Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings

0 Disclaimer

This risk assessment was written having in mind the 5G network as a natural successor of current mobile network infrastructure. Due to the uncertainties regarding the market viability of currently envisioned 5G use cases such as e. g. remote medical and industrial applications; this is currently the only reliable basis for conducting the assessment. Risks that arise due to future applications have therefore not been considered in this document.
The scope of this risk assessment as well as the underpinning set of criteria should be regularly updated as new use cases are developed and deployed.

1 Introduction

The Commission Recommendation (EU) 2019/534 of 26 March 2019 on the Cybersecurity of 5G networks (hereafter 'the Recommendation') sets out a number of concrete actions. In particular, it requests each Member State to carry out a **national risk assessment** of the 5G network infrastructure by 30 June 2019 and to transmit the results to the Commission and to ENISA **by 15 July 2019.**

On the basis of the national risk assessment and taking into account ongoing coordinated action at EU level, the Recommendation provides that **each Member State should review and update applicable security measures**, including 'reinforced obligations on suppliers and operators to ensure the security of sensitive parts of the networks', as well as other obligations, where appropriate.

In parallel, the national risk assessments should form the basis for a **coordinated Union risk assessment**, to be produced **by 1 October 2019**. The coordinated Union risk assessment should be made up of a threat landscape mapping to be conducted by ENISA and a joint review of the Union-wide exposure to risks to be conducted by Member States, with the support from the Commission and together with ENISA.

At the first meeting of the dedicated NIS Cooperation group on 11 April, Member States authorities discussed national risk assessments processes and identified a number of possible elements for a common approach. After the meeting, a first outline was shared with Member States for comments in order to prepare these draft guidelines and structured template, on which Member States were also asked to provide comments.

2 Aim and Scope

This document sets out a set of guidelines on **common elements for national risk assessments** and a **structured template for reporting on the main findings**.

Its purpose is two-fold: (i) promoting consistent approaches in national risk assessments and (ii) facilitating the exchange of relevant and comparable information among Member States to inform their national processes and facilitating the preparation of the EU coordinated risk assessment.

This document builds on the definitions and provisions of the Recommendation and also reflects the discussion and information shared by Member States on their national approaches at the dedicated meeting of the NIS Cooperation Group that took place on 11 April, as well as further input provided by ENISA and by several Member States after this meeting.

Data exchange process

By 15 July, Member States are invited to send:

1. Responses to the questions included in this structured template, to be shared with other Member States and with the Commission and ENISA.
2. The full results of the national risk assessment (excluding classified information) to the Commission and ENISA.

Member State should submit their reports and responses to a dedicated CIRCA address.

3 Common elements for 5G cybersecurity risk assessments and structured template for reporting on findings

As set out in the Recommendation, Member States should carry out a risk assessment of the 5G network infrastructure by 30 June 2019 and transmit the results to the Commission and ENISA by 15 July 2019.

These guidelines do not address risk assessment methodologies in detail. Authorities could use several standard methodologies for performing their national risk assessments of 5G networks (eg. ISO/IEC: 27005).

These guidelines and structured template aim to facilitate a consistent approach and a common understanding of the risks, including for preparing the EU coordinated risk assessment. To this end and while applying the risk assessment methodologies of their choice, Member States are invited to consider the elements listed below in their national risk assessments of 5G cybersecurity and to provide a summary of the findings using the structured template set out therein.

Responses to the questions included in the template should be based on the results of the national 5G cybersecurity risk assessments.

The responses provided should reflect the assessment of the risks at national level from the perspective of the governments (ie. legislators/regulators), supported by other stakeholders' views (including network operators or suppliers) where necessary.

The guidelines and template set out below reflect an approach based on the identification of assets, threats, and vulnerabilities to help identify potential ways, in which threat actors could exploit a certain vulnerability of an asset to impact on the government's objectives. On this basis, end-to-end risk scenarios linking these different elements will be key to identify the main risks to the cybersecurity of 5G networks.

3.1 Definition.

The Recommendation provides that 5G networks means 'a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy network elements based on previous generations of mobile and wireless communications technology such as 4G or 3G. 5G networks should be understood to include all relevant parts of the network'.

