

# **RESISTO:**

## **D5.1\_Cyber-physical countermeasure Identification**



# RESISTO

## D5.1 – CYBER-PHYSICAL COUNTERMEASURE IDENTIFICATION

<b>Document Manager:</b>	Giuseppe Celozzi	TEI	Editor
--------------------------	------------------	-----	--------

<b>Project Title:</b>	RESilience enhancement and risk control platform for communication infraSTructure Operators
<b>Project Acronym:</b>	RESISTO
<b>Contract Number:</b>	786409
<b>Project Coordinator:</b>	LEONARDO
<b>WP Leader:</b>	RM3

<b>Document ID N°:</b>	RESISTO_D5.1_190524_01	<b>Version:</b>	1.0
<b>Deliverable:</b>	D5.1	<b>Date:</b>	24/05/2019
		<b>Status:</b>	APPROVED

<b>Document classification</b>	<b>PUBlic</b>
--------------------------------	---------------

Approval Status	
<b>Prepared by:</b>	Giuseppe Celozzi, Cosimo Zotti (TEI)
<b>Approved by: (WP Leader)</b>	Marco Carli (RM3)
<b>Approved by: (Coordinator)</b>	Bruno SACCOMANNO (LDO)
<b>Advisory Board Validation (Advisory Board Coordinator)</b>	NA
<b>Security Approval (Security Advisory Board Leader)</b>	Alberto BIANCHI (LDO)

## CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Giuseppe Celozzi, Cosimo Zotti, Gaetano Barba, Elena Donnarumma, Gianluca Ferrentino	TEI	Contributor
Alberto Neri	LDO	Contributor
Federico Colangelo, Marco Carli	RM3	Scientific Researchers
Javier Valera, Moisés Valeo, José Manuel Sánchez	INT	Contributor
Michael Skitsas, Nicolas Georgiades, Nikolaos Koutras	ADI	Contributor
Andrei Avădănei	BSS	Contributor
Paula Cravo, Jorge Carapinha	ALB	Contributor
Guilherme Alves,	SEP	TEI Linked 3PP

## DISTRIBUTION LIST

Name	Company / Organization	Role / Title
PMT	RESISTO CONSORTIUM	NA
Markus MULLER	EC DG REA	EC Programme Officer
General Public	NA	NA

## REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.1	23.10.2018	1-16	All	Draft ToC
0.8	10.04.2019	1-43	All	1 <sup>st</sup> Draft for internal review
0.9	24.04.2019	All	All	Release for SAB review
1.0	24.05.2019	All	All	Final Release

## COPYRIGHT STATEMENT



© 2018-2021 This document and its content are the property of the RESISTO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the RESISTO Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the RESISTO Partners. Each RESISTO Partner may use this document in conformity with the RESISTO Consortium Grant Agreement provisions.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, under the Grant Agreement No 786409.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

## PROJECT CONTACT



LEONARDO  
Via Puccini – Genova (GE) – 16154 – Italy  
Tel.: +39 348 6505565  
E-Mail: [bruno.saccomanno@leonardocompany.com](mailto:bruno.saccomanno@leonardocompany.com)

## RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also extreme weather events and natural disasters represents a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. Through RESISTO Communications Operators, will be able to implement a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation.

## EXECUTIVE SUMMARY

An analysis of the cyber-physical threats and related countermeasures is required in order to define the workflows that RESISTO platform has to provide to operators as a guide to react to security attacks.

This document provides such list of threats/countermeasures which serves as starting point for further refinements based on the Use Cases that are defined in the three macro-scenarios addressed in the project. The output serves as reference document for the work which is carried in the subsequent work-packages.

The relevant standard to be taken into account are identified, the classification of the countermeasures is performed and the basic Attack Defense Trees (ADT) are defined.

Both countermeasures related to potential threats that have to be put in place in order to prevent attacks (to be addressed in the Long-Term Control Loop) and those related to run-time activities needed to Detect, React and Mitigate the effects of cyber/physical attack events (to be addressed in the Short-Term Control Loop) are considered.

In addition to the graphical trees, an innovative “dynamic hierarchical interactive” visualization method, based on JSON files, is proposed to be used for the ADT management: it is useful to address scalability issues related to big and complex multi-dimensional trees and for the integration of real-time information related to ongoing attacks with the ADT static model.

## CONTENTS

<b>ABBREVIATIONS .....</b>	<b>10</b>
<b>1. INTRODUCTION .....</b>	<b>12</b>
<b>2. METHODOLOGY .....</b>	<b>13</b>
2.1. CONCEPTS AND TERMS .....	13
2.2. METHODOLOGY FOR SELECTING COUNTERMEASURES .....	14
2.3. STANDARDS .....	14
2.4. CSA TO RESISTO COUNTERMEASURE MAPPING .....	15
<b>3. REVIEW OF AVAILABLE COUNTERMEASURE PERTAINING DEFINED THREATS CLUSTERS.....</b>	<b>21</b>
3.1. IDENTITY MANAGEMENT AND ACCESS.....	21
3.2. DISRUPTION OF DATA OR HW LOSS.....	23
3.3. AVAILABILITY .....	24
3.4. NATURAL DISASTER .....	25
3.5. PHYSICAL SECURITY – PHYSICAL INTRUSION.....	25
3.6. COMBINING COUNTERMEASURES .....	26
<b>4. BASIC ATTACK TREES .....</b>	<b>27</b>
4.1. UNAUTHORIZED ACCESS TO DELIBERATELY COMPROMISE A SITE .....	27
4.2. NATURAL DISASTER COMPROMISING A SITE .....	32
4.3. DISRUPTION OF TELECOM OPERATOR CELL SERVICE .....	37
4.4. ALTERNATIVE VISUALIZATIONS FOR ATTACK TREES .....	44
<b>5. USE CASES .....</b>	<b>46</b>
<b>6. CONCLUSION.....</b>	<b>50</b>
<b>7. REFERENCES .....</b>	<b>51</b>



## List of Figures

Figure 1: ADT Unauthorized Access .....	31
Figure 2: ADT for service disruption caused by storms .....	34
Figure 3: ADT summarizing service disruption caused by natural disaster cases .....	37
Figure 4: ADT for disruption of cell service .....	43
Figure 5: Interactive ADT visualization .....	45

## List of Tables

Table 1: Long term control loop to CSA mapping .....	18
Table 2: Short term control loop to CSA mapping .....	20
Table 3: Password Protection .....	22
Table 4: Badge, smart cards protection .....	22
Table 5: Phishing attacks .....	22
Table 6: Session Hijacking .....	23
Table 7: Disruption of data or HW loss .....	24
Table 8: (D)Dos .....	24
Table 9: Service Continuity .....	25
Table 10: Physical Intrusion .....	26
Table 11: Unauthorized access to deliberately compromise a site .....	30
Table 12: Physical Threat to a site because of weather, flood or earthquake .....	33
Table 13: Congestion of the CN due to overload because of natural disaster .....	35
Table 14: Congestion of the core network because of Natural disaster .....	37
Table 15: Disruption of Telecom Operator Cell Service .....	42
Table 16: Summary table of Events .....	48
Table 17: Summary table of use cases and trees applicability .....	49

## ABBREVIATIONS

<b>2G, 3G, 4G</b>	Second, third and fourth generation of mobile phone systems
<b>3GPP</b>	3rd Generation Partnership Project
<b>5G</b>	5th generation mobile wireless standards
<b>ADT</b>	Attack Defense Tree
<b>API</b>	Application Programming Interface
<b>CN</b>	Core Network
<b>CSA</b>	Cloud Security Alliance
<b>DDoS</b>	Distributed Denial of Service
<b>DNS</b>	Domain Name Service
<b>ETSI</b>	European Telecommunications Standard Institute
<b>EM</b>	Element Manager
<b>EU</b>	European Union
<b>FM</b>	Fault Management
<b>GSM</b>	Global System for Mobile communications
<b>HW</b>	Hardware
<b>IETF</b>	Internet Engineering Task Force
<b>IoT</b>	Internet of Things
<b>IPS</b>	Intrusion Prevention Systems
<b>LTCL</b>	Long Term Control Loop
<b>LTE</b>	Long Term Evolution (= 4G)
<b>M</b>	Mandatory
<b>MNO</b>	Mobile Network Operator
<b>MO</b>	MO Managed Object
<b>eNB</b>	E-UTRAN Node BP
<b>NE</b>	NE Network Element
<b>NIST</b>	National Institute of Standards and Technology
<b>NM</b>	Network Manager
<b>NOC</b>	Network Operation Center

<b>PC</b>	Personal Computer
<b>O</b>	Optional
<b>OSINT</b>	Open Source Intelligent
<b>OS</b>	Operations System
<b>RAN</b>	Radio Access Network
<b>SDN</b>	Software Defined Network
<b>SIM</b>	Subscriber Identity Module
<b>STCL</b>	Short Term Control Loop
<b>SW</b>	Software
<b>TEE</b>	Trusted execution environment
<b>UE</b>	User Equipment
<b>UPS</b>	Uninterruptible power supply
<b>VPN</b>	Virtual Private Network
<b>VNF</b>	Virtual Network Function
<b>WP</b>	Work Package

## 1. INTRODUCTION

The deliverable D5.1 is the report of the WP5-related activities performed in T5.1: “*Cyber-physical countermeasure identification*”. The task addresses important issues related to the countermeasures to be considered in the RESISTO use-cases definition and will serve as a “reference document” for several upcoming WPs. The work involves the identification and classification of the countermeasures relevant for the three macro-scenarios addressed in the project and how they can be formalized using the combination of basic ADT.

The deliverable comprises 6 sections:

- *Section 1* offers a brief introductory overview;
- *Section 2* presents the methodology used to identify the countermeasures to be taken into account discussing the relevant security standards;
- *Section 3* presents the list of countermeasures of relevance to RESISTO;
- *Section 4* provides a draft description of the basic ADT that can be combined and used to model the security countermeasures in RESISTO;
- *Section 5* describes the applicability of the findings of Section 4 to RESISTO use cases.
- *Section 6* summarizes the conclusion of the analysis of the countermeasures and their usability in the RESISTO platform.

## 2. METHODOLOGY

This section presents the methodology adopted by RESISTO, in order to perform a multi-directional analysis of the available countermeasures and how they apply to the proposed use-cases, as these have been selected with the purpose of purely serving the well-defined RESISTO aims. Such kind of analysis will be “multi-directional”, because it will enable deliverable D5.1 to serve as a reference document for the work which will be carried in the subsequent work-packages.

