	
Data encryption mechanisms	x								x	
Secure communication mechanisms including VPN	x								x	
NBI security mechanisms	x									
EWBI security mechanisms	x									
SBI security mechanisms	x									
Hardware security mechanisms (controller/data elements/mobile device)	x									
Mobile device security mechanisms										
Mechanisms for the protection of Virtual Network Functions	x								x	
Non-repudiation/audit/traceback mechanisms										x
Intrusion detection mechanisms	x									x
Incident detection and response mechanisms	x									
Multi-operator cooperation mechanisms	x									
Wireless/Mobile Security (wireless medium) mechanisms										x
Legal and business measures										
Standardization measures	x									
Policy measures	x								x	x
Other (please specify, add additional rows in the table if necessary)										

Table 5 - Involvement of 5G-PPP HORIZON 2020 and other EU founded projects to the SDN threat landscape

7.3 Gap Analysis

Based on the SDN threat mitigation practices that have been developed in existing research or constitute the target of on-going research projects, we have identified gaps that appear to require further research and development effort in order to address 5G/SDN threats. The outcome of this gap analysis is presented in Table 6. The table provides also a summary of good practices and the assets covered by them and clusters good practices, assets and gaps under the different types of threats that were introduced in Sect. 5.6.

Threats	Good practices	Assets Covered	Gaps
Nefarious Activity/Abuse			
Manipulation of Information / Data forging	• Authentication of network nodes • Network service directory with access control list • Centralization of control • Encryption in the SBI • Validation and/or check of flow table entries • Middleware that intercept and check every rule • Faulty rule checking • TCP connection validation	• Data plane data • Control plane data • Application plane data	*Issues*: • System configuration • Security Policy *Stakeholders:* • Administrators
Software/firmware exploits	• Isolation mechanisms between layers • Network application detached from NOS core • Forcing privileges to applications	• Data plane software • Control plane software	Issues: • Lack of comprehensive verification for absence of software/firmware exploits *Stakeholders:* • Developers • Administrators
Denial of Service (DOS)	• Domain controllers for DDoS prevention • Initial data exchange only to the controllers • Network hypervision • Fuzzy DDoS detection • Rule violation checking mechanisms • Rule consistency check • Fast failover mechanisms. Classification stage that perform connection mitigation	• Data plane, • Control plane • Application plane • Service Provider IT infrastructure • SDN users	*Issues*: • System configuration • Network configuration
Remote SDN application exploitation	• Authentication • Encryption • Preconfiguration of credentials • Authorization on per service basis	• Application plane	*Issues*: • Credentials *Stakeholders:* • Operators

	• Sandboxing		• Administrators
SDN API exploitation	• Encryption • Authorization	• Data plane, • Control plane, • Application plane	*Issues*: • Security Policy *Stakeholders:* • Administrators
Malicious Software	• Shim layer between dynamic libraries and NOS	• Data plane, • Control plane, • Application plane, • SDN user, • Service provider IT Infrastructure, • SDN users, • Human agents	*Issues*: • System configuration *Stakeholders:* • Developers • Administrators
Unauthorised activities	• Access control list • Encryption • Application policies	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Network service provider physical infrastructure • SDN user • Human agents	*Issues:* • Security Policy • Credentials *Stakeholders:* • Operators • Administrators
Virtualisation threats	• Domain controller with encryption • Security applications • Real time threat detection	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure Network service provider physical infrastructure • Human agents	*Issues:* • Security Policy *Stakeholders:* • Administrators
Traffic diversion	• Flow tables under NOS access control • Hierarchical authority model for rules • Rule violation checking mechanisms • Run time flow generation as a threat response • Candidate rule prioritization • Non by-pass security policies	• Data plane • Control plane • SDN user	*Issues:* • Network configuration *Stakeholders:* • Administrators

