

RESISTO: D10.11_EXPLOITATION ACTIVITIES- SECOND



RESISTO

D10.11 – EXPLOITATION ACTIVITIES – SECOND

Document Manager:	Federico FROSALI	LDO	Editor
--------------------------	------------------	-----	--------

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

Document ID N°:	RESISTO_D10.11_190723_02	Version:	2.0
Deliverable:	D10.11	Date:	23/07/2019
		Status:	APPROVED

Document classification	Public
--------------------------------	---------------

Approval Status	
Prepared by:	Federico FROSALI (LDO)
Approved by: (WP Leader)	Federico FROSALI (LDO)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	NA
Security Approval (Security Advisory Board Leader)	NA

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Federico FROSALI	LDO	Editor
Maria BELESIOTI	OTE	Contributor
Tuuli LOHMUS	GT	Contributor
Rodoula MAKRI	ICCS	Contributor
Mirjam FEHLING-KASCHEK	Fraunhofer	Contributor
Sylvia BACH	BUW	Contributor
Jorge CARAPINHA	ALB	Contributor

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
0.9	01/06/2019	All	All	Final draft
1.0	11/06/2019	All	All	Final release
2.0	23/07/2019	All	All	Figures improved according to 1st year review remarks

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 RESISSO 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 2 – Genova (GE) – 16154 – Italy
Tel.: +39 348 6505565
E-Mail: 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

Market strategy and Draft Business plan based latest available data for the Critical Infrastructure protection market; Exploitation strategy and Innovation strategy update; IP protection plan

CONTENTS

ABBREVIATIONS	8
1. INTRODUCTION.....	10
2. SECURITY MARKET ANALYSIS.....	11
2.1 Business External Environment	11
2.2 Security Market value	15
2.3 Competitive Landscape (Security Domain).....	19
3. RESISTO BUSINESS PLANNING.....	20
3.1 Market analysis/ Economic outlook for the CI protection/resilience.....	21
3.2 Market analysis and competitive landscape	24
3.3 RESISTO Business Model	26
3.4 RESISTO Go-to-market strategy and Value Proposition	27
4. Exploitation Plan Update	29
5. Innovation Management - update	31
5.1. Elements of innovation in RESISTO Project	31
5.2 Holistic Syst. Modelling and interdependency simulation analysis for Risk Predictor	31
5.3 Blockchain for Data integrity.....	31
6. IP Management Plan	33
6.1 IPR management process	35
6.2 Joint Ownership of Results.....	36
6.3 Access and management of IPR form	36
7. REFERENCES.....	37

INDEX OF FIGURES

Figure 1 PESTE Matrix of Selected Factors of Change	12
Figure 2 Global Trends	13
Figure 3 Security Market Value – split by domain	16
Figure 4 Security Market Value – split by geographic areas	17
Figure 5 Total Market Value (CIP segment details)	18
Figure 6 Competitive Landscape	19
Figure 7 Connections and Interdependencies across Cis and Economic sectors	20
Figure 8 Market Drivers and KSFs	21
Figure 9 Global CIP market size and growth rate, 2016-2023 (USD billion) (Y-o-Y %)	22
Figure 10 Critical Infrastructure Protection Market Size, By Security Technology Snapshot 2018 & 2023: Network Security Segment Is Expected To Grow At The Highest CAGR During The Forecast Period.....	23
Figure 11 CIP market size, by service snapshot (2018 & 2023).....	23
Figure 12 CIP market size, regional snapshot.....	24
Figure 13 Communications systems market size, by region, 2018-2023 (USD million).....	25
Figure 14 Communication systems market size, by technology, 2018-2023 (USD million).....	26
Figure 15 IP management plan	33
Figure 16 IPR management process	35

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone systems
API	Application Programming Interface
APN	Access Point Name
ASIC	Application Specific Integrated Circuit
B2B	Back-to-Back gateway
CCA	Critical Communication Application
CCS	Critical Communications System
DMO	Direct Mode Operations
ETSI	European Telecommunications Standard Institute
EU	European Union
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile communications
GSSI	Group Short Subscriber Identity
HW	HardWare
ISI	Inter System Interface
ISSI	Individual Short Subscriber Identity
ISITEP	Inter System Interfaces for TETRA-TETRAPOL Networks
ITSI	Individual TETRA subscriber Identity
LTE	Long Term Evolution (= 4G)
MNO	Mobile Network Operator
PC	Personal Computer
PPDR	Public Protection and Disaster Relief
PTT	Push To Talk
QoS	Quality of Service
SW	SoftWare
TCCE	TETRA and Critical Communications Evolution
TEA2	TETRA Encryption Algorithm #2
TETRA	TErrestrial Trunked RAdio

TG	Talk Group
TMO	Trunked Mode Operations
UE	User Equipment
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION

This deliverable addresses the following topics

- **Market analysis:** The overall market value for security solutions is introduced, with an analysis of mayr influencing factors (PESTE analysis) and technology trends. The value for CI protection market is estimated as part of the total market potential market for security solutions
- **Draft Business plan:** based latest available market data for the Critical Infrastructure protection, the refinement of RESISTO framework after the first design stages and preliminary business models introduced in D10.10 the first elements of the business plan are drafted taking into account how RESISTO can create and deliver value by identifying: (a) the relevant customers segments; (b) the value proposition; (c) the channels to deliver the value proposition to customers; (d) the activities to be performed and (e) the required partnership. The elements above will be used in phase 2 and linked to revenue and costs streams to quantify the business plan.
- **Exploitation strategy update** where individual exploitation activities are reviewed in light of first year project results and envisioned business opportunities.
- **Innovation strategy update** in order to keep up with technology innovation and market demand evolution focused first year project results and preliminary benchmarking of the surrounding market solutions that RESISTO will have to confront.
- **IP protection Plan:** The IPR plan for the RESISTO encompassing a list of the IP protection actions to be performed during the project to ensure maximization of the IP potential of the project, respect of IPR and a proper balance between the need for protection and the need for dissemination or results.

2. SECURITY MARKET ANALYSIS

In the following chapters the a market analysis is reviewed and updated in the light of the evolution of the context and of latest available market data, and the refinement of RESISTO framework after the first design stages.

Starting from a review of the external environment influencing the market of Security solutions, the main trends of the security market are identified. Then a focus on the Critical Infrastructure (CI) protection market, as part of the larger Security market, is presented, and the market size for RESISTO platform and the solutions developed in the project is defined, characterized and segmented. Then value chains serving each technology are briefly introduced.

2.1 Business External Environment

The following matrix illustrates the main drivers in the external environment influencing the security market from the Political, Economic, Societal/Security, Technology and Environment standpoint (PESTE Matrix) outlining selected factors of change.

<p><u>POLITICS</u></p> <p>The new US National Defense Strategy directs investments in space, cyber-space, nuclear forces, missile defense, autonomous systems, and better logistics. New opportunities?</p> <p>Will Mr. Trump be impeached?</p> <p>Will the US foreign policy (US embassy shift in Jerusalem, Iranian nuclear agreement at risk, NAFTA negotiations) increase instability globally?</p> <p>Will the US vs North Korea confrontation worsen?</p> <p>Will Mr Putin's international influence strengthen after 2018 Russian elections?</p> <p>Will the NATO budget for procurement actually increase?</p> <p>Are we going toward a hard Brexit?</p> <p>Is there still a chance to reverse Brexit?</p> <p>With a new Merkel government and a strong Macron in France, is a French-German led EU 27 in sight?</p> <p>Will the Italian elections impact on European stability?</p> <p>Will the Latin America electoral cycle stabilize this area?</p> <p>Will the Catalan independence go on and impact the EU?</p> <p>Is Saudi Arabia's power play actually changing the equilibrium in the Middle East?</p> <p>Is Turkey going East?</p>	<p><u>ECONOMY</u></p> <p>Will global growth momentum continue?</p> <p>Will the US economy sustain the above-trend growth?</p> <p>Will US – and possible global – protectionism mean less opportunities for European companies?</p> <p>Will a +2.4% growing EU economy offer solid industrial opportunities?</p> <p>Will the new EU Defense policy push for a single EU Defense market?</p> <p>Is China's economic slowdown affecting also the ASD sector?</p> <p>Will Modi revive Indian economy?</p> <p>Will the oil price increase fast?</p> <p>Will upward pressures on inflation be sustained?</p> <p>Will the \$/€, \$/£ exchange rate trends benefit European companies?</p> <p>Will the size and the global influence of emerging economies increase?</p>
<p><u>SOCIETAL/SECURITY</u></p> <p>Will the new US National Security Strategy offer opportunities especially in cyber-security?</p> <p>Will the renewed EU Internal Security Strategy (2015–2020) offer opportunities in border control and cyber-security?</p> <p>Will growing ransomware and data breaches in 2018 increasing detection and response spending?</p> <p>After ISIS has been defeated as a State, will the conflict shift in form of an insurgency?</p> <p>Will Islamic terrorism continue to hit Europe and the West?</p> <p>Will migration fluxes in Southern Mediterranean be kept under control via agreements with North African Countries?</p>	<p><u>TECHNOLOGY</u></p> <p>Will cyber-space become more regulated?</p> <p>Will wearables have a significant role in connected soldiers and other Defense applications?</p> <p>Will augmented/virtual reality transform training & simulation?</p> <p>Will visible light communications give rise to a brand new way of communicating and open up a new market?</p> <p>Will military and civilian Unmanned Fixed and Rotary Wing Aircraft modify the aeronautic market?</p> <p>Will the next-generation GPS impact the security field?</p> <p>Will meta-materials and nanotechnologies be applied more and more to radar improvements, selective frequencies antennas and sensors?</p> <p>Will directed-energy weapons and lasers become marketable?</p>
<p><u>ENVIRONMENT/COMMODITY</u></p> <p>Will tackling climate change be a real industrial opportunity over the next 2 decades for hi-tech companies?</p> <p>Will distributed electric propulsion be an enabler for new energy-efficient aircraft?</p> <p>Will creating a 'green' supply chain in ASD be a key success factor for prime contractors?</p> <p>Will a possible oil price increasing have a major environmental impact?</p>	

Figure 1 PESTE Matrix of Selected Factors of Change

The main global trends outlined in the PESTE analysis have direct impact on the market as outlined in the following matrix