3.2 Cybersecurity threats

National risk assessments should identify the top level threats and their relevance in the case of 5G networks. They should include the following high-level categories of cybersecurity threats and threat actors as well as an assessment of the relevance of the threat based on the capabilities and intent of the threat actors:

3.2.1. Main threat actors

- *non adversary/accidental threat actor, such as an unintended impact or a side effect from an operation not targeting the operation of a mobile communication network*
- *an individual hacker*
- *a hacktivist group*
- *an organized crime group*
- *an insider*
- *a nation state or nation state-backed actor*

3.2.2. Main threats

- *Compromised confidentiality (incl. espionage)*
- *Compromised availability*
- *Compromised integrity of a service*

SUMMARY OF FINDINGS ON MAIN THREATS

Question 1: Please fill the table below, associating the main threats and threat actors, and provide a rating of 1 to 5 according to their relevance (assessed by taking into account capabilities and intent) of the various combinations.

Relevance rating: 1= Very high; 2= High; 3= Medium; 4= Low; 5= Very low

Threat actors Threats	Non adversary / accidental	Individual hacker	hacktivist group	organized crime group	Insider within a telecom operator or subcontractor	Nation state or nation state-backed actor	
Compromised confidentiality	4	3	3	2	2	2	1
Compromised availability	3	3	3	3	3	3	2
Compromised integrity	4	3	3	3	3	3	2

Comments/additional information:

- Assessment very rough due to missing concrete targets of attacks and therefore evaluation of intents of threat actors only based on general experiences from the past and gut feeling
- Internal employees or subcontractors certainly have a wide range of options but little intention.
- Nation state or nation state-backed actors have very diverse possibilities due to the large resources, but usually do not want to attract attention.
- The core and access domains are typically used to describe the asset areas of most concern (and therefore the focus of risk assessment). Resulting in an assessment of Core risk grading.

Question 2: Please describe the main threat scenarios related to 5G, which were considered in your national risk assessment?

Main threat scenarios	Description
High level view	
Outage of telecommunications services	Large-scale outage or significant disturbance of telecommunications services (e.g. voice services, data services, M2M/IoT services, business services) based on 5G related network infrastructure incl. legacy platforms (e.g. IP transport)
Misuse of data	Unauthorized access to confidential data and usage for purposes other than intended respectively unauthorized manipulation or modification of data; e.g. data theft, espionage
Midlevel view	
Increased attack surface	Due to an increased attack surface of 5G networks, it is more likely that attacks will be performed on interfaces to third parties connected to the 5G network. Even more, the number of third parties connected to the network will increase by 5G, and the network operator is challenged to secure those interfaces.
Critical business services in focus of hacker groups	New services on 5G like automotive applications, medial applications etc. will encourage hacker groups to attack the related networks to earn publicity.
Critical infrastructure services centralized on 5G in focus of nation state attacks	If more and more critical services like electronic payment, logistic processes, transportation etc. are built on top of 5G networks, attacks towards 5G networks might have a nation-wide high impact on the essential services in parallel, thus attackers could bring the daily life to a halt (no payment, no transportation, no shopping, etc.).

Technical view	
Software/firmware exploits	One of the listed component will be exploited by a controller system (hacked / or not hacked): Kernel flaws Buffer overflows SQL injection XSS Exploited on a network element: Kernel flaws Buffer overflows
Denial of Service (DoS)	Flooding attack Amplification attack
Access Control	Password disclosure Session policy violation Unauthorized access
Unauthorised activities	Unauthorised access Unauthorised installation of software Unauthorised use of software Unauthorised administration of devices and systems
Remote SDN (Software Defined Network) application exploitation	Network visualization exploitation Network management Mobility management Service provisioning exploitation Traffic engineering exploitation Virtual Cloud networking exploitation
General 5G Radio Access Threats	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 (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 enforce to become lower compared to what path loss models have predicted due to transmission features such as signal fading, multi-path propagation, etc., 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
General risks and threats of a non-technical nature	These threats would contemplate aspects such as the specific characteristics of the suppliers (company structure, governance model ...), the aspects related to the supply chain (Degree of dependence on suppliers, Monovendor / multivendor environments, source of suppliers, legal restrictions imposed by third countries ... etc) • **Dependency/lock-in** • **Vendor-specific** (e.g. company structure and management) • **Third country- related** (legal requirements on vendors, offensive cyber policies, malicious activities of specific third country or entities, model of governance, etc.) • Related to the supply chain (place of manufacturing) • **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 occur53. 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.