	• Fault tolerant group tables • Conditional flow rule activation		
Eavesdropping/Interception/ Hijacking			
Side channel attack	-	• Data plane, • Control plane • SDN user	*Issues:* • Threat as stated *Stakeholders:* • Administrators • Developers
Identity spoofing	• Encryption • Mandate authentication • API that mandates authorization for application installation	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • SDN user • Human agents	*Issues:* • Security Policy • Credentials *Stakeholders:* • Administrators
Software/firmware exploits	• Isolation mechanisms between layers • Network application detached from NOS core • Forcing privileges to applications	• Data plane software • Control plane software	*Issues:* • Lack of comprehensive verification for absence of software/firmware exploits *Stakeholders:* • Developers • Administrators
Memory scraping	• Application Isolation • Real time threat detection	• Data plane • Control plane • Application plane	*Issues:* • System configuration • Security Policy • Credentials *Stakeholders:* -
Virtualisation threats	• Domain controller with encryption • Security applications • Real time threat detection	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure Network service provider physical infrastructure • Human agents	*Issues:* • Security Policy *Stakeholders:* • Administrators

Traffic sniffing	• Reputation database • Digital signing of rules • Run time flow generation as a threat response • Non by-pass security policies • Conditional flow rule activation	• Data plane • Control plane • Application plane • SDN user	*Issues:* • Network configuration • Security Policy *Stakeholders:* -
Mobile 5G user interception	-	• Data plane • SDN user (when wireless communication is used)	*Issues:* • Threat as stated *Stakeholders:* --
Man in the middle	• Authorization • Symmetric key encryption • Predefinition of keys • Inter-thread-communication encapsulation	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Human agents	*Issues:* • Network configuration • Security Policy *Stakeholders:* --
Interception of Information	• Real time threat detection • Security policy enforcement • Run time flow generation as a threat response	• Data plane • Control plane • Application plane • SDN user • Service provider IT Infrastructure • Human agents	*Issues:* • System configuration • Network configuration • Security Policy *Stakeholders:* --

Table 6 - SDN/5G Good practices and gaps

A more detailed account of the issues and stakeholders referenced in the gaps identified in Table 6 is provided below:

- **System configuration:** System configuration refers to the proper installation and configuration of systems/devices and applications within the SDN infrastructure. In order to achieve desired levels of variables such as performance, stability, proper function and security, industry as well as community emerging guidelines must be utilized.
- **Security Policy:** The definition, management, monitoring and enforcement of adequate security policies is of paramount importance when it comes to operation and management of SDNs. Such policies are needed to address important SDN operation and management activities including, for example, authentication between SDN components or establishing the means for proper authentication between humans and devices. Without carefully defined and orchestrated security rules and procedures, it is impossible to imagine a functional and reliable SDN infrastructure. A key related issue is also the provision of automated support for the short and long term evolution of security policies.
- **Network configuration:** In contrast to System configuration which refers to the setup of the SDN components, Network configuration refers to the SDN specific configuration that is applied to each of these components. Whether setting up or maintaining an SDN infrastructure, proper configuration and ongoing tuning is of outmost importance in order to achieve proper function, stability and performance. The SDN components affected are the SDN controllers and the SDN network elements (switches and routers).
- **Credentials:** While Security Policy is the most important aspect when it comes to laying the ground rules for a secure SDN infrastructure, the importance of proper and protected Credentials is a must. Credentials in the form of a password or a certificate are the gateway that can lead to accessing an important system or network asset and in this case a functional component in the SDN infrastructure. When applied properly and used carefully there can be no harm to the protected assets. However, weak as well as improperly or poorly formed Credentials can lead to exploitation and ultimately to a global infrastructure meltdown. The human factor is largely responsible as Credentials can be leaked due to sharing with unauthorized individuals or theft as a result of improper placement.
- **Comprehensive verification of absence software/firmware exploits:** Verifying the absence of potential exploits in software/firmware (e.g., buffer/stack/heap overflows) is an important requirement for providing security assurance for SDN software/firmware[89]. So far, numerous techniques have been used for this purpose, including static verification techniques that operate on software specifications (typically including model checking, invariant checking and theorem proving), static analysis of various forms of software/firmware code and testing. Static verification techniques can check certain properties (e.g., satisfaction of access control policies, properties of virtual and physical topologies such as desired traffic isolation) but not all. More specifically, certain types of exploits, such as range errors and string vulnerabilities, cannot be easily expressed as properties amenable to static verification techniques. Furthermore, such techniques are often