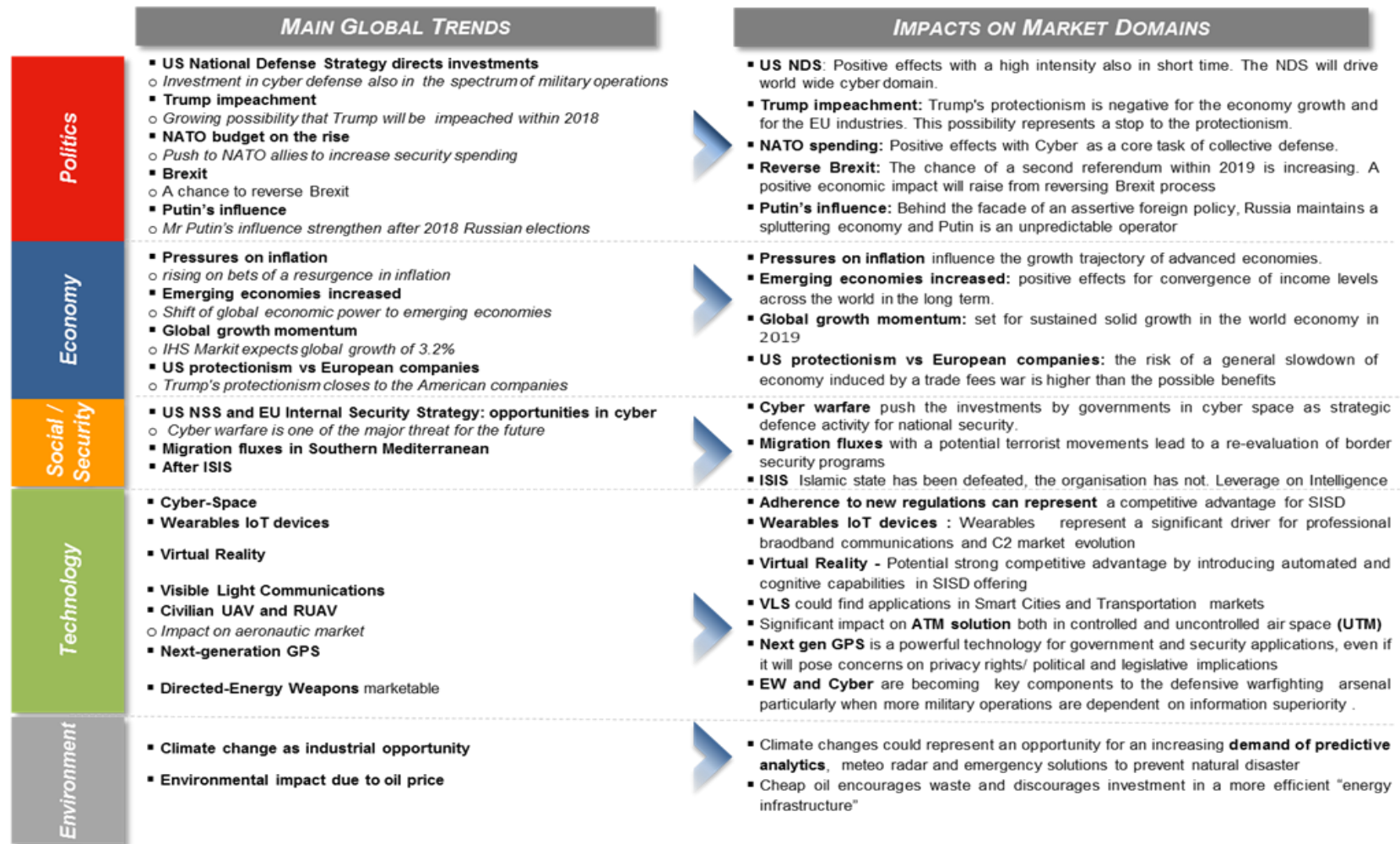


Figure 2 Global Trends

With specific reference to CI protection the following table outlines the main megatrends and technologies influencing the market, the inhibitors that has to be properly taken into account and the main perceived customer needs.

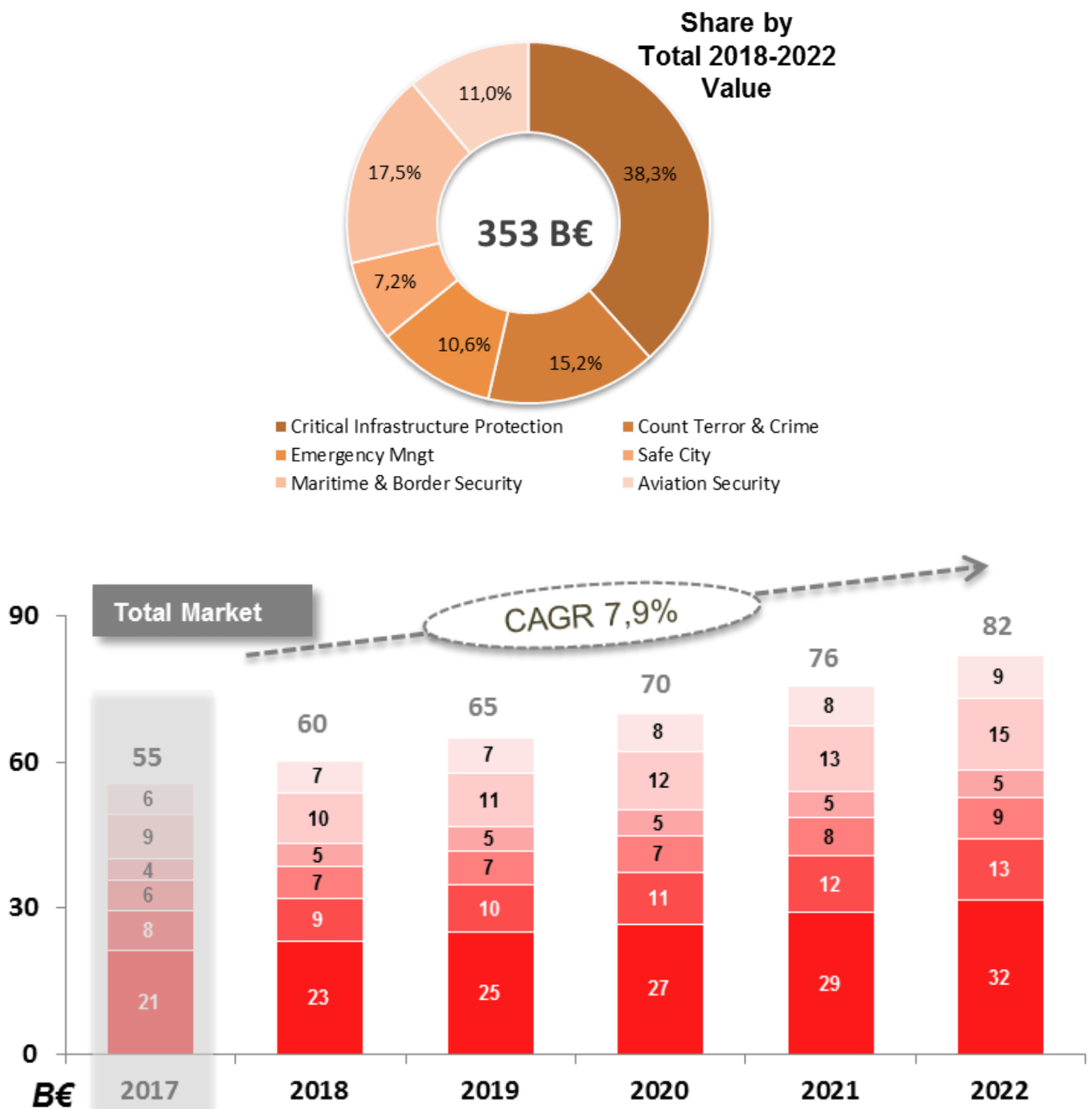
SECURITY / CI protection	
MEGA TRENDS	
<ul style="list-style-type: none"> ▶ Massive migrations ▶ Political tensions ▶ Terrorism (e.g DAESH attacks) ▶ Growth of cyber crime 	<ul style="list-style-type: none"> ▶ Climate Change ▶ Population growth ▶ Urbanization
TECHNOLOGY TRENDS	
<ul style="list-style-type: none"> ▶ "Walk through security" ▶ Cyber security & resilience ▶ Big Data & Analytics ▶ Cognitive Computing ▶ Mobile, IoT, M2M 	<ul style="list-style-type: none"> ▶ Cloud & Edge Computing ▶ Media sources variety, Social ▶ Biometric solutions ▶ Evolution towards LTE ▶ Wearable devices ▶ UAV
INHIBITORS	
<ul style="list-style-type: none"> ▶ Privacy rights/ Political and legislative Implications ▶ Cultural issues limit cross-agency info-sharing programs 	<ul style="list-style-type: none"> ▶ Uncertain return on investment
IMPACTS ON CUSTOMERS NEEDS	
<ul style="list-style-type: none"> ▶ Integration of structured and unstructured data ▶ Situational awareness and command and control ▶ Inter agency data sharing and collaboration 	<ul style="list-style-type: none"> ▶ Actionable intelligence ▶ Real-time decisions support and rapid response

2.2 Security Market value

Security Total market exhibits continuous growth up to 2022, over the five year period the CAGR is **7,9%**. Forecasts are probably **conservative** due to increasing level of terrorism threats (reports underlying the analysis were published before last wave of attacks).

CIP, Maritime & Border Security and Counter Terror & Crime are the dominant segments.

Across all Security Domain, **Cyber** is a critical issue with growing investments to implement higher security on a wider base of solutions and services.



CAGR 2018-22	Total
SECURITY	7,9%
Aviation Security	7,6%
Maritime & Border Security	9,2%
Safe City	3,3%
Emergency Mngt	7,0%
Count Terror & Crime	9,2%
Critical Infrastructure Protection	8,1%

Figure 3 Security Market Value – split by domain

- **CIP** is the largest segment both in terms of total and target market. In this segment, in the medium to long term we will see the convergence between physical and cyber security solutions.
- **Counter Terror & Crime** Total Market is characterized by the growing demand for C3I solutions; the target market is strongly linked to the availability of interoperable solutions (Hybrid Tetra / LTE platform) and references in the domestic market.
- **Emergency management** Total Market is growing also due to technologies not addressed by the SISD (geo spatial, ...), while the target market is conditioned by the availability of *ad-hoc* command and control solutions and broadband comms
- **Safe City** is a relatively new market, rapidly growing as cities are just beyond deploying video surveillance infrastructure; target market is very low mainly due to lack of references, but it could offer good opportunities conditioned to the SISD availability of complete situational awareness solutions, leveraging analytics and more advanced security concepts
- **Maritime & Border** Total Market is driven by the request for border mgmt solutions, while the target market suffers from the lack of recent references and f leading edge solutions (e.g. VTS solutions)
- **Airport Security** Total Market is driven by the growing demand for monitoring, detection, and prevention of threats; the target market is conditioned by the availability of vertical solutions for this segment, new advanced ABC systems and effective marketing actions.