3.3 Assets: what do we want to protect?

As set out in the Recommendation, national risk assessment of 5G should include ‘identifying the most sensitive elements where security breaches would have a significant negative impact. For this purpose, national risk assessments should consider the following categories of assets and provide an assessment of their level of sensitivity:

- *Network components and/or functions*
- *Specific areas, based in particular on the number of potentially affected users*
- *User groups (examples: key governmental entities, law enforcement or military assets, critical infrastructure operators/ operators of essential services, etc.)*

To identify areas or user groups, where security breaches would have a significant impact, the following categories of potential impacts could be considered:

- *National fundamental interests, sovereignty and democracy*
- *Public and interior security, including emergency services and preparedness*
- *Population and environment*
- *Economy/GDP*
- *Personal data protection*
- *Intellectual property protection*

SUMMARY OF FINDINGS ON MAIN ASSETS

Question 3: Based on your national 5G risk assessment, have you identified specific sensitive network components or functions?

Yes

If possible, please indicate which ones:

It will be necessary that MS develop criteria for the identification of sensitive network components and functions.
The network components and functions listed below are presumably included in any list of sensitive network components and functions based on such criteria.

1. Regarding availability of telecommunication services:
    a. Generally: Network platforms / functions where lots of telecommunications services depend on (e. g. transport, DNS), incl. related network management systems

    b. With regard to M2M/IoT services: radio access and mobile core networks (incl. related network management systems)

2. Regarding confidentiality & integrity of data: network nodes highly aggregating user and control data for transmission, storage and processing (e. g. core network databases, core service platforms (incl. related network management systems))

See Question 4 for more details containing network elements and functions.

Comments/additional information:

At 5G we are concentrating for the time being on the same network functions as in the past. Therefore, central network systems such as HLR, Core Router (data and signalling) are the most critical as their failures could affect the complete services. Protecting these systems is therefore essential.

In addition, interconnection points to other networks and third parties need appropriate protection (firewalls, IPS and IDS for instance). We expect that attacks, especially by hacker groups and nation states, will challenge us with great diversity and complexity.

Question 4: If possible, please indicate the relative degree of sensitivity of the various categories of networks elements and functions included in the table below. For each category, if available please provide a more detailed categorisation of specific elements or functions.

	Low	Moderate	High	Critical
Access network functions		base stations, supporting IP systems	aggregating network elements supporting larger regions	
Core network functions			service platforms, and edge routing functions	central databases, central routers
Transport & transmission functions		access network	core network	
Internetwork exchanges			confidentiality and integrity of network data (e. g. Roaming)	
Management systems & Supporting Service				Element & Network Management Systems
Other categories? **……………………………**			Value Added Services (VAS) (e.g. LBS, VMS)	Lawful Interception

Comments/additional information:

MS should develop a harmonized catalogue for criteria used in identification and classification of sensible network components and functions.

Question 5: Have you identified areas where the number of potentially affected users would have a significant negative impact?

Yes

If so, please indicate which thresholds were used to select these areas:

This question cannot be answered in a generic manner without regard to specific use cases.
MS should identify a set of relevant use cases.
According to German telecommunication regulation we have the following thresholds.

- 100,000 subscriber, see Post- und Telekommunikationssicherstellungsgesetz (PTSG), or
- 1,000,000 user hours, Telekommmunikationsgesetz (§ 109 Abs. 5 TKG) based on ENISA Technical Guideline on Incident Reporting

Comments/additional information:

Question 6: Have you identified specific sensitive user groups?

Yes

If so, please indicate which criteria were used to select these user groups?

Possible criteria for identification of user groups:

1. Legal requirements (esp. Secrecy of Telecommunications, General Data Protections Regulation, Post- und Telekommunikationssicherstellungsgesetz (PTSG), Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV))
2. Business relevance (e. g. based on contractual requirements with customers, suppliers & other business partners)

Comments/additional information:

The identification of user groups and their sensitivity will be done when new services are developed/implemented or third parties are connected to a subscriber network. In this case, a risk analysis of the services followed by the implementation of suited security measures shall be performed.

3.4 Vulnerabilities

According to the Recommendation, vulnerabilities in 5G networks can originate from various factors, including technical factors and other factors.

While national risk assessments should review any relevant vulnerabilities, they should include the following set of key vulnerabilities.