[89] ITU-T, Requirements for Applying Formal Methods to Software Defined Networking, Recommendation ITU-T Y.3320, 08/2014, available from: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwjDqoSqjLjJAhXDMhoKHSJaAFIQFghCMAQ&url=https%3A%2F%2Fwww.itu.int%2Frec%2Fdologin_pub.asp%3Flang%3De%26id%3DT-REC-Y.3320-201408-I!!PDF-E%26type%3Ditems&usg=AFQjCNFHJcb_4iCoKn1UDkyaleOn25ZPSw

incapable of verifying systems of non-trivial complexity due to scalability problems, and – even in cases where they are successfully applied – they offer no guarantee that the implementation of the specification analysed by them will preserve this specification and therefore that the desired property. Static analysis techniques have been effective in detecting certain types of exploits (e.g., various types of overflows) but not all of them (e.g., string vulnerabilities and range errors). Furthermore, they are implementation language specific (e.g., C and/or Java specific) and not all of them scale up well to programs of significant size. Finally, testing cannot offer any guarantee of completeness.

- **Operators:** In addition to the Administrators, whose function is described above, the Operators' function is as important as the deal with the day to day activities of maintaining the SDN ecosystem. While Administrators will have to deal with low level support and configuration functions (such as upgrades and enhancements), the Operators will have to perform day to day activities such as monitoring, high level management and light configuration tasks. Because, similarly to the Administrators, the Operators also require security clearance, caution should be used when utilizing SDN Credentials.

- **Administrators:** At the centre of a physical or virtual IT infrastructure are the Administrator teams responsible for the setup, configuration and ongoing maintenance. Similarly to a conventional infrastructure, the Administrators carry the responsibility of establishing an SDN infrastructure that functions as per initial specifications. In addition, performance and security are two important factors that must be addressed from the beginning. Administrators require full security clearance in order to perform low level SDN support and therefore caution should be used when accessing the SDN components.

- **Developers:** SDN depends on Software in order to deliver all the benefits and advantages over a conventional Network infrastructure. It relies on a collection of software pieces that talk to each other through carefully planned interfaces and APIs. The developers responsible for writing these pieces of software carry the responsibility of delivering as per spec, functional, efficient and secure code that will ensure proper function of the SDN device without jeopardizing the SDN ecosystem. This becomes particularly important when upgrading SDN components of on already existing infrastructure.

8. Recommendations

8.1 Technical recommendations

Recommendation 1 (for Network providers): Mandate encryption and authentication in NBI, SBI and EWBI. In SDN deployments, Application Programming Interfaces (API) for the communication between controllers and switching elements (Southbound Interface - SBI) and between controllers and network applications (Northbound Interface – NBI) are utilized. In addition, although SDN uses centralized control of the network (controller) this is a logical architecture that can be distributed into several systems (multiple controller architecture). Communication between SDN controllers is achieved through the East/Westbound Interface (EWBI). Utilizing encryption and advanced authentication in these interfaces is not mandatory for standard implementations. However, network providers should consider deploying encryption and authentication techniques (e.g. TLS) to all SDN APIs.

This recommendation addresses the following gaps:

- Nefarious Activity/Abuse: System Configuration, Security policy, Administrators
- Eavesdropping/Interception/Hijacking: Security policy, Credentials, Administration

Recommendation 2 (for Network providers): Identify and monitor exposed functionalities of SDN controllers. SDN controllers provide northbound APIs (NBIs) that enable network applications to be deployed on top of a unified abstract network layer. These APIs expose the SDN network state to applications and enable applications to dynamically and automatically program the network. Malicious applications can gain access of the network resources by exploiting NBI capabilities. Network providers should be aware of the exposed functionalities of the installed controllers in their deployments. In addition, vulnerable functionalities need to be exposed by sophisticated ways of monitoring the usage of the NBI.

This recommendation addresses the following gaps:

- Nefarious Activity/Abuse: Developers, Administrators, System configuration
- Eavesdropping/Interception/Hijacking: Developers, Administrators

Recommendation 3 (for Network and Service providers): Control and monitor running application resources. The SDN paradigm allows the differentiation of network policies for individual SDN applications. This is important in order to achieve meaningful multi-tenancy in the SDN ecosystem, especially for network providers and even more importantly for service providers. Moreover, SDN introduces a new business model associated to the network and service provisioning (e.g. security as a service). Controlling and monitoring the network resources allocation is a practice that can harden SDN deployments against several threats.