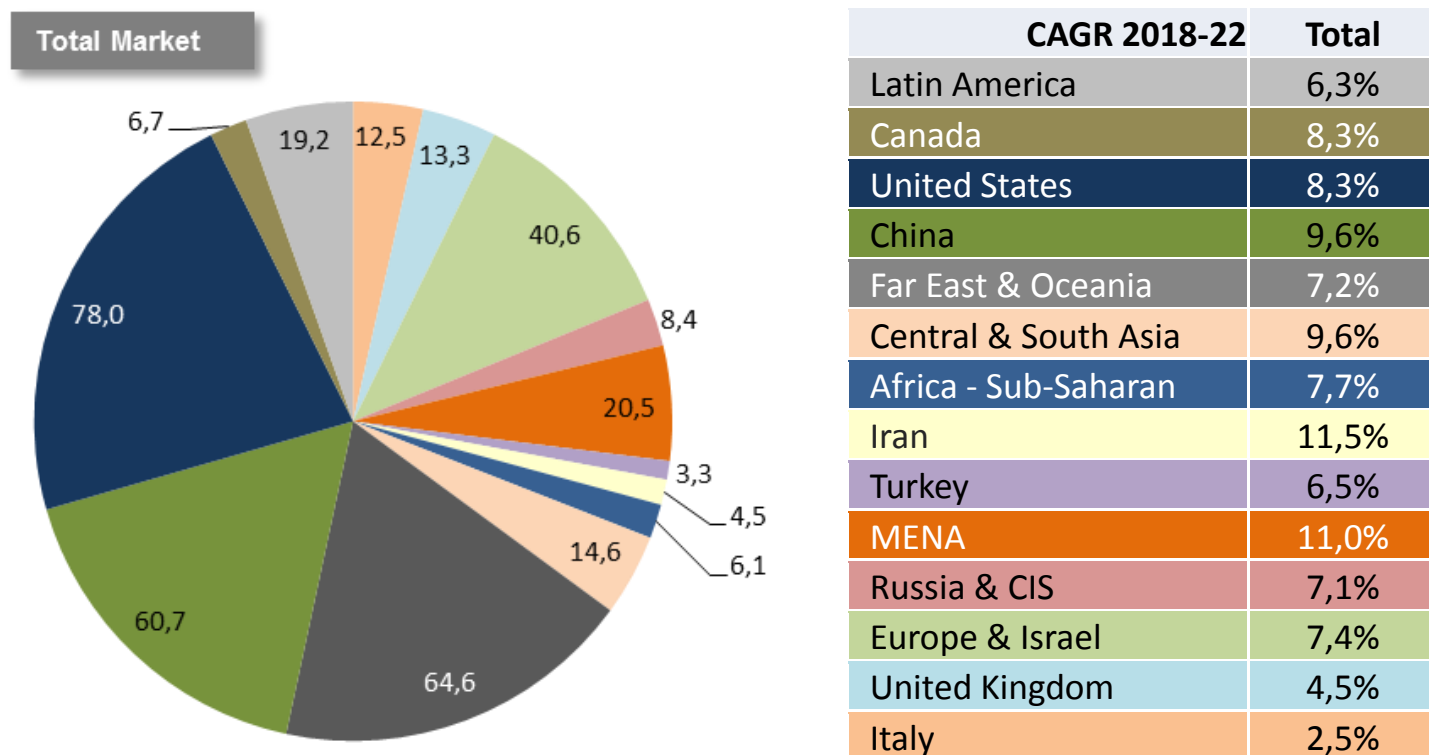
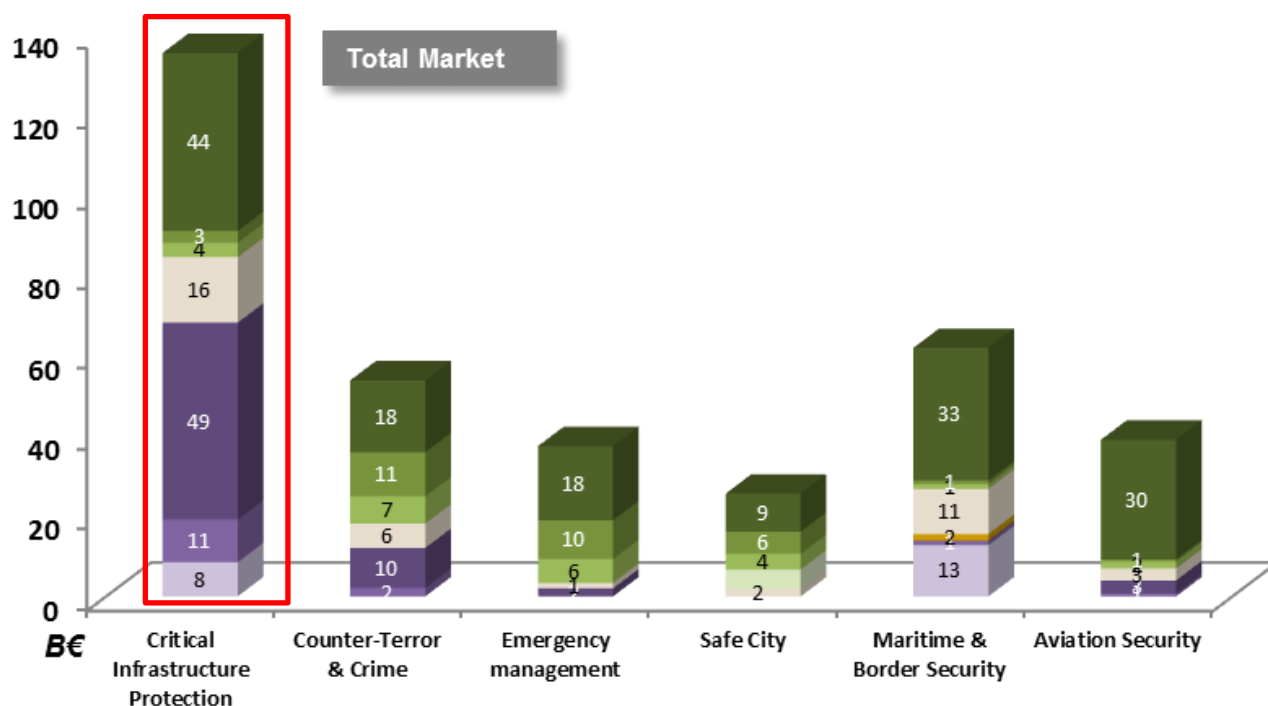


Figure 4 Security Market Value – split by geographic areas



CAGR 2018-22	Total
Critical Information System	8,0%
Intelligence	13,8%
Cyber Security	12,8%
VTS / Coastal and Ports Surv Sol.	9,8%
Services for HSCI	9,5%
Transportation Technologies & Solutions	2,2%
Professional Comms	7,4%
Control Rooms	7,0%
Integrated Security Solutions (including sensors)	5,5%

Figure 5 Total Market Value (CIP segment details)

- **Integrated Solutions** represent the largest share of the market and are addressed by system integrators who leverage proprietary products; Lacking proprietary products, SISD must operate as an integrator of third parties' systems and components.
- **The Control Room** Total Market is driven by technology integration and system interoperability, increasing value placed on "big data" and analytics, and C2 consolidation; Target mkt growth is linked to the availability of customizations addressing end users' SOPs.
- **PMR** Total Market is driven by digital LMR and, in the long term, by broadband networks, with a growing seamlessly interoperable networks' demand; Target market is mainly focused on PSS and Industrial Utility sectors.
- **Transportation Technologies & Solutions** market is projected to grow due to an increasing demand for advanced vehicle-related IT systems, secure comms, automated fleet management, cloud-based data analytics and autonomous vehicle technologies.
- The port management & information systems segment is estimated to lead the **VTS market**, with an increasing focus on e-navigation, multi-sensor trackers and routing monitoring sensors (especially in brown field installations).
- **Cyber security & Intelligence** Market will continue to grow focusing on diagnostics, mitigation and prediction, threat intelligence and the protection of critical infrastructures; target market can be further extended leveraging on deep learning and AI technologies and also expanded across LDO domains building security from the onset of new projects instead of adding it afterwards.
- **Critical Information System** market is driven by the growing digitalization; target market can be widened capitalizing CS&IS capabilities such as Big Data & Analytics, DevOps in the other LoBs/Divisions' offering.

2.3 Competitive Landscape (Security Domain)

The following picture provides a list of main competitors in the Security market split by technological/offering domain.