In the document are described the possible countermeasures to face attacks that RESISTO platform will be able to put in place. The potential attacks and events here identified will be increased with the ones coming from the use cases as soon as their complete definition is available (D2.8). On the basis of the defined countermeasures, a set of different workflows will be defined (T5.4). The workflows will drive the operator to react to each attack combining automatic actions on communication networks or on physical devices (i.e. barriers activation, alarm physical indicators) (T5.2) and/or security or technical team interventions by means of an Emergency Warning Communication Function (T5.5). The complete RESISTO solution will then be integrated in WP6 and demonstrated on the use cases during the WP7, WP8 and WP9.

In this sense, the methodology will allow us to define the technological benefits that will result from RESISTO outcomes as well as the definition of the criteria for the evaluation of the fulfilment of such outcomes.

### 2.1. Concepts and Terms

In this sub-section we provide definitions for the RESISTO methodology concepts and terms; moreover, the interrelations between such concepts are also given. The presented methodology is based on a “set of concepts and terms” which will be used in the preliminary part of the countermeasures’ analysis, in order to define the key aspects which are related to the project’s specific objectives. The following terms are considered:

- **“Countermeasure”**: are actions, control and best practices performed with the scope of reducing the risk associated with a specific use case or scenario.
- **“Action”**: a defense task carried out to counteract an attack, *for example*: Coverage increase and increase in functionality offered to the user.
- **“Attack Defense Tree”**: an attack defense tree is a graph that describes an attack including nodes as attack events and action and countermeasures as defense nodes.
- **“Event”**: is an occurrence of an attack towards a Critical Infrastructure.
- **“Scenario”**: Scenarios describe application examples, highlighting key benefits of the RESISTO context, by attributing those to the dedicated scenario.
- **“Use case (UC)”**: A particular “instantiation” of a specific scenario, having the goal to elaborate upon a parameter of the corresponding scenario, under a set of given conditions.

## 2.2. Methodology for selecting Countermeasures

Some countermeasures are relevant to potential threats and they will be put in place in order to prevent attacks. RESISTO Long Term Control Loop (mainly WP3) is in charge to do this job covering threats Identification and Prevention tasks.

Additional countermeasures will be put in place by Short Term Control Loop (mainly addressed in WP4 and WP5) that is in charge, at run-time, to Detect, React and Mitigate effects of cyber/physical attack events. RESISTO Short Term Control Loop will provide support to the operators to evaluate attack events impacts and select appropriate mitigation actions.

## 2.3. Standards

Documents from Cloud Security Alliance and National Institute of Standards and Technology were found to be not only the most complete in literature describing countermeasures, taking into account the other standards that cover specific countermeasures or control that should be put in place to prevent, detect or act on a threat.

As previously stated, countermeasures categorization in RESISTO is based on the short/long term approach, highlighting how the effective handling of security threats is a combination of two strategies: concentrates on risk and resilience management in the long-term and focus on detecting and reacting to ongoing threats in the short term. The documentation for the short-term loop will be based on the definition attack trees, describing possible attack scenarios as a sequence of actions. More details on the attack tree models are given in Section 4. Actions will be taken from literature and in particular we will use NIST [1] and CSA [2] frameworks that represent a wide source of control procedures while also offering a good summary of a number of references to the security documents of a number of standards (e.g. ISO, BSI). We are going to perform a mapping of the actions into RESISTO short and long categories and will use this taxonomy in the development of the attack trees to be applied in each use case.

CSA in [3] organized controls in 3 classes:

- Preventive
- Detective
- Corrective

While [1] identifies 5 actions instead when handling control and correction:

- Identify
- Protect
- Detect
- Respond
- Recover

We classify Preventive controls from [3] and Identify and Protect from [2] as pertaining to the long-term control loop, while the remaining ones are classified as pertaining to the short-term loop since they identify the threats and perform the recovery action.

In addition, we will add another category to both short and long control loop: the **Predictive** category of controls, making use of models and algorithms that leverages machine learning techniques.

CSA terminology will be used and in the rest of the document we will refer to it as to corrective countermeasures adding to it the predictive category in order to maintain a desirable level of security.

Stallings [6] categorizes these essential countermeasures into six classes (referred to by Stallings as “security services”), namely:

- Access control
- Authentication
- Data confidentiality
- Data integrity
- Non-repudiation
- Availability

Access control includes the policies by which entities will access the system and its functions. We will refer to this in the rest of the document as Identity management. Identity management defines the access control rights and different permissions on the system functions and objects.

Identification of the entities that will access the system need proper authentication.

Authentication ensures guarantees that entities accessing, modifying and communicating data are who they pretend to be. This involves guarantying that data in transit, at rest and modified is adequately protected and that no one is able to impersonate another entity.

Data confidentiality means that no one except the intended communicating agents is able to read the data. Data shall be accessed according to the sensitivity of the information being treated or transmitted. Moreover, the system should prevent attackers analyzing traffic flow characteristics and derive information from it.

Data integrity means that the data is received as it is transmitted, without modification from third-party. It must be guaranteed with the purpose of assuring that data stored transmitted through a network are not corrupted, adulterated or destroyed. Messages during an attack can be modified producing duplication, modification, reordering, and replay of messages. Recovery of corrupted data should also be provided if possible. We will refer to this as disruptions of data and HW. We will include in this topic also non-repudiation, which shall guarantee in case of disputes identification of the entities that participated in a malicious activity.

Availability of system resources ensures that rightful requests are fulfilled according to the system characteristics (i.e. performance specifications and KPI). This will include redundancy which usually solves most of the availability problems.

## 2.4. CSA to RESISTO countermeasure mapping

CSA table in [2] contains a reference mapping for a large number of security standards. Even though it refers to the cloud and virtualization security, this can be generalized to almost any software environment and application, in particular new customer services that are already been provided to enterprise like IOT, smart manufacturing, grid services and fintech, but that will be boosted even more along with the rollout of 5G networks that will be addressed in the relevant use cases foreseen in the project, as specified in D2.8. By providing the mapping for long and short control loop to CSA table we can give an indirect indication that covers all software security standard.

In general, in the below table we will group rules according to LTCL and STCL and to the category indicated by CSA. The complete description of the measure can be found in the original document.

Regarding the distinction between STCL and LTCL, in many cases we have countermeasures that must be considered in general and produce guidelines, policies and be managed in terms of risk, so in many cases rules that are more suited for the STCL can also be used in the LTCL but we will replicate them in both lists only when we consider it appropriate.

Long Term Control Loop	
CSA Control Category	CSA ID
Application & Interface Security	AIS-01 Application Security
	AIS-02 Customer Access Requirements
Audit Assurance & Compliance	AAC-01 Audit Planning
	AAC-02 Independent Audits
	AAC-03 Information System Regulatory Mapping
Business Continuity Management & Operational Resilience	BCR-02 Business Continuity Testing
	BCR-04 Documentation
	BCR-07 Equipment Maintenance
	BCR-09 Impact Analysis
	BCR-10 Policy
	BCR-11 Retention Policy
Change Control & Configuration Management	CCC-01 New Development / Acquisition
	CCC-02 Outsourced Development
	CCC-03 Quality Testing
	CCC-05 Production Changes
Data Security & Information Lifecycle Management	DSI-01 Classification
	DSI-02 Data Inventory / Flows
	DSI-05 Non-Production Data
	DSI-06 Ownership / Stewardship
	DSI-07 Secure Disposal
Datacenter Security	DCS-01 Asset Management
	DCS-02 Controlled Access Points
	DCS-04 Off-Site Authorization
	DCS-05 Off-Site Equipment
	DCS-06 Policy
Governance and Risk Management	GRM-01 Baseline Requirements
	GRM-02 Data Focus Risk Assessments
	GRM-03 Management Oversight
	GRM-04 Management Program
	GRM-05 Management Support/Involvement
	GRM-06 Policy



	GRM-07 Policy Enforcement
	GRM-08 Policy Impact on Risk Assessments
	GRM-09 Policy Reviews
	GRM-10 Risk Assessments
	GRM-11 Risk Management Framework
Human Resources	HRS-02 Background Screening
	HRS-03 Employment Agreements
	HRS-04 Employment Termination
	HRS-05 Mobile Device Management
	HRS-06 Non-Disclosure Agreements
	HRS-07 Roles / Responsibilities
	HRS-09 Training / Awareness
	HRS-10 User Responsibility
	HRS-11 Workspace
Identity & Access Management	IAM-01 Audit Tools Access
	IAM-07 Third Party Access
Infrastructure & Virtualization Security	IVS-13 Network Architecture
Interoperability & Portability	IPY-01 APIs
	IPY-02 Data Request
	IPY-03 Policy & Legal
	IPY-04 Standardized Network Protocols
	IPY-05 Virtualization
Mobile Security	MOS-01 Anti-Malware
	MOS-02 Application Stores
	MOS-03 Approved Applications
	MOS-04 Approved Software for BYOD
	MOS-05 Awareness and Training
	MOS-06 Cloud Based Services
	MOS-07 Compatibility
	MOS-08 Device Eligibility
	MOS-09 Device Inventory
	MOS-10 Device Management
	MOS-11 Encryption
	MOS-12 Jailbreaking and Rooting

	MOS-13 Legal
	MOS-14 Lockout Screen
	MOS-15 Operating Systems
	MOS-16 Passwords
	MOS-17 Policy
	MOS-18 Remote Wipe
	MOS-19 Security Patches
	MOS-20 Users
Supply Chain Management, Transparency, and Accountability	STA-01 Data Quality and Integrity
	STA-03 Network / Infrastructure Services
	STA-04 Provider Internal Assessments
	STA-05 Supply Chain Agreements
	STA-06 Supply Chain Governance Reviews
	STA-07 Supply Chain Metrics
	STA-08 Third Party Assessment
	STA-09 Third Party Audits