This recommendation addresses the following gaps:

- Nefarious Activity/Abuse: Developers, Administrators
- Eavesdropping/Interception/Hijacking: Developers, Administrators

Recommendation 4 (for Network, Service providers and End users): Holistic Support for Security policies. In the complex SDN ecosystem it is important for service providers to operate based on comprehensive security policies. Although the sophistication and scope of such policies may vary depending on the size and nature of the organization in question, the underlying need for operating on the basis of security policy in all levels of the SDN reference architecture is irrefutable. Having a well-written policy that covers all important areas (e.g. system access, user credentials use and good practises), not only supresses a number of risks but also helps recover from most situations in minimal time. To be effective in terms of security, policies need to have holistic support, i.e., support for their specified, verification, monitoring and enforcement to the maximum possible extend.

This recommendation addresses the following gaps:

- Nefarious Activity/Abuse: Developers, Administrators, Operators, Security Policy
- Eavesdropping/Interception/Hijacking: Developers, Administrators, Operators, Security Policy

Recommendation 5 (for Administrators): Access control, Credentials, System updates: The SDN ecosystem consists of several components (e.g. controllers, servers, switching elements). These components may be either virtualized or physical systems and need to communicate with each other. Restrictions of access based on access control lists could harden overall system security. In addition, SDN system and network administrators should enforce a minimum level of security in the system security policies.

This recommendation addresses the following gaps:

- Nefarious Activity/Abuse: Security Policy, Administrators
- Eavesdropping/Interception/Hijacking: Operators, Credentials

Recommendation 6 (for Developers): Sandboxing, Application Isolation. Logically centralized control of the SDN makes it possible for developers to develop custom network applications that perform complex tasks. SDN offers a high level of abstraction to the programmers. When applications are developed caution is required to protect the network operation against application misbehaviour and bugs. To do so techniques such as Sandboxing, application-Kernel isolation and application permission policy enforcement should be utilized.

This recommendation addresses the following gaps:

- Nefarious Activity/Abuse: Developers, Administrators, System configuration
- Eavesdropping/Interception/ Hijacking: Operators

8.2 Organisational recommendations

Recommendation 7 (for Service providers): Develop incident response capabilities and information sharing practices among telecom operators. It is advisable that Telecom Operators develop incident response capabilities by creating (and in case of existing, enhancing) in-house Computer Emergency Response Teams (CERTs) or Computer Security and Incident Response Team (CSIRT), that will be technologically aware of evolving networking technologies, with a particular focus on SDN and NFV. It would be advisable that an assembly or an informal association of Telecom Operator CERTs/CSIRTs is established, as they could function as an information sharing catalyst for Telecom Operators. ENISA could play an instrumental role in this direction[90]. Cooperation with other incident response bodies such as Terena's Task Force CSIRT (TF-CSIRT)[91] and the European Government CERT Group[92] as well as participation in international communities such as the global Forum for Incident Response and Security Teams-FIRST[93] would be highly advisable for every Telecom Operator.

This recommendation addresses the following gaps:

- Nefarious Activity/Abuse: Security Policy
- Eavesdropping/Interception/ Hijacking: Security Policy

Recommendation 8 (for Administrators): Keep systems up to date. As SDN moves many of the networking functionalities in a software environment it is of paramount importance that used systems (Servers, Virtual servers, Network operating systems, Authentication and encryption mechanism etc.) are continuously updated with the latest releases (e.g. Security patches). To do so system and network administrators should schedule periodic system maintenances. During maintenance service availability should not be decreased so redundancy in the network architecture should be taken into account.

This recommendation addresses the following gaps:

- Nefarious Activity/Abuse: System configuration, Network configuration
- Eavesdropping/Interception/ Hijacking: System configuration, Network configuration

Recommendation 9 (for Network and Service providers): Use adequate security methods. Network and service providers should maintain a high level of security in their systems. Specialized software and hardware solutions are available and should be taken into account. In addition SDN provides the capability of security as a service, allowing network and service providers to outsource security to specialized third party vendors.

This recommendation addresses the following gaps:

- Nefarious Activity/Abuse: Administrators, Security Policy
- Eavesdropping/Interception/ Hijacking: Operators, Security Policy

[90] https://www.enisa.europa.eu/activities/cert/support
[91] https://www.terena.org/activities/tf-csirt/
[92] http://www.egc-group.org/
[93] http://www.first.org/

9. Conclusions

SDN/5G brings a brand new level of innovation to arena of networking. Key attributes such as Logically Centralized Intelligence, Programmability and Network Abstraction pave the way to the communications of tomorrow. While significant improvements may be achieved in network security by centralization and programmability, these two great attributes will undoubtedly attract a new level of treats and attacks.