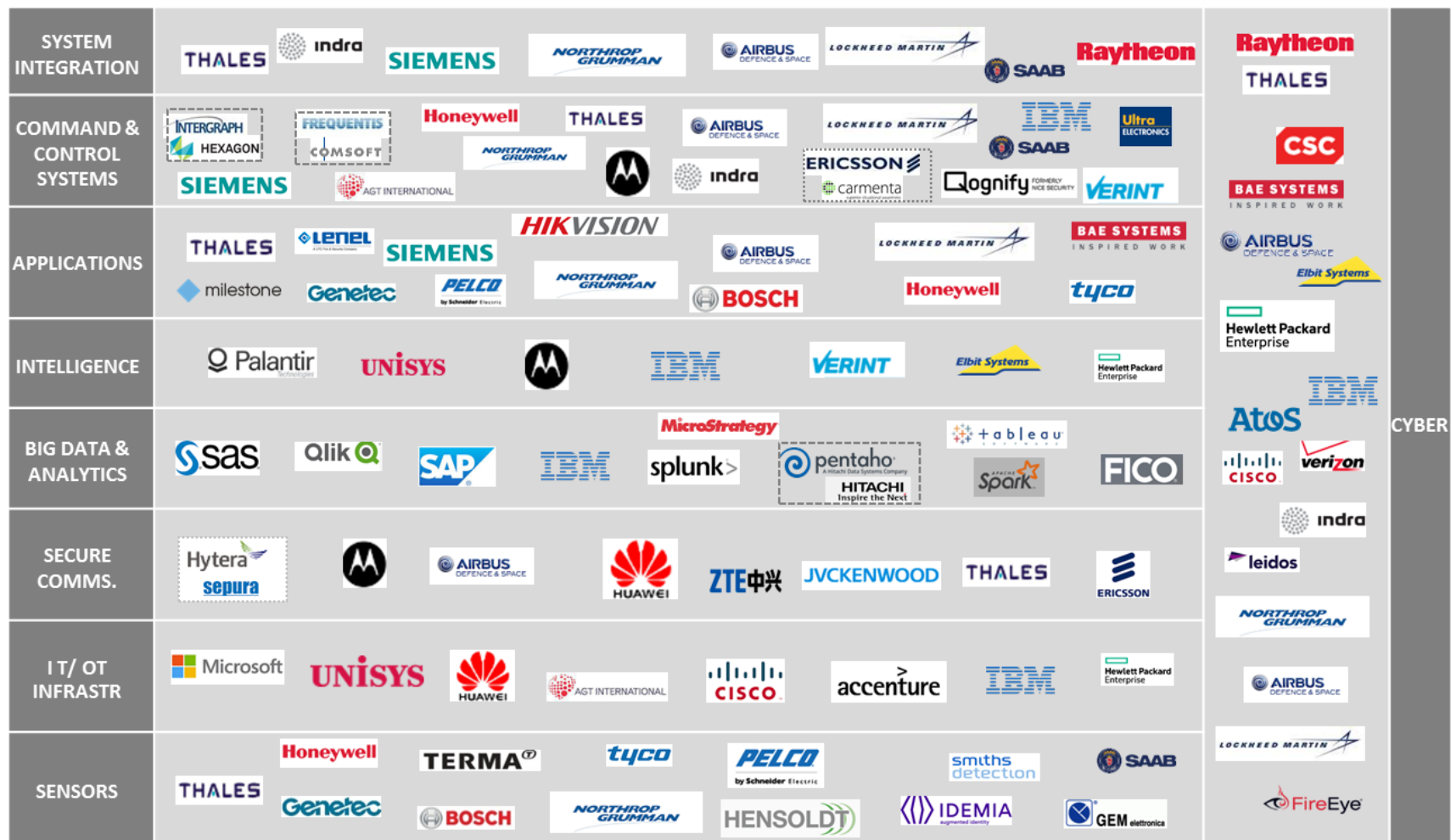


Figure 6 Competitive Landscape

3. RESISTO BUSINESS PLANNING

RESISTO is an innovative solution for Communication Infrastructure providing holistic (cyber/physical) situation awareness and enhanced resilience. RESISTO is intended to support Communications Infrastructures Operators to take the best countermeasures and reactive actions exploiting the combined use of risk and resilience preparatory analyses, detection and reaction technologies, applications and processes in the physical and cyber domains.

Communication infrastructure and networks will evolve and interoperate at a rapid pace to support the next generation of services, increased volume of network traffic, and emerging technologies. Thus, it would be imperative to examine how these future networks could survive under different crisis scenarios that will drive future patterns in usage, service provisioning, technology development, network architecture, and security¹. ISPs and telecom operators will continue to update their infrastructure to support heightened network demand so that they may remain competitive as a wider array of services will be available in different markets.

The telecom managed security services market is expected to grow from USD 17.02 Billion in 2016 to USD 33.68 Billion by 2021, at a CAGR of 14.6% not mentioning the new era to be widely open through the IoT Security Market².

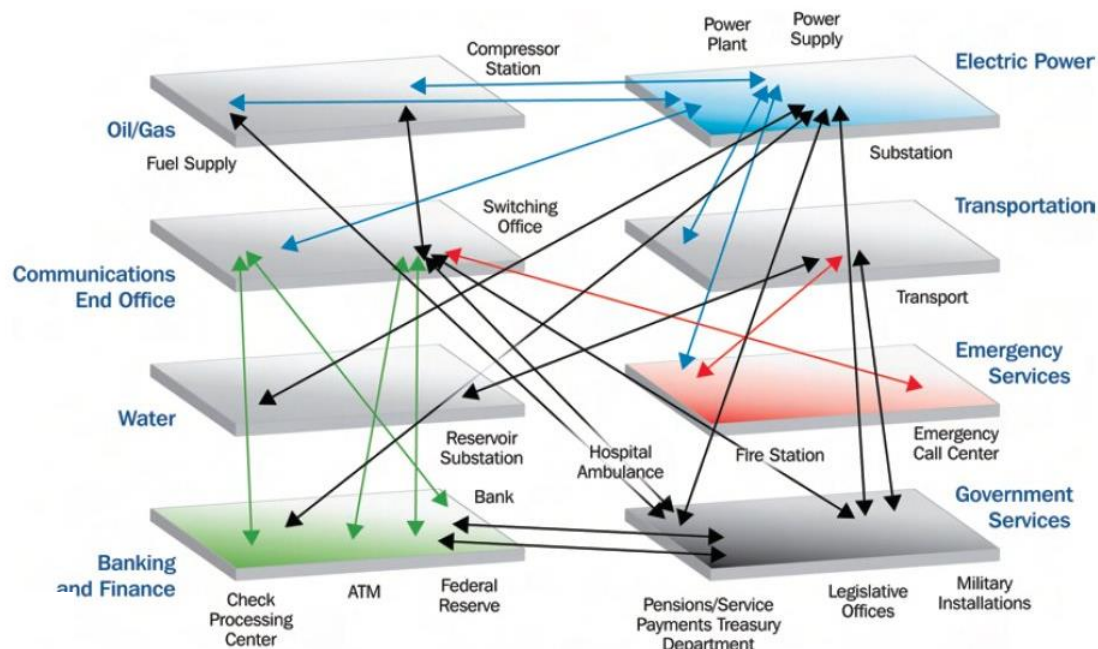


FIGURE 3.1 Connections and interdependencies across the economy. Schematic showing the interconnected infrastructures itative dependencies and interdependencies. SOURCE: Department of Homeland Security, National Infrastructure Protection Plan, available at http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

Figure 7 Connections and Interdependencies across Cis and Economic sectors

¹ "NSTAC Report to the President on Communications Resiliency", The President's National Security Telecommunications Advisory Committee, USA Communications Resiliency Task Force Report, 2011.
² <http://www.marketsandmarkets.com/Market-Reports/managed-security-services-market-5918403.html>

On the other hand, it is difficult to gauge the full extent of the impacts in market terms that a physical-cyber event could have on modern civilization due to the intricate interrelations of every aspect of modern global economics and infrastructure. As illustrated in the picture above, the impacts on one CI alone would have a variety of wide-ranging, impossible to forecast consequences, to the other verticals. One of the big trends predicted in 2016 is a rise in critical infrastructure attacks, as 68% of CI organizations experienced security incident in the past two years³. Additionally, compliance requirements for data security are stimulating the organizations to outsource the data security tasks. However, reluctance to share sensitive data and the growing awareness and concerns about data breaches are the major challenges for the market that would create the opportunities for more holistic approaches like the RESISTO one.

3.1 Market analysis/ Economic outlook for the CI protection/resilience

The market addressed by RESISTO falls within the wide definition of Critical Infrastructure protection being communication infrastructure a CI by itself but also a key asset for all other CIs.

The CI protection market is mainly driven by the need for:

- 1) Increased Situational awareness and response capabilities
- 2) Ability to defence from physical and logical (and combination of) attacks
- 3) Operational efficiency and price flexibility

The main Key Success Factors for the market are:

- a) Unified security platform for a complete security picture and incident response management
- b) Integrated security governance solutions
- c) Control room technology, use of managed security services and integration with legacy systems

The RESISTO solution has been conceived and designed to addresses all the above mentioned drivers



Figure 8 Market Drivers and KSFs

By security technologies types, the CIP market is broadly segmented as Network Security, Physical Security, Secure Communication, RADARS, CBRNE, Vehicle Identification Management, SCADA security

³ <http://www.crn.com/slide-shows/security/300080454/10-companies-getting-into-the-critical-infrastructure-security-market.htm>

RADARS technology contributes most to the growth in critical infrastructure protection market in safety and security. RADARS has laid itself in ground surveillance radar system, it has been so designed to sense targets moving towards the surveillance zone on the ground. If any object is moving or not, the radar detects new entities that pass in the area by releasing the radar signals off of the objects. It has surveillance cameras to have closer identification of the risk. Security personnel attached with RADAR takes the next steps for preventing any disturbance to secure the area. In network security, there is layered protection in a computer network infrastructure in order to provide security and safety at each phases of networking and prohibits unauthorized access.

Physical security is the protection of hardware, programs, personnel, and data from physical conditions vulnerable to some actions and events such as fire, natural disasters, burglary, theft, vandalism, and terrorism that could result in serious fatalities or damage to an institution, enterprise, or agency. In CBRNE agents such as chemical, biological, radiological, nuclear, and explosives can be identified under CBRNE detection technologies. These detection systems generally include trace detection, vapor sampling, and other threat detection technologies. The Vehicle Identification Management (VIM) tracks and identifies threats with accuracy in a faster way. Its powerful analysis features helps take immediate decisions regarding risk flexibly. Secured communication enables safe communication and quick deployment of the response teams to the effected site. The term SCADA refers to centralized systems that monitor and regulates the sites and systems spread across large areas. Building Management System (BMS) is automated computer-based control system installed to control and monitor the building's mechanical and electrical equipment such as lighting, ventilation, security, and fire systems.

By verticals, the energy and transportation sectors suffer increasing levels of dependence on the information communication technologies or the information infrastructure. CIP other than energy and transportation verticals have a wide portfolio of applications across telecommunications, manufacturing and chemical industry, sensitive infrastructures such as stadiums, government facilities, manufacturing, banking facilities, historical monuments, holy places, and defense establishments. Currently, sensitive infrastructures and chemical and manufacturing verticals, are the high focus areas and need to be improved. The innovation and growth is already seen in this vertical. There are implementations of security across segments such as government monuments, dams, power reactors, manufacturing & automation, banking & **telecommunication**, and public safety & emergency response for better security and protection of the assets.