**Table 1: Long term control loop to CSA mapping**

Short Term Control Loop	
CSA Control Category	CSA ID
Application & Interface Security	AIS-03 Data Integrity
	AIS-04 Data Security / Integrity
Business Continuity Management & Operational Resilience	BCR-01 Business Continuity Planning
	BCR-03 Datacenter Utilities / Environmental Conditions
	BCR-05 Environmental Risks
	BCR-06 Equipment Location
	BCR-08 Equipment Power Failures
Change Control & Configuration Management	CCC-04 Unauthorized Software Installations
	CCC-05 Production Changes
Data Security & Information Lifecycle Management	DSI-03 Ecommerce Transactions
	DSI-04 Handling / Labeling / Security Policy
	DSI-05 Non-Production Data
	DSI-07 Secure Disposal

Datacenter Security	DCS-03 Equipment Identification
	DCS-07 Secure Area Authorization
	DCS-08 Unauthorized Persons Entry
	DCS-09 User Access
Encryption & Key Management	EKM-01 Entitlement
	EKM-02 Key Generation
	EKM-03 Sensitive Data Protection
	EKM-04 Storage and Access
Human Resources	HRS-01 Asset Returns
	HRS-02 Background Screening
	HRS-05 Mobile Device Management
	HRS-08 Technology Acceptable Use
	HRS-11 Workspace
Identity & Access Management	IAM-02 Credential Lifecycle / Provision Management
	IAM-03 Diagnostic / Configuration Ports Access
	IAM-04 Identity & Access Management Policies and Procedures
	IAM-05 Segregation of Duties
	IAM-06 Source Code Access Restriction
	IAM-08 Trusted Sources
	IAM-09 User Access Authorization
	IAM-10 User Access Reviews
	IAM-11 User Access Revocation
	IAM-12 User ID Credentials
	IAM-13 Utility Programs Access
Infrastructure & Virtualization Security	IVS-01 Audit Logging / Intrusion Detection
	IVS-02 Change Detection
	IVS-03 Clock Synchronization
	IVS-04 Information System Documentation
	IVS-05 Vulnerability Management
	IVS-06 Network Security
	IVS-07 OS Hardening and Base Controls
	IVS-08 Production / Non-Production Environments
	IVS-09 Segmentation
	IVS-10 VM Security - Data Protection

	IVS-11 Hypervisor Hardening
	IVS-12 Wireless Security
Interoperability & Portability	IPY-04 Standardized Network Protocols
Security Incident Management, E-Discovery, & Cloud Forensics	SEF-01 Contact / Authority Maintenance
	SEF-02 Incident Management
	SEF-03 Incident Reporting
	SEF-04 Incident Response Legal Preparation
	SEF-05 Incident Response Metrics
Supply Chain Management, Transparency, and Accountability	STA-02 Incident Reporting
Threat and Vulnerability Management	TVM-01 Anti-Virus / Malicious Software
	TVM-02 Vulnerability / Patch Management
	TVM-03 Mobile Code

**Table 2: Short term control loop to CSA mapping**

### 3. REVIEW OF AVAILABLE COUNTERMEASURE PERTAINING DEFINED THREATS CLUSTERS

The list of the countermeasures relevant to RESISTO to be considered in the attack trees and corresponding use cases, structured in security categories are reported below. In each categories the countermeasures are classified as belonging to STCL or LTCL. Furthermore, security-related activities, policies and best practices pertaining each threat cluster are included. While this category of actions cannot be implemented as part of an automated response approach, they can be considered complementary to the RESISTO platform.

#### 3.1. Identity management and Access

Typical threats related to identity management categorized in communication systems are spoofing of identities and elevation of privilege. Typical identity spoofing involves illegal access of a user's authentication (e.g. username and password, smart card, badge, a phone used for multi authorization).

Once a user identity is spoofed the next step is elevation of privilege. If the attacker manages to penetrate the system's defenses, gaining access to the trusted system, this is one of the most dangerous situations. Generally, the possibility to raise the user privileges paves the way to a compromised or destroyed system.

Identity management is thus an extremely important set of actions. For an infrastructure, similar issues are faced in both the physical and the digital part of the CI of telecommunications systems. We have several countermeasures that are related to the pretended identity of a person that operates a telecommunication infrastructure. Stealing the operator identity in our analysis is described both in terms of physical assets than of the telecommunication software systems.

Credentials to access either a physical infrastructure or a software system both need to be carefully protected and procedures must be defined to handle their lifecycle and operation.

An operator of a telecommunication infrastructure is identified with a set of credentials physical (e.g. a badge, a key) or a digital identity (e.g. a PIN, a user/password).

The tables below list some countermeasures related to Identity Management and Access protection.

#### Password protection

##### Long Term Control Loop

- Do not allow passwords to be sent in cleartext.
- Encrypt the passwords with encryption algorithms or hashing functions.
- Employ one-time password tokens and/or other 2fa authentication methods (eg. biometrics)
- Use hard-to-guess passwords of at least 10 characters long.
- Rotate passwords frequently.
- Employ an IDS to detect suspicious behavior.
- Use dictionary-cracking tools to find weak passwords chosen by users.
- Use special characters, numbers, and upper- and lowercase letters within the password.
- Keep software up-to-date including latest security patches
- Protect password files.
- Salt the password database
- Any software system shouldn't use default accounts and passwords
- Periodic Vulnerability Scan
- Do not allow password reuse
- Use captcha when multiple wrong passwords are submitted from an account, IP or other

identity
•
Short Term Control Loop
<ul style="list-style-type: none"> <li>• User account lock out, de-authentication or revocation</li> <li>• Force password resets</li> <li>• IP address lockout</li> </ul>
Policies/Activities/Best practices
<ul style="list-style-type: none"> <li>• Develop responsible disclosure &amp; bug bounty programs to encourage security researchers to report vulnerabilities identified in a defined scope</li> </ul>
•

**Table 3: Password Protection**

Badge, smart cards protection
Long Term Control Loop
<ul style="list-style-type: none"> <li>• Access limitations for critical rooms/areas</li> <li>• Access logging</li> <li>• Video monitoring</li> </ul>
Short Term Control Loop
<ul style="list-style-type: none"> <li>• Badge lockout</li> </ul>

**Table 4 Badge, smart cards protection**

Phishing attacks
Long Term Control Loop
<ul style="list-style-type: none"> <li>• When submitting any type of financial information or credential data, use SSL</li> <li>• connection should be set up, which is indicated in the address bar (https://)</li> <li>• and a closed-padlock icon in the browser at the bottom-right corner.</li> <li>• Up-to-date antivirus to detect keyloggers</li> <li>• Report any suspicious email addresses to the responsible in IT security departments</li> </ul>
Short Term Control Loop
<ul style="list-style-type: none"> <li>• Spam and e-mail filtering in place</li> <li>• Send alerts regarding fraudulent messages found</li> <li>• Disable User Account</li> <li>• Block a Malware Domain</li> <li>• Block any malicious sender IP addresses</li> </ul>
Policies/Activities/Best practices
<ul style="list-style-type: none"> <li>• Review the address bar to see if the domain name is correct.</li> <li>• activity for raising awareness.</li> <li>• Be skeptical of e-mails indicating you must make changes to your account.</li> <li>• Call the legitimate company to find out if this is a fraudulent message on a different communication channel</li> <li>• Do not click an HTML link within an e-mail. Type the URL out manually instead.</li> <li>• Do not accept e-mail in HTML format.</li> <li>• Do not download or open any suspicious attachment files</li> </ul>

**Table 5: Phishing attacks**

Session Hijacking
Long Term Control Loop
<ul style="list-style-type: none"> <li>Enforce Encryption to prevent sniffing style attacks.</li> </ul>
Short Term Control Loop
<ul style="list-style-type: none"> <li>Multi Authentication to check against identity of the user.</li> <li>Regenerating of Session ID after a Successful Login.</li> </ul>

**Table 6: Session Hijacking**

### 3.2. Disruption of data or HW loss

This section describes the following classes of threats: Data tampering, Repudiation, Information disclosure.

Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.

Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise. For example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-repudiation refers to the ability of a system to counter repudiation threats.

Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it. For example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

The table below lists some countermeasures related to these threats.

Disruption of data or HW loss
Long Term Control Loop
<ul style="list-style-type: none"> <li>Continuity plan in place</li> <li>Backup and recovery measures in place</li> <li>Encrypt sensitive data</li> <li>Organized data in segments protected according to sensitivity levels, including the development of data access policy</li> <li>Tamper protection for security-critical components</li> <li>Protection against theft</li> <li>Protection against third-party influence</li> <li>Protection against illegal use of removable media</li> <li>Removable media locking</li> <li>Network segmentation</li> <li>Implement an anomaly detection methods for data transferred between employees and external connections</li> <li></li> </ul>
Short Term Control Loop

<ul style="list-style-type: none"> <li>• Backup and recovery procedure for data</li> <li>• Switch procedure on stand-by HW/SW systems</li> </ul>
<b>Policies/Activities/Best practices</b>
<ul style="list-style-type: none"> <li>• Geographical redundancy of HW/SW defined for critical systems</li> <li>• Regular Security Reviews</li> <li>• Usage of OSINT (Open Source Intelligence) tools to monitor popular internet services against leaked information</li> <li>• Develop responsible disclosure &amp; bug bounty programs to encourage security researchers to report vulnerabilities identified in a defined scope</li> </ul>

**Table 7: Disruption of data or HW loss**

### 3.3.Availability

Denial of service (DoS) attacks deny service to valid user, for instance flooding its target machine with so much traffic that it prevents it from being accessible to any other requests. The target machine is kept busy responding to the traffic it is receiving from its attacker and therefore rightful users cannot get the required services. A distributed denial of service (D-DOS) attack adds a many-to-one dimension. Protecting against DoS threats improves system availability and reliability.

DoS can be related to any part of the network at all protocol levels and devices (i.e. phones, routers, switches). Auditing and monitoring of this type of activity should be in place to uncover patterns that could indicate an attack. Example of this are phone dialing, SYN flood, UDP flood, MAC flooding, etc. Examples of countermeasures related to this category of threats are listed in the table below.