Security within the SDN paradigm will arguably be a challenge, as all layers, sub-layers and components will need to communicate according to strict security policies. In this report, we have attempted to create awareness by identifying key valuable assets of the SDN infrastructure that are needed in order to ensure proper network function and interoperability. As these assets may, however, become the target of attacks, they can also become the main driver of a threat analysis targeted at securing SDNs.

Annex A: Description of SDN/5G Assets

- ***Data Plane assets*** – i.e., physical network devices e.g., routers and switches
    - Network Elements – i.e., devices that connect electrically and logically other networked devices by forwarding and/or routing data to them using the address of these devices; can be virtual
        - Hardware
            - I/O – i.e., hardware to input and output packets e.g., Ethernet port
            - CPU – i.e., central processing unit that process packet switch and routing
            - Memory – i.e., volatile and non-volatile memory of the switch or router pretium mattis, nunc.
        - Software
            - Control - Dara-Plane-Interface agent (CDPI agent) – i.e., the software component that realises the northbound API of the network elements
            - Forwarding engine – i.e., the software component that forwards packets to realise a data path
            - Firmware – i.e., software that controls switch resources and is in charge to perform changes in the forwarding state (additions/deletions of flow table entries)
            - Audit agent - i.e. the software in charge of providing accountability and traceability (e.g. logging, and notifications).
            - Cryptographic components that provide encryption services to the communication with the controlers
        - Data
            - Flow States –i.e g. the data held in a network node to determine where packet data should be forwarded and/or which actions should be performed on ingress/egress packets; such data should also include matching rules and relevant verification, with specific attention to the check of malformed packets which otherwise could be used as possible attack channel
            - Flow Statistics – i.e., the data held in counters and tracking the amount of packets/bytes received for a flow, and the relevant associated triggers when applicable (e.g. OpenFlow v1.3+ meters, etc)
            - Stored packets – i.e., packets stored temporarily in a switch or router (e.g., store-and-forward functions, misc. analysis, QoS, per-packet consistency for the purpose of security); available only for switched operating at certain OSI levels
    - Communication medium
        - Wired (SDN backbone)
            - Fibber Optic – i.e., a cable containing one or more optical fibres that are used to carry information as light pulses
            - Twisted pair – i.e., copper based cables e.g., Ethernet cable
        - Wireless (Radio Access)
            - 5G radio access mechanisms – i.e., mechanisms to control multiuser radio access
                - Cognitive radio access/Software defined radio
                - Spectrum Sensing mechanisms – i.e., mechanisms that sense frequency band occupancy
                - Spectrum analysis mechanisms – i.e., mechanisms that analyse frequency spectrum

                - Spectrum allocation mechanisms – i.e., mechanisms that select frequency for transmitting
            - 5G Base stations – i.e., the infrastructure used to provide wireless access to users
            - Mobile/wireless end user devices – i.e., customer owned mobile devices

- ***Control Plane Assets*** – i.e., assets controlling the creation and destruction of network flows and paths (e.g., OpenDaylight, ONOS realising components)
    - Software
        - Firmware – i.e., hardware specific software
        - File system – i.e., software that control how data is stored and retrieved
        - Operating System – i.e., software that manages computer hardware and software resources
        - Functional components realising the Northbound API (aka “NBI agents”)
            - Translator of SDN application requirements to SDN data paths
            - Network statistics component
        - Functional components realising the East/West bound API
            - Components for Controller State Synchronization
            - Components for Redundancy & High-availability (master-slave controllers)
            - Components for Holistic management of multi-Controller Infrastructure
            - Multiple, alternative controllers to achieve diversity
        - Functional components of South bound API (aka “CDPI drivers”) Controller and Infrastructure Communication:
            - Components realising flow communication to the Data Plane for provisioning physical and network devices
            - Components realising real-time adjustments to the network to meet demands
            - Components realising control to IT and Network Administration in order to maximise Network resource utilization
        - Cryptographic Components that provide encryption to the communication of the controlers to the other SDN elements
    - Hardware
        - Servers - that run SDN controller software
            - I/O - Hardware to input and output information
            - CPU - Central processing unit
            - Memory – i.e., volatile and non volatile memory of the device
    - Data
        - Data flow traffic towards the Data Plane via the Southbound Interface (SBI)
        - SDN Application traffic towards the Application Plane via the Northbound Interface (NBI)
        - Inter-Controller traffic towards other Controllers via the East/West bound Interface (EWBI)
- ***Application Plane Assets***
    - Software
        - Cryptografic Componetns that provide ecrytpion to th communication of the applications with the controlers.
        - Firmware – i.e., hardware specific software
        - File system – i.e., software that control how data is stored and retrieved
        - Operating System – i.e., software that manages computer hardware and software resources
        - SDN Applications
            - Network Visualization Applications – i.e., applications that provide visualization of the complex SDN topology enhancing the ability to monitor and troubleshoot issues