3.4.1 Vulnerabilities related to technical factors

- *Software-related vulnerabilities*
- *Hardware-related vulnerabilities*
- *Process- related vulnerabilities (including access controls and network architecture) , configuration related vulnerabilities)*

3.4.2 Vulnerabilities related to other factors

- *Policy related or organisational vulnerabilities (including people, and outsourcing)*
- *Supplier-related vulnerabilities, including when arising from the legal and policy framework to which 5G equipment suppliers may be subject in third countries*[1]
- *Dependency from one/a limited number of suppliers*
- *Other supply chain vulnerabilities*

[1] As far as risks related to other factors are concerned, the Recommendation states that they 'may include regulatory or other requirements imposed on information and communications technologies equipment suppliers. An assessment of the significance of such factors would need to take into account, inter alia, the overall risk of influence by a third country, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection between the Union and the third country concerned, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection. '

SUMMARY OF FINDINGS ON MAIN VULNERABILITIES

Question 7: Please indicate the most relevant and critical vulnerabilities in each category and indicate whether they are specific to 5G as a whole network, or increase with 5G.

a) Vulnerabilities related to technical factors

Types	Main vulnerabilities	Specific to 5G? or increase with 5G (Specific/Increase)	Specific to certain network elements? If so, please indicate which ones?
Software-related vulnerabilities	Exploits in SW	no	Third party SW including increasingly Open source SW included in vendor's software packages
	Software not up-to-date (vendor related)	no	Especially for Open-Source-SW included in vendor's software packages, but of course valid for all SW.
	Software complexity (for example with increased use of the virtualization layer)	Increase	Access, Core
	Undocumented functions	no	
	Deficient software quality	Increase	IoT devices (due to cost pressure or time-to-market pressure)
	Weakness of physical sites	increase, due to larger number of sites	Local radio stations
	Weakness of processors, chips and hw-design, which can be used for an attack.	no	
	Deficient physical protection	Increase	Active NEs at edge
Hardware-related vulnerabilities	Undocumented functions	no	
	eUICC and crypto accelerator hardware	no	
	Attacks against Management systems	no	Management systems
	Attacks against office	no	no

	computers and infrastructure leading to outage of engineering and configuration tasks (e.g. trojans, phishing etc.)		
	Misconfiguration and Mismanagement, especially End to end network slicing misconfiguration	yes (for private networks of corporates)	RAN and core network
	Access to networks and functions	Yes for private networks of corporates	RAN and core network Threats on SEPP (Security Proxy) like: Signalling attacks from internetwork Packet Exchange (Ipx / Roaming) Lack of confidentiality and integrity through IPX intermediaries.
Process- related vulnerabilities	Deficient physical access control	Increase	Active NEs at edge
	Functional dependences on society level (e.g. industry 4.0 or smart power infrastructure interdepend on 5G) A focus auf use-cases is necessary	Increase	Transport
	Automation of configuration (automatic dynamical and AI-based configuration)	Increase	
	Interconnection points to third party	yes	

b) Vulnerabilities related to other factors (non-technical)

Types	Main vulnerabilities	Specific to 5G? or increase with 5G (Specific/Increase)	Specific to certain network elements? If so, please indicate which ones?
Policy and other organisational vulnerabilities	Integrity of operations people of private networks interworking with public networks	no	Access and core networks.
	Social engineering or phishing, to get access to confidential data and access to sites, networks and systems. Attacks against integrity of data and communication processes.	no	
	Privileged admin rights	no	
	Remote access of supplier	no	
	Insufficient security awareness	no	
Supplier-related vulnerabilities	Insufficient security awareness and capabilities of (new) suppliers	no	
	Distribution of supplier's support staff across the world, with frequently changing responsibilities, might lead to transfer of confidential data and knowledge. Could be a good point of access for nation state attackers	no	
	Legal requirements on data access	no	
	Legal restrictions on use of technology	no	
	Dependence on supplier expertise	Increase	Mgmt. systems (automation)
Dependency on one/a limited number of suppliers	A homogenous one-vendor network could make it easier to attack a network or services, especially in case a vendor acts as an attacker. Depends on network structure and redundancy concept.	no	

	Relying on an one-vendor concept can limit the selection of best security implementations, when that vendor does not provide suited security functions	no	
	Stop of supply	no	
Other supply chain vulnerabilities	Vendors more and more use open source software in combination with their own software. If the release and patch management of their own SW vs. the third party (for example open source) software do no match, there is a risk that the software versions are not upgraded in time when the open source community releases an update. This could lead to security weaknesses in the older SW.	no	
	Stop of professional services	no	

Comments/additional information:

3.5 End-to-end risk scenarios

In order to link the different parameters described in this document and based on the replies provided in the sections above (threat/threat actors, assets and vulnerabilities), Member States are invited to identify main risk scenarios involving specific threat actors targeting specific sensitive assets and using a specific vulnerability.