<b>(D)Dos</b>
<b>Long Term Control Loop</b>
<ul style="list-style-type: none"> <li>• Perform brute force attacks to find weaknesses and hanging modems.</li> <li>• Make sure only necessary phone numbers are made public.</li> <li>• Provide stringent access control methods that would make brute force attacks less effective</li> <li>• Limit number of MAC addresses that can be learned on ports</li> <li>• Dynamic packet filtering rules on MAC addresses installed by a AAA server</li> <li>• DMZ protection against unauthorized access from outside and controlled connection establishment from the LAN into public networks/services</li> <li>• Perform fuzzing against popular services such as http, telnet, dns, ftp, pop, smtp, etc.etc.</li> <li>• Perform vulnerability scanning against systems to identify known vulnerabilities</li> <li>• Perform stress testing against services</li> </ul>
<b>Short Term Control Loop</b>
<ul style="list-style-type: none"> <li>• Block/Shun an IP</li> <li>• Device lockout</li> <li>• Dynamic (D)dos detection</li> <li>• Employ IDSs</li> <li>• Set and enforce lockout thresholds</li> <li>• Disable Switch Port</li> </ul>

**Table 8: (D)Dos**



### 3.4. Natural Disaster

Natural disaster (weather, flood or earthquake) countermeasures (see table below) are related to the possibility to operate the infrastructure when major natural events happen in a certain area. They are very similar to the ones described in the availability section apart from the fact that the damage can impair a large number of equipment at the same time.

Service Continuity
Long Term Control Loop
<ul style="list-style-type: none"> <li>Continuity plan in place</li> <li>Geographical redundancy of HW/SW defined for critical systems</li> <li></li> </ul>
Short Term Control Loop
<ul style="list-style-type: none"> <li>Switch procedure on stand-by HW/SW systems</li> <li>Operate with temporary equipment installation</li> </ul>
Policies/Activities/Best practices
<ul style="list-style-type: none"> <li>Disaster Recovery procedures in place for large disasters with spare equipment that can be moved easily to the disaster area (i.e. in a box solutions)</li> <li>Plan for spare capacity of resources to allow relocation of services in case of disaster</li> </ul>

**Table 9: Service Continuity**

### 3.5. Physical Security – Physical Intrusion

Physical security countermeasures (see table below) address physical intrusion concerns that could affect the infrastructure and the assets. The physical protection of telecom infrastructure assets (i.e. data center) can be implemented with multiple layers of security. The first layer of protection may include fences, gates, lighting systems enhanced with intrusion detection sensors (i.e. fibre optic, vibration sensors, perimeter CCTV systems, etc.). The second layer, which is located within the area of the infrastructure, includes patrolling of security personnel, badge checks, incident response procedures, emergency communications, video/audio surveillance systems, etc.. The last level of security refers to the means of securing the building's and equipment. Such means may include, intrusion detection systems, monitored electrical/mechanical door locks, smart access control, CCTV systems, etc.

Physical Intrusion
Long Term Control Loop
<ul style="list-style-type: none"> <li>Identify all critical resources in the area (fire stations, hospitals, etc)</li> <li>Utilize topographic plans to assess adjacent land use</li> <li>Monitor CCTV system automatically</li> <li>Provide intrusion detection sensors</li> <li>Anti-drone systems for the detection of possible aerial threats</li> </ul>
Short Term Control Loop

<ul style="list-style-type: none"> <li>• Use vehicles (patrol units) as temporary physical barriers during high risk period</li> <li>• Make proper use of signs to inform interested group of people (i.e. evacuation process)</li> <li>• Remote control to restart electronic systems in case of temporary failures</li> <li>• Send security personnel to verify an occurred event that may be threat</li> <li>• Monitor alternative video feeds (adjacent cameras, UAV systems)</li> </ul>
<b>Policies/Activities/Best practices</b>
<ul style="list-style-type: none"> <li>• Remove any dense vegetation for the perimeter area</li> <li>• Open space inside the fence along the perimeter</li> <li>• Select and design barriers based on threat level</li> <li>• Install security lighting</li> <li>• Install CCTV (Video/Audio Surveillance) system</li> <li>• Prohibit parking beneath or within a building</li> <li>• Designate entry points for commercial and delivery vehicles away from high-risk areas</li> <li>• </li> </ul>

**Table 10: Physical Intrusion**

### 3.6. Combining countermeasures

Combining different sources of information and attacks that include both a cyber part and a physical attack to the infrastructure are among the contributions that RESISTO is going to address. In this section we show how different countermeasures can be combined to respond to those combined attacks/or disaster events:

- OSINT analysis or input from weather sensors give indication of large storms with flood, strong wind. We can thus expect a reduction of throughput on the equipment. Alternative resources can be installed or operated in order to guarantee the minimum level of functionality for public safety, as reported in Section 3.4.
- Antenna tilting sensor indicates more than 45% tilt. This can imply that someone compromised the antenna on purpose. A camera on the site could have reported an intrusion to the unattended site, a rescue team must be sent on site to fix the issue.
- OSINT analysis can provide input regarding terroristic actions in certain locations so a CP and DR plans must be put in place. All potentially interested equipment can be localized cross-analysing locations from the news.
- A person picture taken by a local camera accessing a building is cross-checked with the employee's database picture and the name from the badge used to identify un-authorized personnel. The user account and badge are locked out to avoid further progress in the potential intrusion and a guard is sent to verify the identity.
- Virtualization technologies like VNF and SDN offer a range of possible actions compared to traditional equipment. It is possible to migrate virtual machines or containers automatically to handle increase in load by resource scaling to handle for instance to DDOS attacks or congestion in the network. It is possible to remove a compromised virtual machine, change the path of data if a physical port or an entire switch fail.

## 4. Basic attack trees

ADT are models that represent an attack as a sequence of possible actions. The root node of the tree is the final objective of the attack (e.g. impair service from site, steal data from storage), while subsequent nodes describe the steps necessary to get to the final objective (e.g., to steal user data, the attacker needs to either access the storage physically or digitally. To gain physical access, a fake badge is needed and so on). Countermeasures are represented as below the action they counteract. ADT provide a simple and intuitive way to model an asset security, enabling at-a-glance understanding of the weak points of the security model as well as detailed understanding of the workflows of attacks.

This section includes a number of basic ADT that can be re-used in several use cases.

Basic attack trees represent the attack in a more general way and can be expanded based on the structure that must be protected. As an example, analyzing the objective of gaining access to a restricted area, while a basic tree will only have a node, marked as “force door”, a more detailed tree will include a node for each point of access to the facility.

Note, that the attacks nodes are red circles whereas the defense nodes (countermeasures) are green rectangles with different hues to differentiate among predictive, detective and corrective countermeasures.

### 4.1. Unauthorized access to deliberately compromise a site

#### Basic Tree #1.

##### Steal user credentials

Any attempt to use credential in a location or timeframe that is not commonly used can be elaborated and generate alerts in RESISTO. In case cameras are present on the site during access they need to be put out of service or creating false perceptions - freezing video of digital (IP) cameras or streaming recorded footage to the guard's monitor.

##### Countermeasures

- Detection of potentially anomalous accesses shall raise the alert level and trigger an inspection; example of events that can increase the alert level are: use from IP address range that is not usual: analogously for the PC or smartphone used (IMEI or PC serial number should be registered and checked during connection), for the source IP address used; number of failed logon attempt over a certain level. The same information should be considered aggregated for group of users with similar profile (since they could be trying on several user credentials). Work schedule of the users should be centralized to cross-check if user should be working when the access was attempted, but also if the user actually succeeds in the end; furthermore, the trail logs shall be analysed and the commands given during the session could be ranked and analysed.
- If two independent systems are used for physical (badge) and cyber (login credentials) access, the analysis shall consider the two together (only people that are supposed to be inside according to the physical access should be actually using the terminals inside a facility).
- Camera system used shall be able to detect impairment and freezing of video. The following also shall be implemented:
  - Camera movement/displacement detection
  - Camera tampering detection

- Camera blur detection
- Facial recognition shall be used to match the user id with the picture of the owner to prevent undetected use of a badge from another person. If this is impossible due to the person “hiding” in some way the personal traits (e.g. by wearing a scarf) this should raise an alert and increase the level of alert of the RESISTO system.
- User account lock out.
- IP address lockout.
- Adding filtering on e-mails.

## **Neutralize remote surveillance**

### **Countermeasures**

- In case cameras are present on the site during access they need to be put out of service or creating false perceptions - freezing video of digital (IP) cameras or streaming recorded footage to the guard's monitor. Freezing of video should be detected.
  - Camera movement/displacement detection
  - Camera tampering detection
  - Camera blur detection
- Facial recognition shall be used to match the user id with the picture of the owner to prevent undetected use of a badge from another person. If this is impossible due to the person “hiding” in some way the personal traits (e.g. by wearing a scarf) this should raise an alert and increase the level of alert of the RESISTO system.
- User account lock out.
- IP address lockout.
- Adding filtering on e-mails.

## **Gaining Physical access to the site**

- Breaking or Disconnecting cables.

### **Countermeasures**

- LOS alarms can be detected from the NOC and depending on the alarms reported the cause of the problem and distinguish between a voluntary damage or a failure in some equipment component, in any case a backup path is available or a redundancy is present in the equipment a reconfiguration can solve the issue
- Auxiliary alarms can be used to detect unattended remote site issues reporting alarms to the network management system (e.g. door open, badge reader not working).
- Tilting an antenna to impair line of sight.

### **Countermeasures**

- Antennas tilting sensors can be installed to distinguish between a situation that is temporary or one where personnel must be sent on site to fix the antenna position

**Hacking onsite operational systems** creating a direct outage or damage to power, elevators, fire alarms, and even damage production systems.

### **Countermeasures**

If a sensor is connected to RESISTO this can raise an event indicating the UPS is being used

### Hacking the production system

Physically connecting to the equipment (need user and password or similar of course) from a terminal for instance and execute commands that can damage or alter the production system.