            - Service Provisioning Applications – i.e., applications that provide tailored networking services as required and when needed
            - Network Management Applications – i.e., applications that actively monitor the performance and capacity of all components within the SDN Infrastructure
            - Traffic Engineering Applications – i.e., applications that analyze network traffic and perform intelligent real-time adjustments
            - Mobility Management Applications – i.e., applications that maintain session continuity to mobile users across heterogeneous networks without interruptions
            - Sentinel Security Applications – i.e., applications that provide an on-guard holistic level of security, based on predefined rules and conditions
            - Virtual Cloud Network Applications – i.e., applications that provide on demand shared computing resources within a public cloud environment
            - Load balancing and redundancy Applications – i.e., applications that provide uninterrupted service of high availability through redundant networking resources
            - Energy-efficient Networking Applications – i.e., applications that help reduce power consumption by actively managing unused resources
    - Hardware
        - Servers – i.e., servers that run SDN controller software
            - I/O – Hardware to input and output information
            - CPU - Central processing unit
            - Memory - temporary data storage
- ***SDN users***
    - End user data
        - Audio/video content – i.e., delivery of audio/video content delivered to end users (e.g., video on demand)
        - Voice content – Voice in basic communication services for end users (e.g., mobile phones)
        - End user multimedia communication - communication with audio and video and data support e.g., Skype
        - End user data - file storage for end users e.g., cloud storage
        - IoT and CPS data - Data collected by sensors and CPS actuations
        - Sentinel Security parameters/data – cryptographic hardware components (e.g. SIM card), cryptographic keys including network subscriber keys, security algorithms (e.g. algorithms for authentication and encryption such the ones stored on the SIM card)
    - SLAs and regulations
        - Multi-operator SLAs – SLAs/contracts with other network operators, including mechanisms for their run-time implementation, which enable to access the network infrastructure in different operator domains and provide path-level QoS across different operator
        - SLAs with organizations that are not network operators (e.g. the campus of an organization) - contract between network operator and customer organization that defines the expected level of provided service e.g. data throughput
- ***Service provider IT Infrastructure***
    - IT Infrastructure - Non network related it infrastructure e.g., operator PCs
    - Billing systems - time and billing tracking as well as invoicing customers for services and products
    - Operator data - data related to the operator operation
    - End user data - data belonging to the customers
- ***Network service provider physical infrastructure*** – i.e., physical infrastructure of the network service provider
    - Facilities

        - Premises - operator entire property
        - Buildings - structure on property
        - Network system rooms e.g., closets with network elements
        - Offices - of the operator employees
        - Data centres - facility used to house computer systems
        - Cabling - all operator owned cables
        - Cooling systems - control systems operating temperature of IT systems
    - Energy/power
        - Main Substation – i.e., infrastructure for transformation of the electric voltage
        - Power distribution – i.e., infrastructure for distribution of the electrical power
        - Backup power – i.e., power source in case of external power failures
            - UPS - Short period fast response auxiliary power
            - Electrical generators - Long period auxiliary power
- ***Human agents*** – i.e., human agents involved in the operation of SDNs or using the services enabled through SDNs
    - SDN Administrators – i.e., human agents responsible with the maintenance and monitoring of the SDN network
    - SDN Application Developers – i.e., human agents who build applications and enabling software operating at the SDN application layer
    - Network Service Operators – i.e., human agents responsible for the generic services provided via SDN network (e.g., ISP services)
    - End User Application Developers – i.e., human agents who build end user applications communicating through SDNs and any enabling software for these applications
    - End User Application Administrators – i.e., human agents acting as system administrators for end user applications
    - End User Service Providers – i.e., human agents responsible for the provision of services realized through end user applications
    - End Users – i.e., end users of services provided by end user applications enabled by SDNs