On the basis of service, the CIP market is segmented into risk management services, consulting services, managed services, maintenance and support

The global CIP market is expected to grow from USD 102.47 billion in 2018 to USD 144.82 billion by 2023, at a CAGR of 7.16% from 2018 to 2023.

Particular	2016	2017	2018	2023	CAGR (2018-2023)
Critical Infrastructure Protection Market	87.97	95.03	102.47	144.82	7.16%
Y-O-Y		8.03%	7.82%	6.74%	

Figure 9 Global CIP market size and growth rate, 2016-2023 (USD billion) (Y-o-Y %)

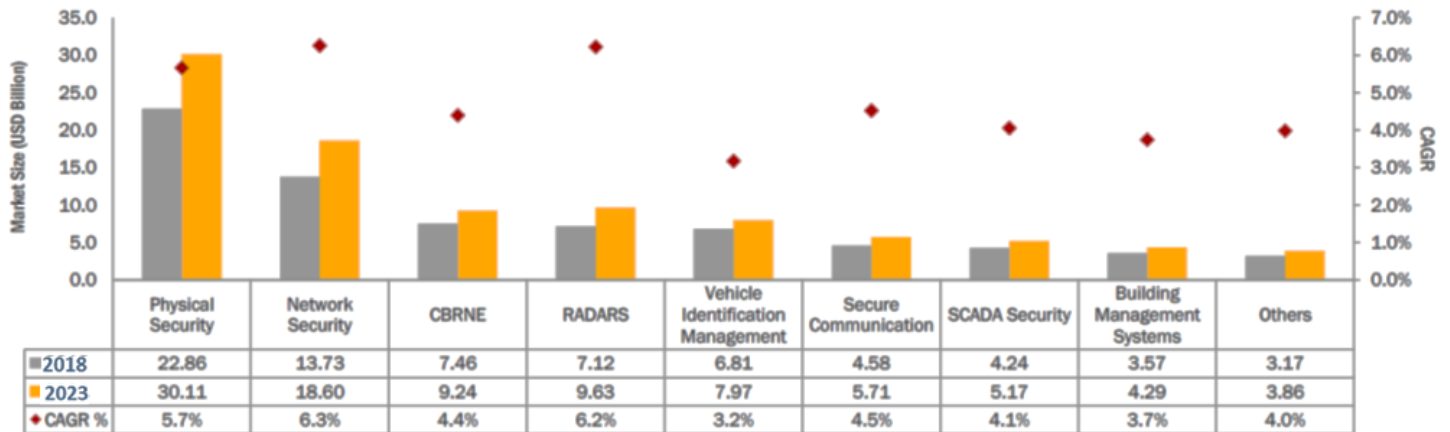


Figure 10 Critical Infrastructure Protection Market Size, By Security Technology Snapshot 2018 & 2023: Network Security Segment Is Expected To Grow At The Highest CAGR During The Forecast Period

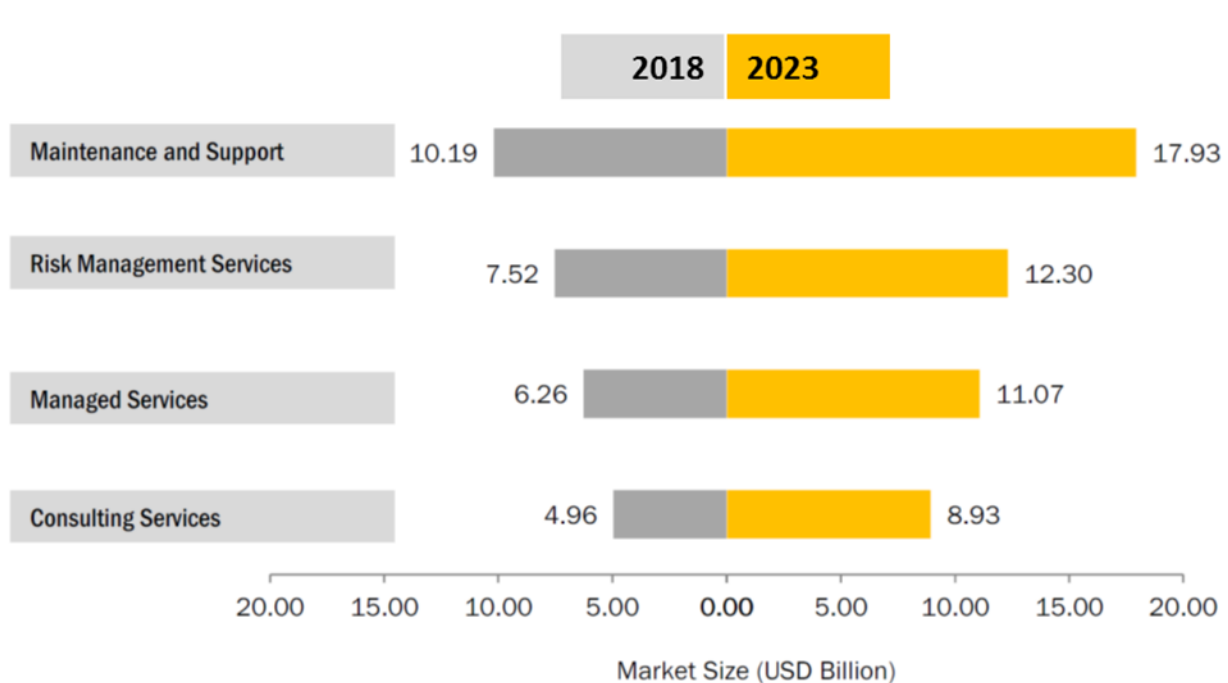


Figure 11 CIP market size, by service snapshot (2018 & 2023)

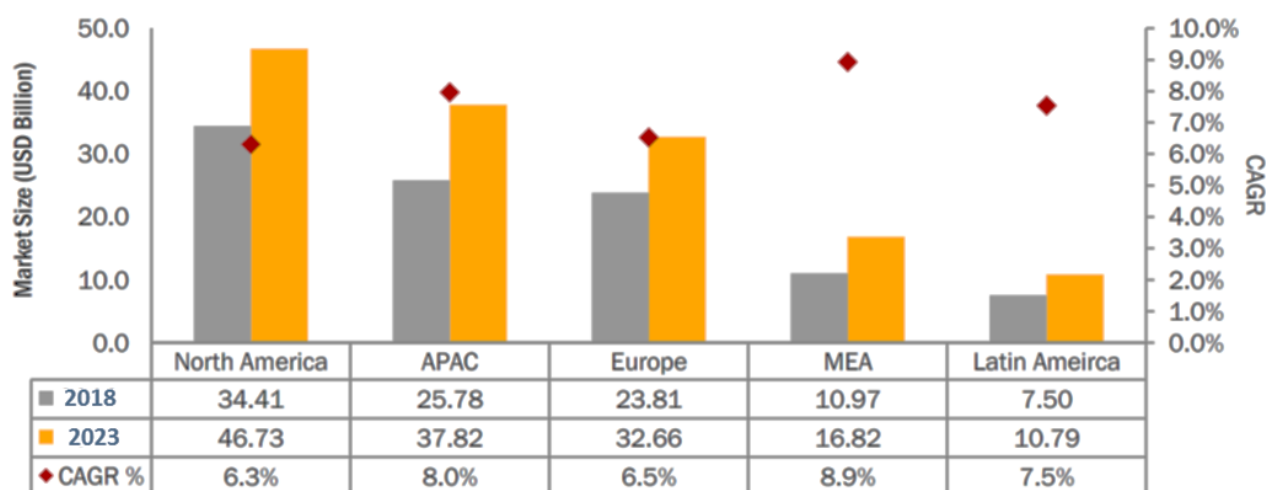


Figure 12 CIP market size, regional snapshot

The global CIP market exhibits a profitable growth potential for the next five years. In the past, the systems and networks of the infrastructure elements were logically and physically independent. They had little interaction or connection with each other or other sectors of the infrastructure. With advancement in technology, the structures within each division became automated, and interlinked through computers and infrastructures facilities. As a result, the flow of oil, gas, electricity, and telecommunications throughout the country are linked, which may affect traditional security borders.

One issue confronted by examination on critical infrastructure is the compelling scope of scales at which security issues may emerge. The progress of this market is driven by the increasing number of cyber threats, which have devastating impact on mission critical industries such as oil and gas, airports infrastructure, railway infrastructure, energy and utilities, and others. Other verticals include nuclear power plants, seaports, highways and bridges, BFSI, government facilities and defense establishments, communication systems, chemicals and manufacturing, stadiums, holy places and public places, and others. All critical infrastructures are nowadays highly dependent on telecommunications such as public telephone network, the internet, or it may be wired or wireless networks. So, it is proven that the market is doing a huge investment on IT and smart grid technology, which is driving the growth in the CIP market. This in turn has invited various collaborations & partnerships, mergers & acquisitions, by major players in order to provide customers with integrated CIP solutions and services. The high growth potential in emerging markets such as MEA and APAC makes this market more competitive

3.2 Market analysis and competitive landscape

The CIP market incorporates a myriad of solutions designed to manage numerous critical infrastructures and offers access to the right resources at the right time. This helps businesses in better management of resources and improving overall business value. The CIP market is diversified and competitive with a large number of market players including mid-tier companies and start-up firms. However, the bigger firms in the market are increasingly acquiring small players in an attempt to expand their offerings across the globe. Companies across industry verticals are looking for easy to

integrate and easy to configure CIP solutions to secure the critical business infrastructure. They are looking for rapid Return on Investment (RoI) with proven path to deliver the value.

The CIP market is consumer driven and major end-users are Small and Medium Businesses (SMBs) and large enterprises. Large enterprises dominate the CIP market share in comparison with SMBs and will continue to do so in the years to come. The bargaining power of suppliers is moderate, while that of the buyers is also moderate due to high supplier concentration. Systems for monitoring security actions must be planned, and administrations must have complete possibility plans for natural disasters, cyber-attacks, and other unplanned events.:

The value chain and ecosystem of the CIP market shows different combinations on how different vendors, service providers integrate with each other to deliver unique security solutions/services to the end-user. Companies independently offer physical and network security solutions such as protection from Distributed Denial of Service (DDoS), antivirus/malware, Unified Threat Management (UTM), data protection solutions, radars, video surveillance, secure communications, and access control systems.