### Countermeasures

This can be found analyzing the equipment command logs and account can be blocked or disconnection of the user forced

The countermeasures which would be adopted to prevent, detect and correct these attacks are the following:

Countermeasure	Type	RESISTO Platform Loop	Associated attacks	Description
<b>Detecting usage anomalies</b>	Predictive	Short Term	Stolen credentials	Access from unusual locations, and any other anomaly in the behavioural pattern can be identified in the predictive engine of RESISTO
<b>Camera frozen or disabled</b>	Corrective	Short Term	Un-authorized access	Techniques to check a camera is not reporting still images shall be in place, this can be done using ML techniques. Cameras with directional arms could be also used.
<b>Camera movement/displacement detection</b>	Detective	Short Term	Physical intrusion	This module can be considered a type of security warning detecting whether the camera is manually moved by the intruder.
<b>Camera tampering detection</b>	Detective	Short Term	Physical intrusion	Module that detects if a camera has been obscured or blinded. The main reasons for this kind of tampering are the sunshine and the climatologic conditions. This module, however, is also able to detect if an intruder is manually tampering the camera.
<b>Camera blur</b>	Detective	Short Term	Physical intrusion	Module that detects if the camera image is blurry. It enables to detect if the camera is not correctly focused due to changes on position or zoom.
<b>Disable device account</b>	Preventive	Short Term	Stolen Device	If a smartphone or any other device used for multilevel authorization device should be

				disabled and put on a black list
<b>Account lockout</b>	Corrective	Short Term	Stolen credentials	In case user credentials are suspected to be in someway been captured with a phishing attack or similar technique accounts can temporarily disabled
<b>Report power issue</b>	Detective	Short Term	Storm	If the team on site verifies that power supply is not working shall report an issue to the company responsible for the power grid (cascading effect)
<b>Send temporary equipment</b>	Corrective	Short Term	Disrupt Cell	Movable equipment can be sent in the disaster area to provide temporary coverage for telecom services to public safety and rescue teams
<b>Detecting modification to equipment</b>	Predictive	Short Term	Damage telecom Node	Command logs can be analyzed and commands that are not in line with user profile or that are suspicious can be reported as alarms (removal or transfer of large number of files, configuration commands that if misused can impair a system, etc.etc.)
<b>Detecting tampering on files containing sensitive information</b>	Detective	Short Term	Acquire sensitive info for instance to access the node	Alarms are raised when sensitive files like the ones containing passwords or logs are modified to cover unauthorized access and/or commands
<b>Damage to equipment can create a cascading effect to the other CI</b>	Predictive	Short Term	Damage another CI	IOT or other CI can use a telecom infrastructure to provide a service and so tampering a telecom site can create a cascading effect on the other CI

**Table 11: Unauthorized access to deliberately compromise a site**

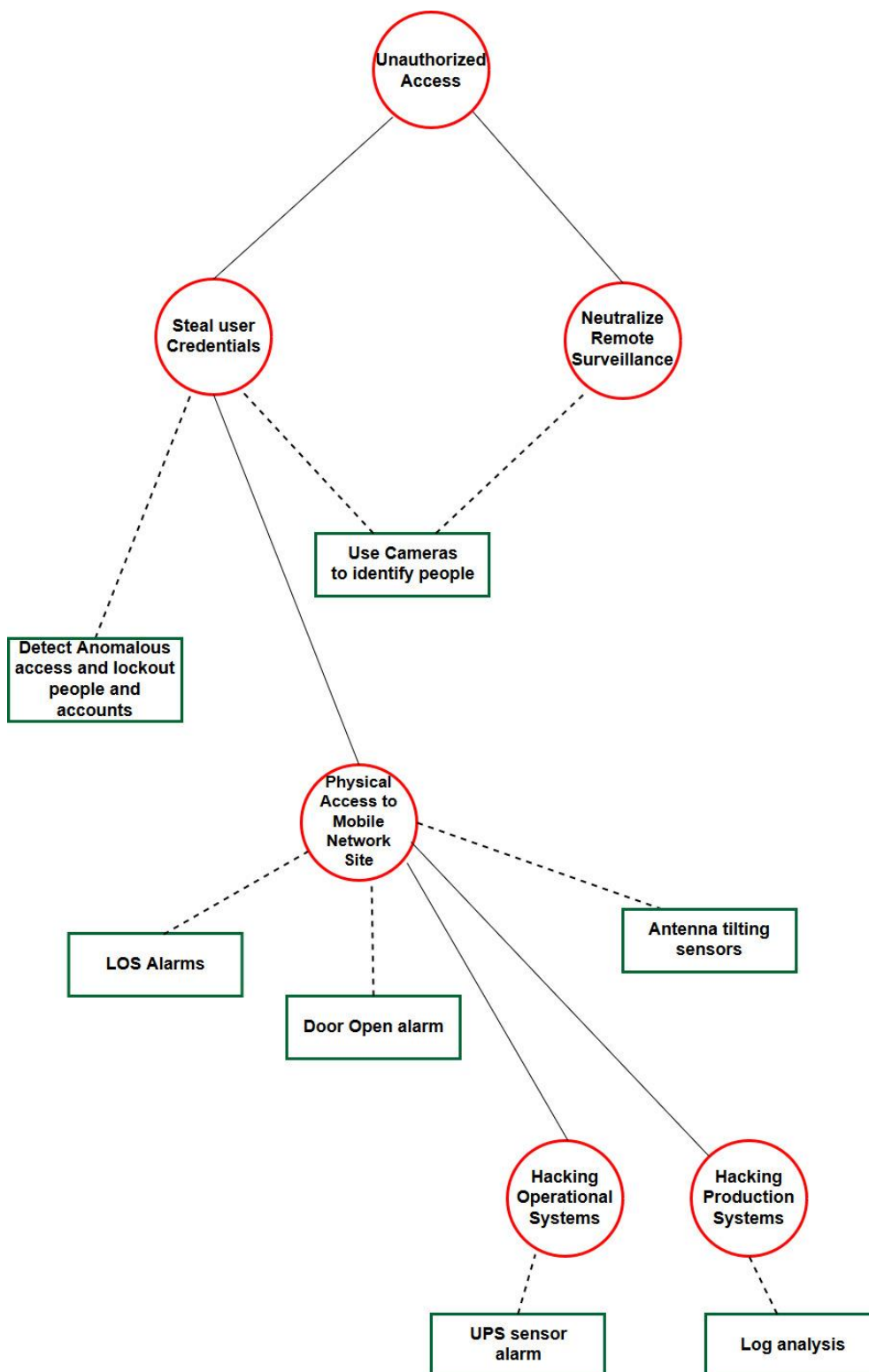


Figure 1: ADT Unauthorized Access



## 4.2. Natural disaster compromising a site

### Basic Tree #2.

#### Physical Threat to a site because of weather, flood or earthquake.

In case of disaster the following points need to be available in RESISTO through some sensors and OSINT techniques this will add new steps to the standard handling of such an event.

#### Attack

- A storm is approaching

#### Countermeasures

- Osint analysis alerts the system that in a certain area there is a storm with subsequent flood
- Verify that all procedures are in place for the locations interested by the storm
- Depending on the expected/predicted damages the inventory is verified for the area
- If available emergency equipment and corresponding teams are alerted and prepared

#### Minor Severity storm:

- Breaking or Disconnecting cables of the equipment
- Limited damage of onsite operational systems - outage or damage to power, elevators, fire alarms, and even damage production systems that can be recovered in a few hours with right spare parts
- Tilting an antenna so that does not have line of sight

#### Countermeasures

- Send team on damaged sites
- Report to the owner of the power grid that site is out of power

#### Extreme Severity storm:

- Building where the antenna is installed is damaged preventing access.
- Damage onsite operational systems - outage or damage to power, elevators, fire alarms, and even damage of production systems.
- Antenna pole tilted with damage to all the antennas that cover a large area.

#### Countermeasures

- Plan for installation of moveable equipment to guarantee basic communication in the areas.
- Re-plan and extend the coverage of the cells.
- Verify that all procedures are in place for the locations interested by the storm.
- Depending on the expected/predicted damages, verify th inventory for the area.
- Alert and prepare available emergency equipment and corresponding teams.



Geographical relocation of services. The countermeasures which would be adopted to prevent, detect and correct these attacks are the following:

Countermeasure	Type	RESISTO Platform Loop	Associated attacks	Description
<b>Osint weather analysis generates alerts</b>	Predictive	Short Term	Storm	Osint analysis alerts the system that in a certain area there is a storm with subsequent flood
<b>Verify natural disaster procedures</b>	Preventive	Short Term	Storm	Verify that all procedures are in place for the locations interested by the storm that personnel is alerted and they have the correct equipment to handle this specific. Depending on the expected/predicted damages the inventory are verified for the area. If available emergency equipment and corresponding teams are alerted and prepared
<b>Send team on damaged sites</b>	Preventive	Short Term	Storm	Send team on damaged sites where physical intervention is needed with spare equipment to replace or repair equipment
<b>Perform network reconfiguration to cover the area</b>	Corrective	Short Term	Storm	Perform reconfiguration of the network from the telecom operator operation center
<b>Report power issue</b>	Detective	Short Term	Storm	If the team on site verifies that power supply is not working shall report an issue to the company responsible for the power grid (cascading effect)
<b>Send temporary equipment</b>	Corrective	Short Term	Disruption of site equipment	Movable equipment can be sent in the disaster area to provide temporary coverage for telecom services to public safety and rescue teams