Question 8: Please describe the main risks as end-to end scenarios, describing ways how threats could exploit a certain vulnerability of a specific asset, which were considered in your national risk assessment?

Risk scenarios	Description
1.	Attacks against telecommunications services by exploiting software vulnerabilities of e. g. IoT devices and high bandwidth capabilities of 5G networks
2.	Espionage of data initiated by nation states or nation state-backed actors based on legal requirements on suppliers or exploitation of undocumented functions
3.	Large-scale outage or significant disturbance of telecommunications services by nation states or nation state-backed actors exploiting undocumented functions or attacking interdependent critical infrastructures (esp. power supply)
4.	Attacks e. g. by Trojans, which impacts the office infrastructure. The risk is that data will be encrypted, deleted or changed. This could lead to a complete switch-off of the office infrastructure for several days/weeks. In that time no network configuration can be done, no troubleshooting, monitoring, etc. No new customers can be acquired and supported. In worst case, business and services will be brought done for days.
5.	Attacks against the network impacting customer services, with potential impact to the nationwide public services. Those attacks could be performed by DDoS attacks but also by more hidden lateral attacks in case of nation state attacks. In the latter case, the time of an attack (preparation) and the time of the visible service degradation (execution) could differ.
6.	Hidden attacks focusing on the services and the data carried. Here hidden attacks against the service integrity could lead to degraded service quality or product quality of business customers.

3.5 Risk mitigating measures

National risk assessment should include an assessment of risk mitigating measures, which are in place or planned and could serve to mitigate the identified risks scenarios, and an assessment of their effectiveness.

This should include the identification of actors, who will need to implement and/or enforce the risk mitigating measures:

- *The network supplier*
- *The outsourced partner that handles field operations or the company operating the network equipment assembly*
- *The delivery chain operator*
- *The telecom operators*
- *The end user (private individual or wholesale user of the 5G services, eg. energy company, hospital, a port or an airport, autonomous driving roadside infrastructure operator)*
- *Targeted Critical Infrastructure operators and Operators of Essential Services.*
- *Key governmental entities/public authorities*

SUMMARY OF FINDINGS ON EXISTING OR PLANNED MEASURES

Question 9: For each of the main risk scenarios identified in the table in question 8, please indicate if mitigating measures are already in place or planned, and if so, which ones, and whether they effectively reduce the likelihood of a vulnerability being exploited.

Risk scenarios	**Existing or planned mitigating measures (Yes/no)**	**Description**	**Relevant actor (eg. telecom operator, supplier, etc.)**	**Effectiveness (Low/Medium/High)**
1a.	Yes	DDoS protection functionality in operator networks	Telecom operator	Medium
2a. **3a.**	Yes	Certification of suppliers' product security incl. escrow of software source code	Regulator, supplier	Medium
2b.	Yes	Use of end-to-end encryption	User	High
2c. **3b.**	Yes	Security assessment of each new supply and contract	Operator and supplier	high
4a.	Yes	Regular audits for critical services and systems	Operator	high
5a.	Yes	Using SIEM to identify attacks for outside and inside of the network	Operator	high
6a.	Yes	Risk management for all new services	Operator	high
all	Yes	Data protection needs analysis, followed by the Technical and Organisational Measures (TOMs) for all critical systems	Operator	high
all	Yes	Security monitoring and scanning	Operator	high

Comments/additional information:

Annex

Example of a more detailed threat categorisation applicable to Software Defined Networking (source: ENISA SDN 5G threat landscape report) - for possible reference in the context of the national risk assessments.

- ***Nefarious activity/abuse***: 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”
- ***Eavesdropping/Interception/ Hijacking:*** This threat category is defined as “actions aiming to listen, interrupt, or seize control of a third party communication without consent”
- ***Physical attacks:*** 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”
- ***Damage:*** 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”
- ***Unintentional Damage:*** 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 ”
- ***Failures or malfunctions:*** This threat category is defined as “insufficient functioning of an (Internet infrastructure) asset”.
- ***Outages:*** This threat category is defined as “unexpected disruptions of service or decrease in quality falling below a required level “
- ***Disaster:*** This threat category is defined as “serious disruption of the functioning of a society”
- ***Legal:*** 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”