Solutions providers such as Accenture, IBM, McAfee, CNL Software, Cassidian, and Fidelis Security Solutions offer network related security whereas companies such as Honeywell, Cisco, Terma, Thales Group, BAE Systems, General Electric, and Nice systems are a few key market players in providing physical security.

The CIP ecosystem also comprises vendors who provide consulting and integration services. These enterprises provide advanced designing, implementation, maintenance, operational, and lifecycle management services to the government, and critical infrastructure owners. Companies such as Cisco, IBM, Accenture, Motorola Solutions, and Nice Systems offer a comprehensive portfolio of high performance services and applications that are robust and cost-effective in critical work environments

Communication systems are a collation of communication networks, transmission systems, and relay stations. Hence, the need to secure communications using crypto security, transmission security, emission security, and physical security of the equipment is required to protect classified traffic on the networks. Spam was initially used to send unsolicited commercial messages; they now also serve to spread worms, viruses, and other malicious code that harmfully impact the security and stability of the global telecommunication network. It is a global problem that needs a multifaceted and comprehensive approach.

Region	2018	2023	CAGR (2018-2023)
North America	2,115.6	2,899.1	6.5%
Europe	1,463.8	2,026.2	6.7%
APAC	1,585.2	2,346.3	8.2%
MEA	674.4	1,043.7	9.1%
Latin America	461.3	669.5	7.7%
Total	6,300.4	8,984.7	7.4%

Note: e-Estimated, p-Projected

Figure 13 Communications systems market size, by region, 2018-2023 (USD million)

Technology	2018	2023	CAGR (2018-2023)
Network Security	844.3	1,153.8	6.4%
Physical Security	1,405.4	1,867.8	5.9%
RADARS	438.1	597.7	6.4%
CBRNE	458.4	573.5	4.6%
Vehicle Identification Management	419.0	494.2	3.4%
Secure Communication	281.4	354.2	4.7%
SCADA Security	260.6	320.8	4.2%
Building Management Systems	219.5	266.2	3.9%
Others	195.2	239.4	4.2%
Total	4,521.9	5,867.7	5.3%

Figure 14 Communication systems market size, by technology, 2018-2023 (USD million)

The table given above highlights the communication systems market size by technology. The physical security technology is estimated to grow from USD 1,405.4 million in 2016 and is projected to reach USD 1,867.8 million by 2021, growing at a CAGR of 5.9%. The network security and RADARS technologies are expected to have the highest CAGR of 6.4% during the forecast period from 2016 to 2021.

3.3 RESISTO Business Model

As already outlined in D10.10

Candidate RESISTO Business Models are here introduced to guarantee the medium and long-term economic sustainability of the product/service offering.

RESISTO is an innovative solution for Communication Infrastructure providing holistic (cyber/physical) situation awareness and enhanced resilience. RESISTO is intended to support Communications Infrastructures Operators to take the best countermeasures and reactive actions exploiting the combined use of risk and resilience preparatory analyses, detection and reaction technologies, applications and processes in the physical and cyber domains. Based on this proposition **RESISTO business model** must address different kind of customer segments: B2B (Business to Business): mainly Telco/Communication Operators but also other CI operators (managed security services); B2G (Business to Government) since protection of CI sites involves also National Governments and local institutions; S2B (Science to Business) to take into account technology innovation transfer from research institutions to industries as the case for the universities and research centres in the consortium (RM3, EMI, ICCS).

The most appropriate business models for the RESISTO platform identified at this stage are:

- **The system integrator business model:** Under this kind of model Large Enterprises like LDO and TEI, can provide RESISTO platform as a scalable solution/system customized on the end-user. This kind of model requires heavy investment in innovation, effective partnership with innovative technology providers and RTOs/universities, reputation in the field of CI protection and customer intimacy. The profit of this kind of model is high for high end (complex) solutions

over large systems. This model represents a clear opportunity for technology providers (like GT, INT, TEI) and capability providers (RM3, ICCS, ADI, BSS) under the condition of being able to keep up with the competition

- **The security as a service business model.** Telco operators already provide managed security services to their customers. RESISTO platform may be adopted by Telco operators (like TIM, BT, OTE ORO, RTV) to extend or reinforce their offering targeting their CI customers and largely leveraging on their customer intimacy. Large Enterprises with expertise in managed services like TEI, and CI protection may embrace this business model as well.
- **The service oriented business model.** This kind of business model includes consultancy service, design service, supervision service, training service, maintenance service. It is expected that consultancy, design and training services will be sold as part of the solution (to this regard the Cisia Pro tool and the modelling approach from EMI can be very powerful) while supervision and maintenance services can be sold long after the delivery of the system. The profit of this kind of business model is higher in % compared to the previous model due to reduced investment required (mainly opex cost). The partner in the best position to exploit this business model are the Large Enterprises with expertise in the field of CI protection security management, like LDO; and managed security services providers like the telco operators (TIM, BT, OTE ORO, RTV) and TEI.

3.4 RESISTO Go-to-market strategy and Value Proposition

Go-to-market strategy - Major drivers for selling the RESISTO platform to the market are

- the ability to improve detection reaction and mitigation capabilities of the communication operators in the short term
- In face of complex cyber-physical attacks the ability to improve decision making process, leading to a more efficient selection and use of countermeasure and mitigation
- The ability to increase infrastructure resilience in the medium/long term

The main obstacle to RESISTO adoption relies in the need to integrate data from many different domains (cyber and physical), typically managed by different department in the same organization, implying the need to review also company processes and responsibilities.

As soon as the RESISTO platform integration steps will be completed and the IPR aspects agreed, the RESISTO platform can be proposed to a number of telco operators and CI operators in EU also leveraging on AB members involvement. Our first estimation is that in the EU exist more than **300 relevant authorities and participants** in this field. Another important dimension is that RESISTO will be available, as said, as either a stand-alone configurable platform, to be embedded on an end user infrastructure, or as a service.

Value proposition - The RESISTO value proposition covers the following areas

Internal benefits	External benefits
<ul style="list-style-type: none"> • Cost savings, protecting Telco infrastructures from potential damages and service outages coming from either combined and independent cyber and physical threats; • Enhanced Resilience, reducing the risk of service interruption toward their customers during terrorist attack and/or stress over the infrastructure due to natural disasters • Increasing incentives for cyber security, adopting standard certification and being compliant with European regulation; 	<ul style="list-style-type: none"> • Maintaining competitive advantage for Telco operators; • Return on investment, selling security as service; • Increasing customer loyalty, selling not just the infrastructure but the security on that; • Extend Service offering building new relationship with suppliers and wider CI protection community

4. EXPLOITATION PLAN UPDATE

Hereafter we present an update on how the project beneficiaries will benefit from and exploit the solutions developed in RESISTO. As already introduced in D10.10 we expect that exploitation will be performed twofold: within the partners through the possibility to develop a joint proposition to the market, ideally at consortium level, promoting the RESISTO platform as a whole (or self-consistent parts of it), and at individual partner level, exploiting RESISTO as a way to market specific components, networking with partners and potential customers.

The following table reports highlighted in yellow the main changes.

P.	Individual Exploitation Plan (short description) for LEs/SMEs/RTOs
1. LDO	LDO exploitation plan aims at increasing its expertise in the field of Critical Infrastructure protection, at innovating its systems and at increasing its position on the national and international CI market establishing links with a number of potential customers. LDO business model looks at the exploitation of the RESISTO platform results to enhance its product portfolio (with specific reference to SC2 solution and Security Governance Portal for cyber security) and introduce innovation solutions in current systems.
2. RM3	Over the last years, RM3 research group has been appointed as consultant for CIP and CIIP activities by several industrial and governmental entities thus acquiring a valuable knowledge about mechanisms and architectures of actual CIs both at national and European level. RM3 will exploit RESISTO results and contacts with end-users to further develop its consultancy services in the field of CIP and risk management. At this stage RM3 also envisions the possibility to develop an industrial product based on CisiaPro, through the collaboration with Leonardo and other LES in the project
9. TEI	TEI is involved in developing Mobile Telecommunication infrastructure with a strong commitment on 5G evolution. RESISTO results in the field of security of telecom systems and of SDN and NFV in particular will be exploited in the development and extension of future TEI telecom infrastructure product portfolio. The Emergency Warning Communication Function validated in RESISTO will be exploited within the mission critical communication market. The collaboration with Leonardo is seen as a great opportunity to this aim.
11. EMI	EMI cooperates with leading industrial companies. The planning supporting and disaster management tools developed and adapted by EMI to the Communication CI domain will be exploited both to reinforce and extend cooperation with industrial companies in the field of CIP and to enhance its IP (Intellectual Property) knowledge portfolio.
12. ICCS	RESISTO will give ICCS the opportunity to improve its position in scientific fields of anomaly detection, radio networks, 5G, sensors and signal processing. ICCS will exploit project results by pursuing patents applications, creating new research links, establishing further research collaborations within national and European projects, participating in exhibitions and related events, exploiting its connections with the Hellenic Public/Private Security Sector and Regulatory Bodies. It will give the opportunity to employ skilled researchers and PhD students contributing to further high-tech jobs creation on cutting-edge research topics.
13. BUW	Project results will be included in the safety engineering curricula of the university, especially in the courses „Organization and Communication in Crisis Management“ and „Principles of Crisis Management“. It is assumed that the participation will strengthen the competencies of the institute in EU and international crisis management R&D.
14. CER	CER will evaluate potential adoption of RESISTO methodologies and approaches in order to promote them for certification and validation purposes inside its institutional activities.
15. INT	Through RESISTO, INT will have the opportunity to reinforce its leading position in the satellite spectrum monitoring market, offering commercial 5G network operations tools, also addressing new business models from being provider of complete packages towards offering of pluggable RF simulation and measurement components. The prototype of industrial IoT sensors validated in RESISTO will open to the company the appealing possibility of offering security solution for telecommunication physical sites protection improving also its professional consultancy services on the deployment of network system/applications.
16. GT	GT is the largest industrial blockchain platform provider, offering Keyless Signature Infrastructure (KSI) technology that enables massive scale data authentication without reliance on centralized trust authorities. GT is KSI technology provider to TEI and other telecommunication providers and partner in industrial blockchain commercialization. Through integrating KSI into the innovative RESISTO solutions, GT expects to get in touch with a number of new potential customers in the Telco sector and to promote its solution in the CI cyber protection market exploiting new commercialization opportunities.
17. ADI	ADI will exploit RESISTO results with reference to its solutions for video analysis and UAV detection with key stakeholders in Cypriot market and other areas where ADI operates (e.g. Balkans and Middle East): Cyprus Telecommunication Providers, in particular with Cyprus Telecommunications Authority (CYTA) with which ADI has a successful collaboration track; Office of Electronic Communications & Postal Regulations (OCECPR), ENISA national contact point of ENISA. ADI will promote RESISTO to the Cyprus Research Promotion Foundation, coordinator of the EEN Cyprus that is expected to offer collaboration and commercialization possibilities and potential joint ventures