**Table 12: Physical Threat to a site because of weather, flood or earthquake**

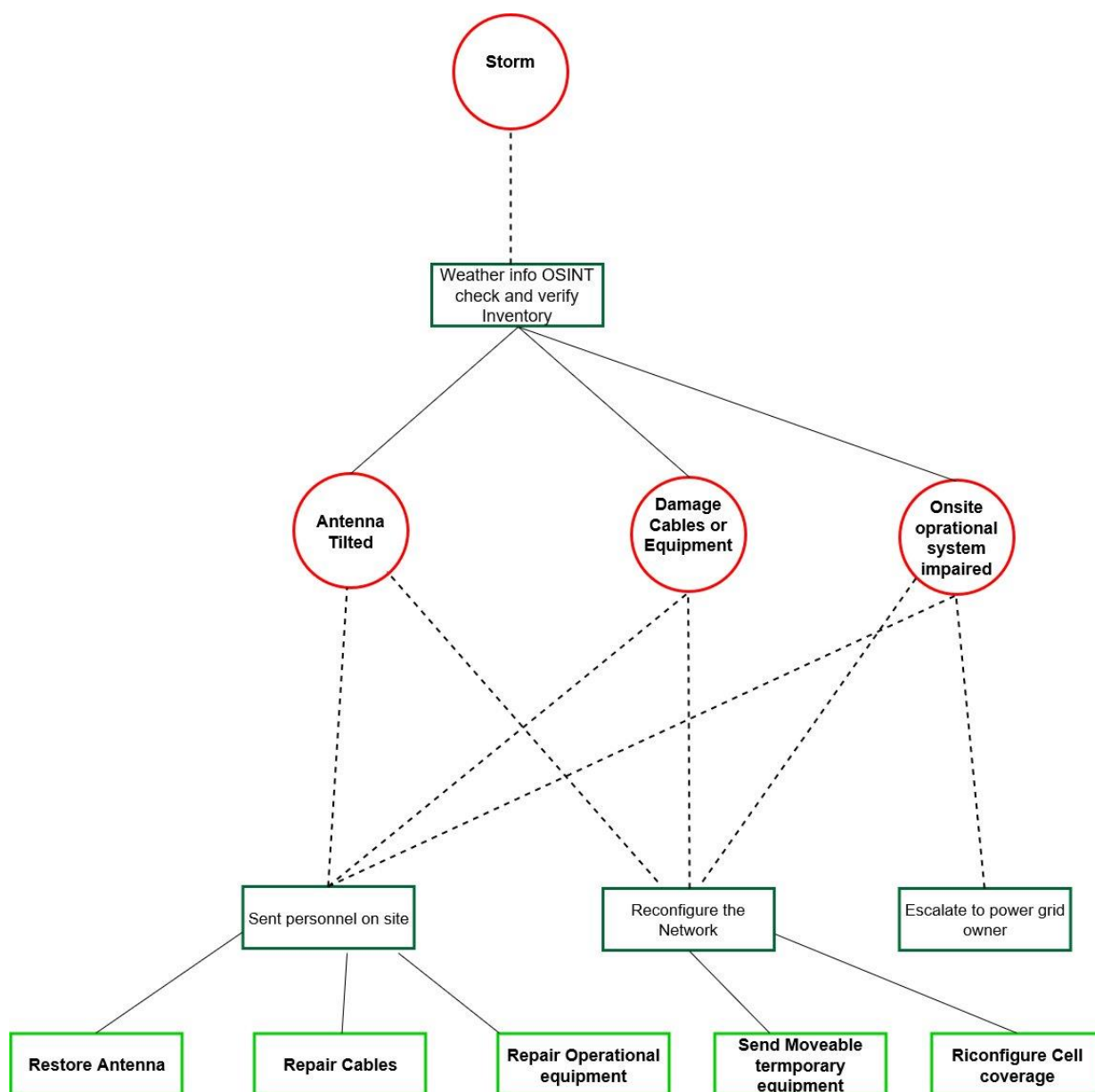


Figure 2: ADT for service disruption caused by storms

### Basic Tree #3.

#### Congestion of the core network due to of natural disaster (e.g. Weather, flood, earthquake).

In case of major natural disaster, described with basic tree #2, further consequences can be reported for instance some buildings hosting core network equipment can become inaccessible and a large part of the network can divert the operations towards the rest of the telecom network, causing an overload. Moreover, all the load at the same time many people

will try to use the telecom network to contact relatives, friends and public safety organization (i.e. police, fire brigades, hospitals).

### Attack

- Service requests increase for equipment
- Increased network load
- Failure in the initiation of requests causes an additional increase of the initial phases of the service requests.
  - Effect: Network congestion spreads

### Countermeasures

- Geographical relocation of services
- Increase capacity to specific core network nodes<sup>1</sup>

The countermeasures which would be adopted to prevent, detect and correct these attacks are the following:

Countermeasure	Type	RESISTO Platform Loop	Associated attacks	Description
<b>Geographical relocation of services</b>	Corrective	Short Term	Natural disaster	Osint analysis alerts the system that in a certain area there is a major natural disaster
<b>Perform Geographical switch to backup site</b>	Corrective	Short Term	Natural disaster	If the continuity plan has foreseen a geographical redundancy of the telecom nodes the switch to the backup system can be performed
<b>Perform network reconfiguration</b>	Corrective	Short Term	Natural disaster	Perform reconfiguration of the network from the telecom operator operation center to increase capacity on the network part that is still working

**Table 13: Congestion of the CN due to overload because of natural disaster**

### Basic Tree #4

#### **Congestion of the core network or edge network in 5G due to of natural disaster (e.g. Weather, flood, earthquake).**

In case of major natural disaster, described with basic tree #2, further consequences can be reported for instance some buildings hosting core network equipment can become inaccessible and a large part of the network can divert the operations towards the rest of the telecom network, causing an overload. Moreover, all the load at the same time many people will try to use the telecom network to contact relatives, friends and public safety organization (i.e. police, fire brigades, hospitals).

In this description we specialize Basic Tree #3 in case the network based on 5G and slicing enables a more flexible reconfiguration of the network thanks to the virtualization of the

<sup>1</sup> note this is a very limited capacity, if at all possible, for most of the equipment in current networks, in the 5G scenario we will see that virtualization allows maximum flexibility using capacity scaling

resources and the possibility to define networks in software. In 5G it is also possible that a service provider uses different operators' infrastructures for the same service. In this case planning of service availability should be implemented by more than one organization. More details on this topic are given in "5G network response to a security breach".

In this case there are several actors that are collaborating to provide a service. the most complex scenario has different levels; there is in fact a Communication Service Customer which can be a manufacturing company that uses the Communication Service, the Operator which provides a Communication Service and is the consumer of the Network Slice(s) and Network Slice Provider which is a Network Operator which provides a Network Slice aggregating Network Slice Subnets provided by a Subnet Network slice provider.

### Attack

- Service requests increase for equipment.
- Increased network load.
- Failure in the initiation of requests causes an additional increase of the initial phases of the service requests.
  - Effect: Network congestion spreads.

### Countermeasures

- Increase capacity to specific core network nodes using spare capacity using virtualized resources orchestration features.
- Slices failures occur in the network.
  - Effect: services provided by the slices are not available.

### Countermeasures

- Geographical relocation of services, recreating the slices using the resources that are still available.
- Increase capacity to specific subnetworks using spare capacity in the virtual infrastructure or use slice priority to perform the allocation of the additional resources.

The countermeasures which would be adopted to prevent, detect and correct these attacks are the following:

Countermeasure	Type	RESISTO Platform Loop	Associated attacks	Description
<b>Geographical relocation of services</b>	Corrective	Short Term	Natural disaster	Osint analysis alerts the system that in a certain area there is a major natural disaster
<b>Orchestrate virtual resources to scale capacity</b>	Corrective	Short Term	Natural disaster	Increase capacity to specific core network nodes using spare capacity using virtualized resources orchestration features
<b>Perform Geographical relocation of slices</b>	Corrective	Short Term	Natural disaster	Operators in 5G have the possibility to share part of the network resources slicing could be implemented in a way as to span of different telecom providers

Perform slices reconfiguration	Corrective	Short Term	Natural disaster	Perform dynamic orchestration of the subnet network slices to restore network slices to guarantee services to the customers
--------------------------------	------------	------------	------------------	---

Table 14: Congestion of the core network because of Natural disaster

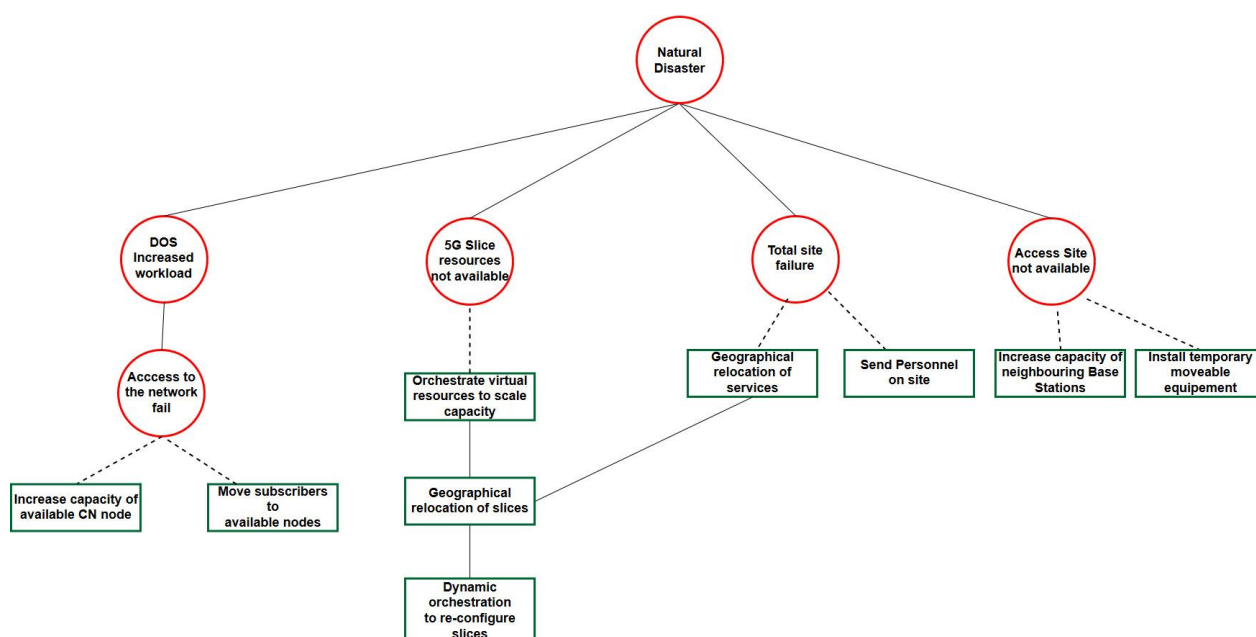


Figure 3: ADT summarizing service disruption caused by natural disaster cases

### 4.3. Disruption of Telecom Operator Cell Service

#### Basic tree #5

This section describes the potential set of attacks that a telecom operator RAN network site (base station) could suffer, affecting the regular service that one or several of the cells associated to that site should be normally providing.

Below, a list of potential attacks by which a malicious attacker could reach their main goal of disrupting the cell service is shown, along with additional remarks. In this case, given that the attack is caused by a human agent (as opposed to a natural event), the workflow is more articulated and the resulting ADT more complex.