Annex B: Detailed Mind Map for SDN/5G Assets

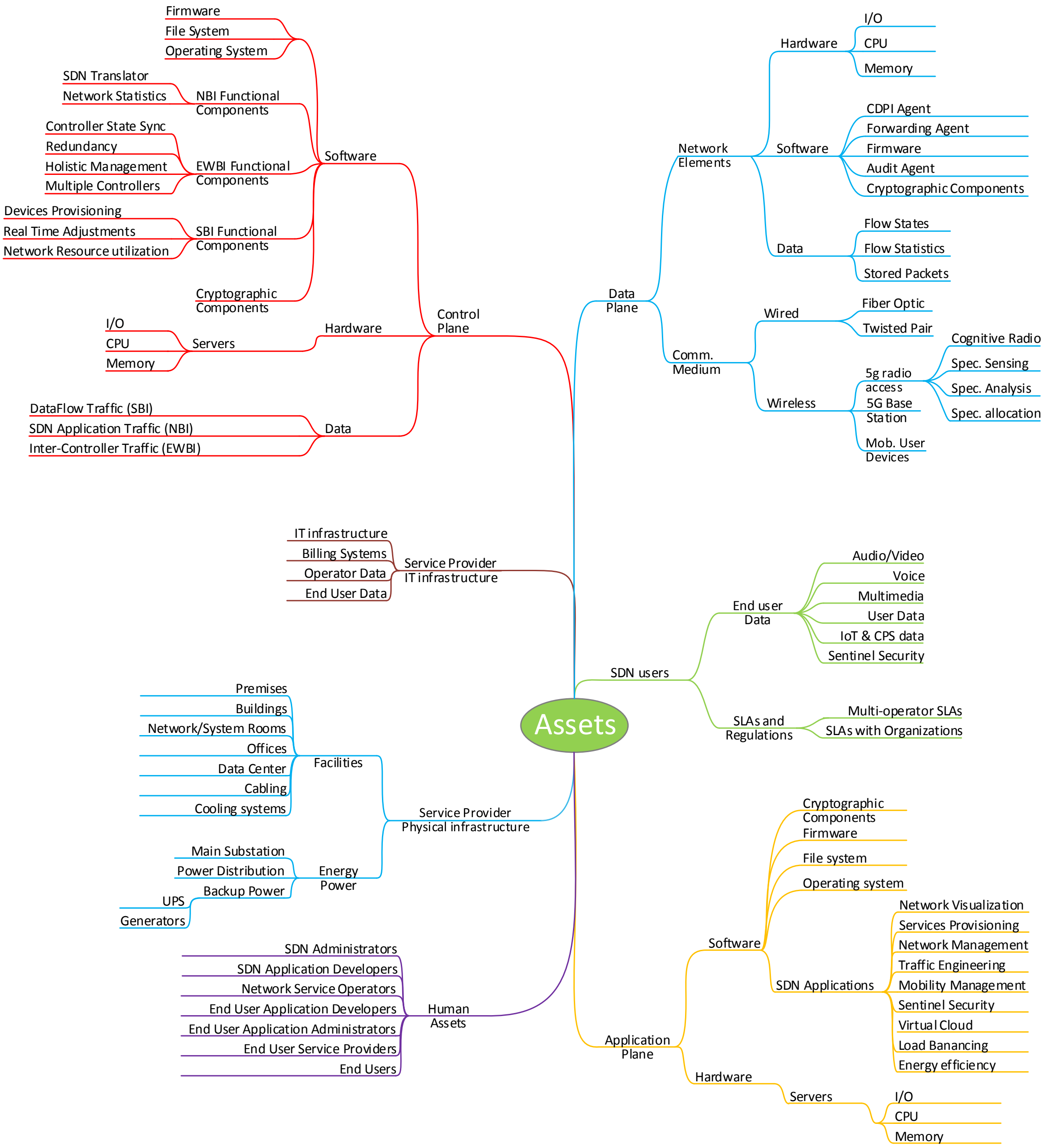

Figure 7 - Detailed mind map for SDN/5G Assets

Annex C: Detailed Mind Map for SDN/5G Threats

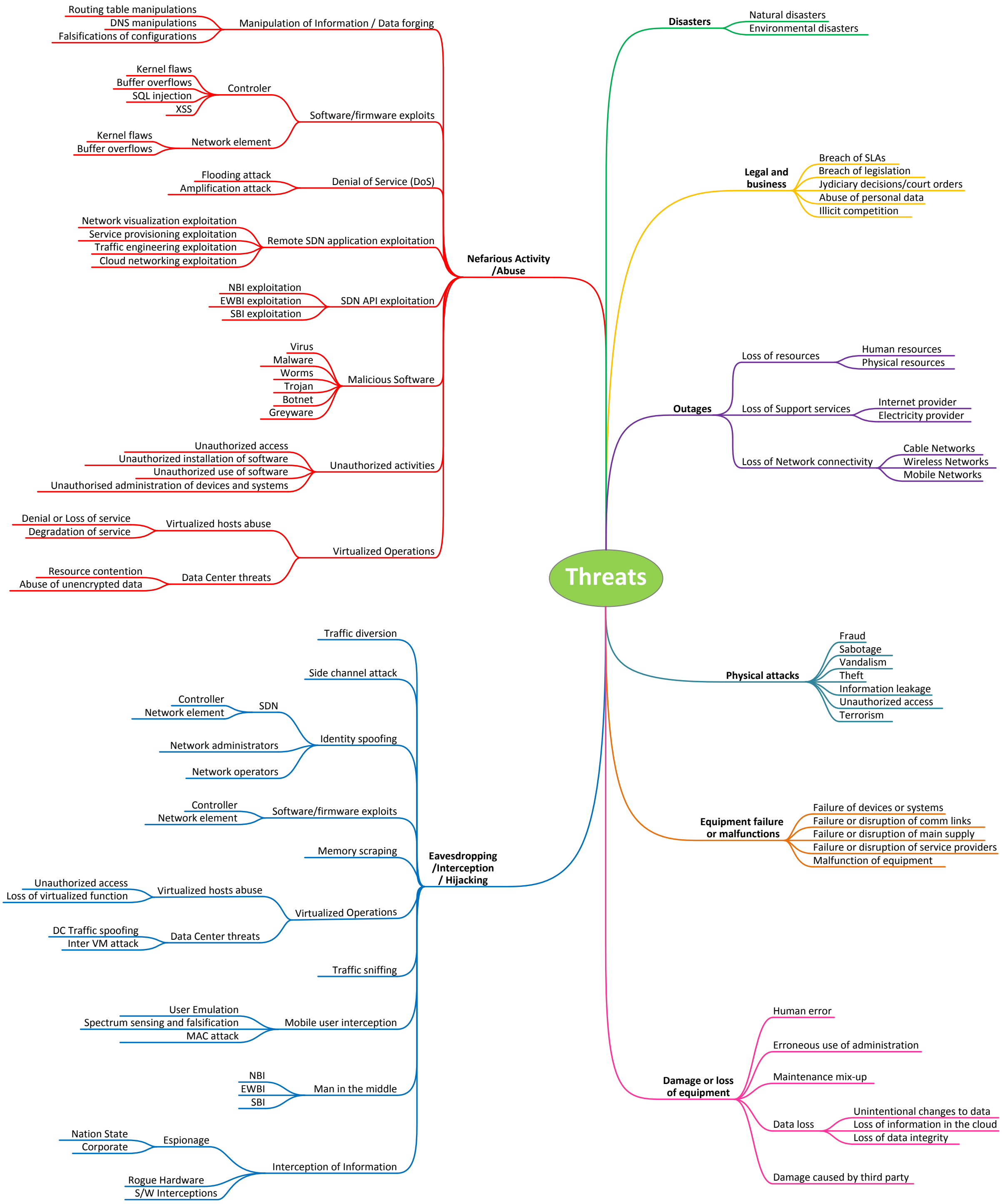

Figure 8 - Detailed mind map for SDN/5G Threats

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-04-15-942-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-161-8
DOI: 10.2824/67261