19. BSS	BSS goal is to promote RESISTO platform to business customers that are operating Critical Infrastructures. BSS plans to use and engage its offensive, defensive and intelligence capabilities combining them with operations and innovative functionalities brought by integrating RESISTO ecosystem within its customers' CIs systems. In this way BSS will develop new services for customers until this point not accessible.
------------	--

Table 1 **Individual Exploitation Plan for RESISTO LEs/SMEs/RTOs**

P.	Individual Exploitations and/or Potential Adoption Plan (short description) for End Users
3. TIM	TIM, being an international infrastructure operator and TLC-ICT services provider, has interest in exploiting RESISTO results internally and in the market. RESISTO solutions will be included in its existing and future platforms, with the aim of enhancing their security with clear positive impact on its image. RESISTO adoption will also help TIM to comply with the Directive 2009/140 EC. TIM also will exploit RESISTO in the service offering in the 5G area (e.g. 5G for Italy), and extend its Managed security services portfolio
4. OTE	Telecom security managers are not only users of the threat detection system or even detectors themselves by being assisted by a possible visualization tool, but are also, and perhaps more importantly, human beings who need to take themselves decisions in terms of the best strategy for defending against a detected threat, cyber, physical or a combination of the two. RESISTO's core strategy for innovation and exploitation focuses on its design approach. The innovation activities developed in RESISTO will contribute to extend the OTE offering in telecommunications, specifically those services related security functions, both internally and externally. Through the combined use of advanced threat identification, detection, automated defence recommendation and finally mitigation RESISTO platform has the potential to offer improved situational awareness to telecom infrastructure providers and consequently to elevate the security level of the systems
5. BTC	BTC expects to incorporate the project results in evolved and extended versions of its unified Cyber Security Platform (CSP). CSP is used to implement its own cyber self-protection and as a basis for managed Cyber Security Operations Centre services for major public and private sector customers.
6. ORO	ORO will promote RESISTO platform as a service towards the business customers operating CIs such as utility (water, gas, energy) providers in line with ORO cyber security strategy and ORO cyber security solutions portfolio including the Security Operation Center (SOC) and security solutions for Industrial Control and Metering Systems. RESISTO innovative functionalities will be integrated in ORO SOC. ORO will also promote RESISTO at France Telecom group level
7. RTV	RTV will exploit RESISTO to set up a platform to protect its internal infrastructures and RTV's Maritime critical infrastructure to enhance its resilience. Moreover in full synergy with 5G City project RTV will exploit RESISTO results to secure the LTE-PPDR virtual slicing system to provide to the Mission Critical market the most secure and performant broadband connectivity service.
8. ALB	ALB will exploit RESISTO results by leveraging their products and services with a potential to be deployed in a 5G environment (e.g. OSS/BSS, access & transport network solutions), in scenarios related to cyber/physical security. In addition, RESISTO use cases to be developed by ALB will be incorporated in the Aveiro 5G experimentation facility, thus enriching the breadth of the 5G pilot and strengthening the competences of ALB in emerging technological domains, based on 5G and network virtualization.

Table 2 Individual Exploitation Plan and/or Potential Adoption Plan for End Users

5. INNOVATION MANAGEMENT - UPDATE

5.1. Elements of innovation in RESISTO Project

In the following paragraphs, we report the major updates compared to D10.10 analysis on key potential innovation elements characterising the RESISTO platform.

5.2 Holistic Syst. Modelling and interdependency simulation analysis for Risk Predictor

State Of The Art with respect to *performance degradation modelling and simulation*. The approach followed covers the time-dependent analysis of interdependencies of different system layers and level such as Physics, Cyber, Logic and Geographic, modelling infrastructure on an abstract level. The CISIApro simulator⁴ (Critical Infrastructure Simulation by Interdependent Agents) analyzes the effects of failure both in terms of faults propagation and with respect to performance degradation and effects of mitigation, in particular response and recovery. Currently such abstract models are not directly linked with models with higher resolution that allow to predictively assess the effect of natural and man-made physical but also cyber threats. Existing physical damage models or investigations for telecommunications subsystems cover, e.g., seismic⁵, heavy storm⁶, ice rain⁷ but also (terroristic) explosive loading⁸, impact⁹ and flooding. Possible effects of drones are known¹⁰, also shelling occurred in similar cases¹¹ but are respectively much less investigated. By now tools with drag and drop capability exist that allow for the assessment regarding, e.g. explosive and seismic threats. The CAESAR simulator analyses cascading effects in interconnected networks (e.g. water, power, communication) and provides resilience quantification methods for the evaluated networks..

Progress Beyond State Of The Art. RESISTO will use models and engineering-simulations to refine and develop telecommunication subsystem damage and resilience behaviour models sufficient for predictive assessment regarding critical risks as put forward by the sample cases, in particular out of the set (terroristic) explosions, effects of drones, impact, cyber induced effects, and seismic. It starts out with existing structural model inventories adding typical nodes and edges of Telecommunication CI, e.g. sending masts, ground stations, backbone-components.

5.3 Blockchain for Data integrity

State Of The Art *Traditional solution for data authentication which relies on centralized trust authorities (Public Key Infrastructures – PKI) suffer from problems of scalability and resilience (single point of failure). Furthermore, data integrity relies traditionally on the 'hardened box' concept where perimeter security keeps 'bad' actors out and 'good' actors in. Data transferability is facilitated by checksums and key-based digital signatures, which rely on trusted functions like key management, certification infrastructure and providing root of trust. Guardtime's KSI blockchain technology enables massive scale data authentication without reliance on centralized trust authorities. KSI ensure data integrity, traceability, provenance and auditability along all the data lifecycle (processing, formatting, logs etc.). All the data changing history and event integrity can be retrieved from the blockchain security solution and the data validity, time of change and signing entity is ensured in a way that third party validation independent from system can be used.*

⁴ <http://cisiapro.dia.uniroma3.it/>

⁵ K. K. Sharma, S.K. Duggal, D. K. Singh, A.K. Sachan, Civil Engineering and Urban Planning: An International Journal (CIVEJ) vol.2, no.3 (2015), pp. 13-31.

⁶ G. Ghodrati Amiri, Computers and Structures, vol. 80, no. 03, (2002), pp. 349-364, <http://www.sciencedirect.com/science/article/pii/S0045794901001754>

⁷ N.D. Mulherin, Cold Regions Science and Technology, vol. 27, no. 2 (1998), pp. 91-104, <http://www.sciencedirect.com/science/article/pii/S0165232X97000256>

⁸ Mark G. Stewart, Michael D. Netherton, David V. Rosowsky, Natural Hazards Review, vol. 7, no. 3 (2006), pp. 114-122, [http://ascelibrary.org/doi/abs/10.1061/\(ASCE\)1527-6988\(2006\)7:3\(114\)](http://ascelibrary.org/doi/abs/10.1061/(ASCE)1527-6988(2006)7:3(114))

⁹ C. U. Penalba, New Orleans Structures Congress (1999), <https://trid.trb.org/view.aspx?id=511641>

¹⁰ See e.g.: http://www.business-standard.com/article/news-ians/interpol-warns-of-drone-attacks-by-terrorists-on-critical-infrastructures-117021400178_1.html

¹¹ See e.g.: https://en.wikipedia.org/wiki/Metcalfe_sniper_attack

Progress Beyond State Of The Art: *RESISTO will integrate an innovative mature blockchain technology into its system which is provided by Guardtime. KSI is an industrial scale full stack blockchain infrastructure¹², the deployment of which offers a myriad of new security solutions¹³ and service revenue opportunities for telecom operators. It will enable the telecommunications providers in the RESISTO platform to guarantee the state of their network without relying on trusted administrators or the procedures that define the security of their network*

¹² Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees. Ahto Buldas, Andres Kroonmaa, Risto Laanoja, Hanne Riis Nielson, Dieter Gollmann. Secure IT Systems - 18th Nordic Conference, NordSec 2013, Proceedings. LNCS 8208, Springer, 2013.
¹³ Efficient Record-Level Keyless Signatures for Audit Logs. Ahto Buldas, Ahto Truu, Risto Laanoja, Rainer Gerhards, Karin Bernsmed, Simone Fischer-Hübner. Secure IT Systems - 19th Nordic Conference, NordSec 2014, Proceedings. LNCS 8788, Springer, 2014

6. IP MANAGEMENT PLAN

The IPR plan for the RESISTO project will be built step by step during the entire duration of the project mainly by gathering all IP process of partners regarding their own results in order to maximize IP potential of the project. However, to avoid as much as possible conflict and ensure the coherence of the dissemination and protection processes during the project, a global management has been set up. This management is based on:

- Global planning of the IP actions to perform during the project
- A management process to ensure the respect of IPR and the right balance between the need for protection of potential IP produced and the need for dissemination of results.
- A first overview (considered as confidential) of the potential contents qualifiable to IP and the expected IPR route chosen by the partners to protect their innovations.

The figure below describes the planning of the IP actions to perform during the project and the responsibility of each partner.