- **Change Cell Configuration (Change Tx power, cell IDs, control channel parameters...)**
  - Get into OT Network (Operational Technology Network)
    - Steal Access Credentials
      - Evil Twin (MITM attack to get credentials from users)

- Employee Rogue Wi-Fi AP (*unauthorized, poorly configured AP*)
- Place Rogue Wi-Fi AP (*connected to the OT network*)
  - Unauthorized Access
    - Climb Tower
    - Break in
      - Force door
      - Force Window
    - Steal Keys/Key card
- **Stop/Degrade Tx and/or Rx (*The TRX equipment is tampered with*)**
  - Damage/Steal Cables or Equipment
    - Unauthorized Access
      - Climb Tower
      - Break in
        - Force Door
        - Force Window
      - Steal Keys/Key card
  - Damage/Tamper with AC System
    - Unauthorized Access
      - Climb Tower
      - Break in
        - Force Door
        - Force Window
      - Steal Keys/Key card
    - Disconnect Power Supply
- **Prompt Cell Restart or Failure (*Cells with wrong IDs leading to e.g. PCI collision*)**
  - Uncoordinated cell (*Femtocell, bordering cells, poorly installed cell, etc...*)
  - Rogue cell (*IMSI-catchers*)
- **Degrade Overall Cell C/N+I (*Could make any communication with that cell impossible*)**
  - Uncoordinated Cell (*Femtocell, bordering cells, poorly installed cell, etc...*)
  - Rogue cell (*IMSI-catchers*)
  - Barrage Jammer (*Jamming interference occupying the whole cell channel*)
  - Other transmitters (*DVB-T towers, repeaters, amplifiers, filters...*)
  - Channel Jammer (*Jamming interference targeting a specific PHY cell channel*)
  - IM (*Intermodulation Interference*)
- **Degrade Cell Specific Physical Channel C/N+I (*Could prevent connection and handovers to that cell*)**
  - Channel Jammer (*Jamming interference targeting a specific PHY cell channel*)

The countermeasures which would be adopted to prevent, detect and correct these attacks are the following:

Countermeasure	Type	RESISTO Platform Loop	Associated attacks	Description
Send Specialized Team/Temporarily Disable Cell	Corrective	Short Term	Disrupt Cell	Upon whitelisted cell anomaly alarm reception, corrective measurements should

				be applied: A specialized team should be sent to the site and/or the cell be temporarily disabled
<b>Raise Cell Anomaly Alarm</b>	Detective	Short Term	Disrupt Cell	If an anomaly in any value of the whitelisted cells has been detected this might mean the service has been disrupted, an alarm should be raised. This can be a combination of both a physical alarm and a notification to operator security staff
<b>Detect Cell Anomaly</b>	Detective	Short Term	Disrupt Cell	The SSS tool should monitor the whitelisted cells key parameters such as received power or ID to check that there aren't any anomalies in signal and configuration monitored values
<b>Change Network Configuration</b>	Corrective	Short Term	Get into OT network	If the attacker has managed to gain access into the Operational Technology network, the main parameters for the network configuration should be changed (credentials, ports, IP addresses)
<b>Change Access Credentials</b>	Corrective	Short Term	Steal Access Credentials	If the attacker has managed to steal the access credentials to the Operational Technology network, the access credentials should immediately be changed
<b>Detect Unknown AP</b>	Detective	Short Term	Evil Twin, Employee Rogue Wi-Fi AP or Place Rogue Wi-Fi AP	The SSS tool should detect unknown (non-whitelisted) Access Points
<b>Raise Unknown AP Alarm</b>	Detective	Short Term	Evil Twin, Employee Rogue Wi-Fi AP or Place Rogue Wi-Fi AP	If an unknown Wi-Fi AP (i.e. is not included in the SSS whitelist) has been detected, an



				alarm will be raised. This alarm can be a combination of both a physical alarm and a notification to the operator's security staff
<b>Blacklist Unknown AP</b>	Preventive	Long Term	Evil Twin, Employee Rogue Wi-Fi AP or Place Rogue Wi-Fi AP	If an unknown Wi-Fi AP (i.e. is not included in the SSS whitelist) has been detected, the AP should be automatically blacklisted
<b>Estimate Unknown AP Location</b>	Detective	Short Term	Evil Twin, Employee Rogue Wi-Fi AP or Place Rogue Wi-Fi AP	If an unknown Wi-Fi AP (i.e. is not included in the SSS whitelist) has been detected, the SSS tool could roughly estimate the location of the AP (outside or inside the site)
<b>Detect Unknown Device</b>	Detective	Short Term	Unauthorized Access	The SSS tool should detect unknown (non-whitelisted) Wi-Fi and Bluetooth Devices
<b>Raise Unknown Device Alarm</b>	Detective	Short Term	Unauthorized Access	If an unknown Wi-Fi or Bluetooth Device (i.e. is not included in the SSS whitelist) has been detected, an alarm will be raised. This alarm can be a combination of both a physical alarm and a notification to the operator's security staff
<b>Blacklist Unknown Device</b>	Preventive	Long Term	Unauthorized Access	If an unknown Wi-Fi or Bluetooth Device (i.e. is not included in the SSS whitelist) has been detected, the device should be automatically blacklisted
<b>Estimate Unknown Device Location</b>	Detective	Short Term	Unauthorized Access	If an unknown Wi-Fi or Bluetooth Device (i.e. is not included in the SSS whitelist) has been detected, the SSS tool could roughly estimate the location of the AP (outside or inside the



				site)
<b>Contact Owner</b>	Corrective	Short Term	Uncoordinated Cell	If an uncoordinated cell is detected, the owner of the cell should be contacted to let him/her know to stop transmitting. This could be a femtocell (e.g. Home eNB) user or another cell operator.
<b>Improve C/N+I</b>	Corrective	Short Term	Degrade Overall Cell C/N+I And Degrade Cell Specific Physical Channel C/N+I	If the Cell overall C/N+I has been degraded, a set of actions including: decreasing the modcod, increasing the transmitting power, changing antenna tilt among others could be applied to the cell transmitter to improve the quality of the signal to interference and noise ratio
<b>Detect Rogue Cell</b>	Detective	Short Term	Rogue Cell	The SSS tool should detect rogue cells
<b>Detect Uncoordinated Cell</b>	Detective	Short Term	Uncoordinated Cell	The SSS tool should detect uncoordinated cells
<b>Blacklist Unknown Cell</b>	Preventive	Long Term	Uncoordinated Cell and Rogue Cell	If an unknown (uncoordinated or rogue) cell (i.e. is not included in the SSS whitelist) has been detected, this should be automatically blacklisted
<b>Raise Unknown Cell Alarm</b>	Detective	Short Term	Uncoordinated Cell and Rogue Cell	If an unknown (uncoordinated or rogue) cell (i.e. is not included in the SSS whitelist) has been detected, an alarm should be raised. This can be a combination of both a physical alarm and a notification to operator security staff
<b>Raise Interference Alarm</b>	Detective	Short Term	Barrage Jammer, Other Transmitters, Channel	If some interference has been detected, an alarm should be raised.

			Jammer and IM	This can be a combination of both a physical alarm and a notification to operator security staff
<b>Detect Interference</b>	Detective	Short Term	Barrage Jammer, Other Transmitters, Channel Jammer and IM	The SSS tool should detect different types of radio interferences in the cell.
<b>Detect AC system down</b>	Detective	Short Term	Damage/Tamper with AC System	If an attacker was able to tamper with the site's AC system, an anomaly in supplied power at the site should be detected
<b>Raise AC Alarm</b>	Detective	Short Term	Damage/Tamper with AC System	If an AC supply anomaly is detected, an alarm should be raised. This alarm could be a combination of both a physical alarm and a notification to the operator's security staff
<b>Switch to back-up AC system</b>	Corrective	Short Term	Damage/Tamper with AC System	If AC system down alarm has been received, an attempt to switch to a backup AC power source should be issued.

**Table 15 Disruption of Telecom Operator Cell Service**

A detailed ADT has been created to put together all the countermeasures and their associated attacks for the cell disruption adversary target.

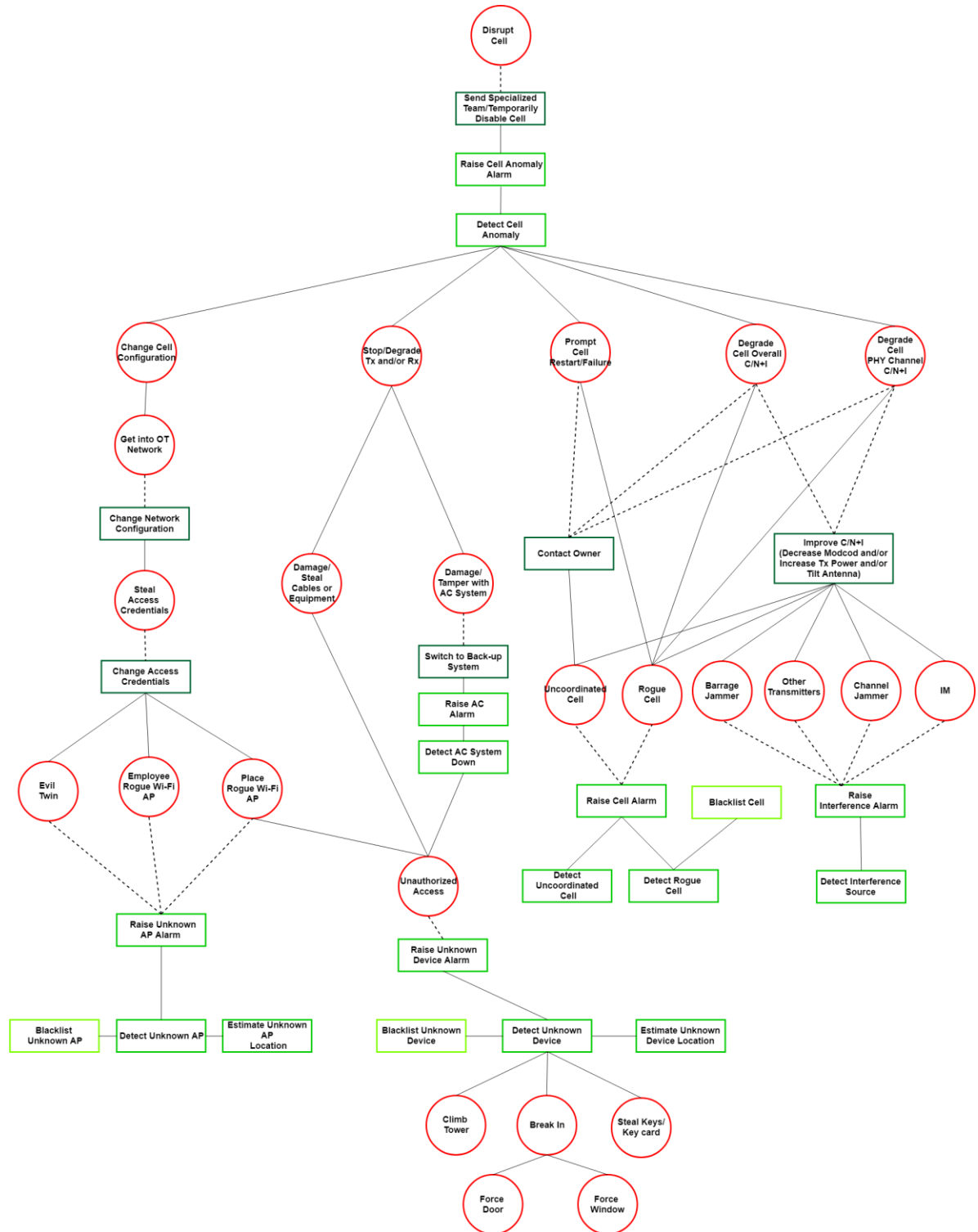


Figure 4: ADT for disruption of cell service

#### 4.4. Alternative visualizations for attack trees

ADTs offer a simple and intuitive way to represent the workflow of an attack as well as identify potential criticalities in the security model of a site. However, there are some drawbacks in the default representations shown in this Section.

The first drawback is scalability. As can be seen, as the target asset becomes more complex (e.g. larger attack surface, larger site, more assets), the correspondent tree becomes progressively less interpretable and intelligible. This pattern becomes immediately apparent by comparing Figure 1 and

Figure 4 as the model gets more complex, it is increasingly difficult to understand it.

A second issue in using ADT is how to integrate real-time information about the system status and ongoing events. As a matter of fact, the ADT only describes the workflow of the attack, their usefulness is limited to the assessment/long-term planning phase of the system security. On the other hand, if real-time events could be integrated in the tree (e.g. current risk of attack to a given service is considered higher due to an unusual number of failed login attempts), operators could use the ADT to get an immediate understanding of the current situation, complete with possible repercussions of the ongoing attacks.

To cope with this limitations, alternative visualizations and implementations of ADT have been and are being studied.

To cope with visualization issues in high-dimensional trees, hierarchical visualization was found to be the only feasible way. By hierarchical visualization we mean displaying only the top-most nodes of the tree, giving the operator the possibility to zoom on and explore on the tree's branches by clicking. Trees are represented as JSON files, so that it is possible to encode additional information about any given attack. As an example, to enable the operator to get an immediate understanding of the current situation, a value is assigned to each leaf node of the ADT that corresponds to a hostile action. The root node will be colour-coded, and display information on the currently most critical node (i.e. a darker shade will mean that there is at least one node with a risk score higher than a certain value. The node involved will be shown underneath the root node). In this way, the operator can quickly navigate through the graph, and understand how the system is being attacked as well as get an intuition of how the platform is reacting.

Figure 5 illustrates a preliminary implementation of the proposed approach to ADT visualization, corresponding to the ADT of Figure 4. As can be seen, the root node assumes the colour and the value of the most critical node in the tree, displaying the corresponding risk score. Any node can be clicked in order to zoom and obtain a clearer view of the current situation. A more refined version of this visualization technique will be presented in D5.4.

At the link below the file with the json code of "Disruption of cell service tree (Figure 5)" is available:

<http://bit.ly/2UUFg27>

while the following link is the web page where the interactive visualization of the tree is available:

<http://bit.ly/2W5awrM>



Figure 5: Interactive ADT visualization

## 5. USE CASES

Main focus of RESISTO is the support of the scenarios described in the following via a number of use-cases, in different contexts and applications, while serving a wide variety of service provision aspects. These include: changes in network topology; increasing capacity requirements in dense environments, etc. These scenarios will exploit system capabilities and solutions together with network and topology integration. Each included use-case will be described in terms of the attack steps and detective and corrective actions.

Below we are reporting a summary table of events with relevant information to be considered in the implementation of RESISTO control loop.

Event	Threat	Detection	Sensor	Human Action	Corrective Action
Badge stolen	Unauthorized access to damage CI	Report a badge was stolen and all accesses are controlling that badge is not used	Badge not used by the intended person	Security personnel can stop and arrest the unauthorized user	Badge is disabled
Credentials stolen	Unauthorized access to damage CI	Check phishing was not on going (maybe can be reported)  Anomalous activity from the logs, wrong time of the day, wrong place	Id are not used by the intended person	Security personnel can stop and arrest the unauthorized user	User account disabled
Local Login into equipment	Unauthorized access to damage CI	Analyze equipment logs	Internal cameras verify there is someone in the telecom site	Security personnel can stop and arrest the unauthorized user	User account disabled
Slice failure	Natural disaster	Osint weather conditions, fire news via Osint, public safety network or fire alarm sensors, seismic sensor networks alerts	A disaster has happened and the area affected is detected, parts of the network are not available so network elements will report alarms or performance	Use dynamic reconfiguration using the virtualized orchestration of the network resources	Slices are reconfigured

			degradation		
Network congestion	Storm	Osint weather conditions, alarm and performance thresholds alarms	In the area affected by the storm network elements will report alarms or performance degradation	Increase capacity in the part of the network that are still available to provide	Service level is restored to the best possible level
Camera frozen or disabled	Unauthorized access to damage CI	Camera is disconnected or image looks still	Cameras are frozen	Security personnel can stop and arrest the unauthorized user	Camera software shall detect this kind of anomalies
Detecting modification to equipment	Unauthorized access to damage CI	Analyze equipment logs	Internal cameras verify there is someone in the telecom site	Security personnel can stop and arrest the unauthorized user	Command logs can be analyzed and commands that are not in line with user profile
Door is forced open	Unauthorized access to damage CI	Alarm raised via auxiliary board to network management	Internal cameras verify there is someone in the telecom site	Security personnel can stop and arrest the unauthorized user	Verify alarm list
Site is running on UPS	Unauthorized access to damage CI or natural disaster	Alarm raised via auxiliary board to network management	Internal cameras verify there is someone in the telecom site or a disaster has happened and network elements will report alarms or performance degradation	Notify power CI supplier or send personnel on site to fix the issue	Verify alarm list for LOS or threshold alarms
Equipment disconnected from the network manager	Unauthorized access to damage CI or natural disaster	Alarm raised by the network manager	Internal cameras verify there is someone in the telecom site or a disaster has happened and network	Maintenance personnel can stop and arrest the unauthorized user	Verify alarm list for LOS or threshold alarms

			elements will report alarms or performance degradation elements will report alarms or performance degradation		
Disrupted cell	Unauthorized access to site, intentional/malicious attacker	Detect Unknown AP/Device, uncoordinated/rogue Cell and/or interference source	SSS (Smart Spectrum Surveillance System)	Receive alert and arrive to site, change cell/OTE network configurations, contact/search for AP/cell owner	Change network configuration, Improve cell signal C/N+I, contact/search for disruption source

**Table 16: Summary table of Events**

The below table is included to summarize which of the trees described in chapter 4 can be applied to each use case. A more detailed analysis will be reported in D5.4.



USE CASE	TREE				
	#1	#2	#3	#4	#5
Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites	✗				
Telecommunications congestion caused by natural (Earthquake) or man-made (i.e. Multiple Terrorist Attacks) hazards in Athens	✗	✗	✗		
Protection of (TI Sparkle's) ISP Backbone Nodes	✗		✗		
Telecommunication sites	✗				✗
Disruption of major sporting event by combined physical & cyber-attack by a terrorist organisation	✗	✗	✗		
Protection of (TI Sparkle's) ISP Backbone Nodes	✗		✗		
Protection of Cloud Storage Services	✗		✗		
Cyber and physical protection of network and network elements mechanisms used by critical services that impact users	✗	✗	✗		
Maritime Safety and Emergency Case		✗			
Smart Manufacturing Data Integrity Protection using a block-chain based mechanism	✗				
PPDR Virtual Operator		✗			✗
5G network response to a security breach	✗	✗		✗	✗

Table 17: Summary table of use cases and trees applicability

## 6. CONCLUSION

In summary RESISTO will propose the following classification for actions and a corresponding implementation for each:

- Preventive
- Predictive
- Detective
- Corrective

The predictive actions will be a novel characterization of RESISTO and will produce additional indication using data collected from the telecom network.

Moreover, the short and long control loop are addressed by specifying which countermeasures are more suited for the long-term improvement of the infrastructure and which can be implemented as a direct response to threats in the short term.

OSINT techniques can be used to provide hints on threats and disruptive events, and they should be integrated in the attack trees to show how this information can be used in order to complement traditional monitoring of telecom infrastructure. Building a predictive engine and providing information on the likelihood of an event adds a significant dimension to the normal modelling of threats and countermeasures, behavioural anomalies or new attack patterns can be predicted using machine learning techniques.

The scenarios analysed in the present document will form the baseline of the countermeasures that will be used against attacks, including both physical and cyber aspects, the application of which will define protections to be applied in the next tasks of the WP5, given the use case definition that will be finalized in WP2.

In WP4 RESISTO will analyse “Tools and techniques for Monitoring and Detection of cyber-physical threats”, which includes a variety of hardware and software tools and technologies for detection and monitoring of anomalous conditions, intrusions and threats:

- To define, enable and implement a complete set of sensors and cyber tools necessary to detect cyber/physical attacks.
- To extract potential intrusion events and process them into alert functionalities for constant alarm monitoring.

The above sensors are the ones indicated in the attack trees to implement in practice the controls able to detect various attacks. More specifically task 4.1 has already defined a set of sensors able to monitor and detect intrusions anomalies in the vicinity of telecom CIs (i.e. buildings, remote antenna parks, “grey zones”, telecom pillars on high rooftops), either ground-based or airborne (small UAVs or drones).

## 7. REFERENCES

INDEX	REFERENCE
1	Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 NIST
2	CSA_CCM v.3.0.1 11-12-2018
3	Top Threats to Cloud Computing: Deep Dive Release Date: 08/08/2018 by CSA
4	LTE; Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes - ETSI TR 133 926 V14.0.0
5	Virtual network security: threats, countermeasures, and challenges Bays et al. Journal of Internet Services and Applications (2015) 6:1 DOI 10.1186/s13174-014-0015-z
6	Stallings W (2006) Cryptography and Network Security: Principles and Practice. Pearson/Prentice Hall, Upper Saddle River, New Jersey, USA
7	Virtual Network Security: Threats, Countermeasures, and Challenges December 2015 DOI: 10.1186/s13174-014-0015-z
8	Foundations of Attack–Defense Trees, September 2010, DOI: 10.1007/978-3-642-19751-2_6