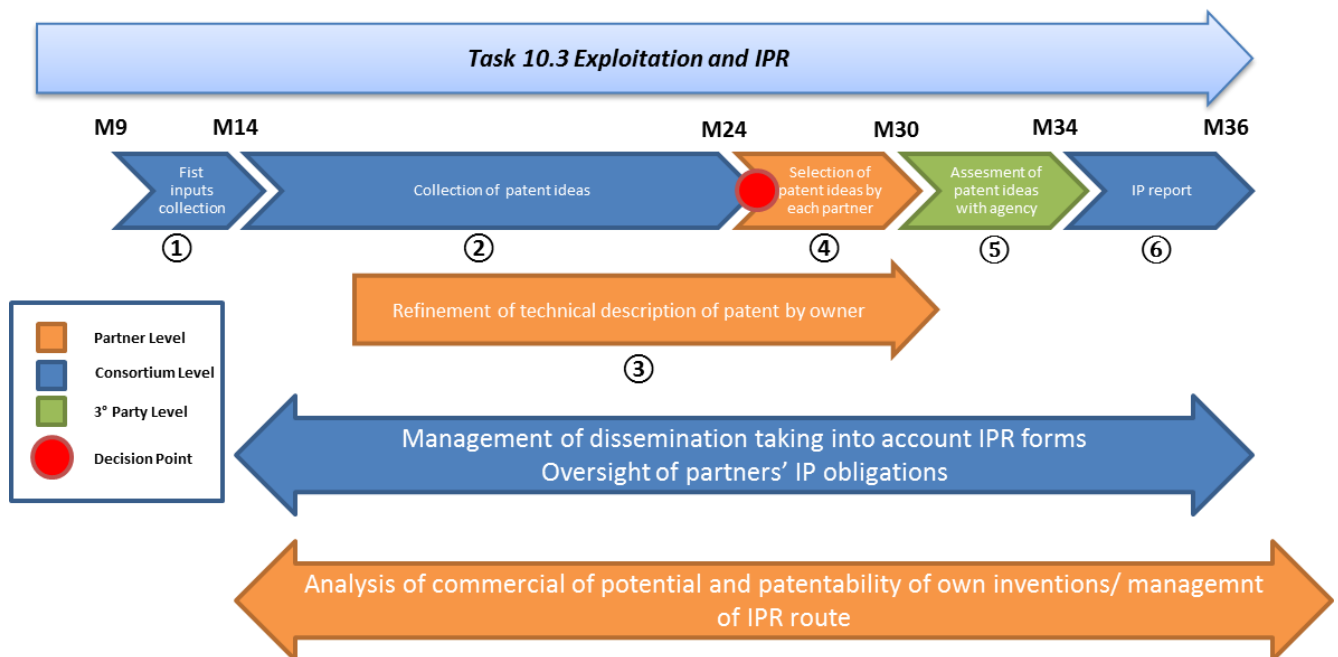


Figure 15 IP management plan

The planning can be described as following:

1. Gathering of first partners' inputs regarding the potential content qualifiable to IPR and relative IPR route.
2. Collections of patent ideas (IPR forms) during the entire duration of the project
3. Refinement of technical description of innovation regarding innovation qualifiable to patent, trademark, etc.
4. Selection by innovation owner of IP agencies to assess the patentability of innovation according to worldwide innovation and patent panorama

5. Assessment of partners' innovations by IP agencies. Each IP agencies should provide a report which will be shared (entirely or partially) with the consortium.
6. Reporting by consortium of a consolidated report regarding the patentability of project innovations according to IP agency's reports.

Linked to IP actions and in parallel, the consortium will manage the dissemination activities to avoid accidental IP leakage and will ensure awareness about IPR of results and oversight on IPR obligations. The general principle is that a party shall not publish foreground generated by another party or any background of such other party without the other party's prior written approval. To this aim the Consortium Agreement (CA) establishes that *"during the period of the Project and for a period of twelve months starting from the end date of the Project, the Dissemination of own Results by one or several Parties including but not restricted to publications and presentations of whatever form (excluding patent applications(s) and other registrations of IPRs), shall be governed by the procedure subject to the following provisions:*

- *Prior written notice of the final version of any planned publication, including copy of the proposed publication, shall be given to the other Parties at least thirty (30) calendar days before the planned publication submission date. Any objection to the planned publication shall be made in writing to the Party or Parties proposing the dissemination and the Coordinator within twenty (20) calendar days after the receipt of the written notice. If no objection is made within the time limit stated above, the publication is permitted.*
- *An objection to a planned publication by a Party is justified if:*
 - (a) the protection of the objecting Party's Results or Background would be adversely affected;*
 - and*
 - (b) the objecting Party's Legitimate Interests in relation to its Results or Background would be significantly harmed;*
 - (c) (iii) the proposed publication includes Confidential Information of the objecting Party;*
- *Any and all objection(s) shall include a precise request for necessary modifications*
- *If an objection has been raised on one or more of the above mentioned grounds, the objecting Party and the publishing Party shall discuss how to overcome the justified grounds for the objection on a timely basis (for example by amendment to the planned publication and/or by protecting Confidential Information before publication) and the objecting Party shall not unreasonably continue the opposition if appropriate measures are taken following the discussion.*
- *The objecting Party can request a publication delay of not more than 60 calendar days from the time it raises such an objection. After 60 calendar days the publication is permitted.*

During the same time, each partner should regularly analyse the commercial potential of their own inventions to select, manage and correct IP route accordingly.

6.1 IPR management process

To facilitate the completion and respect of the IP actions described above, the consortium will follow a specific management process. This process is described in the following figure:

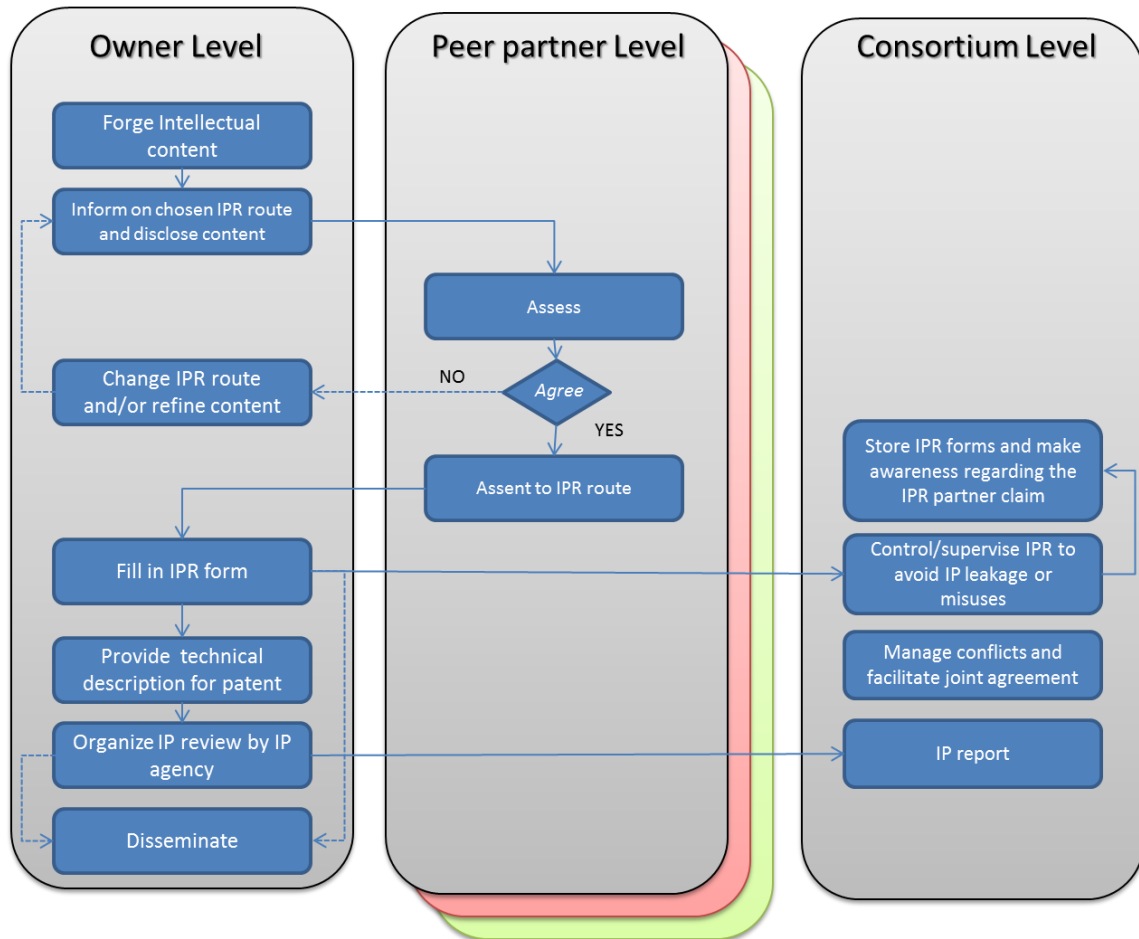


Figure 16 IPR management process

The management process will be conducted at three levels:

1. At specific owner level, each innovation owner shall forge the intellectual content, inform by email other partners of IP issues and IPR route chosen, provide IPR form (to be stored into the consortium database located in the RESISTO website document management system), eventually provide technical description for patent registration (or assimilated process: trademark, utility models, etc.), organise IP review by IP agencies, report to the consortium the results and disseminate the results accordingly.
2. At peer partner level, each partner should assess IP issue regarding content provided by the owner and agree the owner treatment of IP.
3. At consortium level, the consortium will provide IPR form, manage the awareness regarding new IPR form among the partners, oversight the IP obligation respect, manage the potential conflicts by facilitating joined agreement and define the consolidated report according to IP agency's reports.

6.2 Joint Ownership of Results

The principle is that the ownership of joint knowledge belongs to the Parties that generate it according to their share of participation to the common work. The Parties shall agree on how that joint ownership will be exercised.

As defined in the CA, two or more partners shall own results jointly if:

- a) *they have jointly generated them; and*
- b) *it is not possible to:*
 - (i) *establish the respective contribution of each Party; or*
 - (ii) *separate them for the purpose of applying for, obtaining or maintaining their protection*

The joint owners will strive to, within a six (6) month period as from the date of the generation of jointly-owned Results and before any industrial or commercial Exploitation, enter into a written separate joint ownership agreement to set the terms and conditions of the allocation of ownership, all protection measures and on the division of related costs and/or the conditions to Exploit.

6.3 Access and management of IPR form

To facilitate the gathering of IPR form, an on-line version of IPR form will be available from M14 on the RESISTO website. The access will be granted only for RESISTO partners. After reviewing by project manager and WP8 leaders, the forms will be made available for all partners into the RESISTO documents repository in pdf. The form will contain the following field.

Title:
Partner(s) (Acronym):
Kind (*background/foreground/side ground*):
Description:
Conditions for access (*Public/Available to project partners upon request/Other*):
Contact Name:
Contact Email:
Contact Phone:
Start date:

7. REFERENCES

INDEX	REFERENCE
[Ref1]	RESISTO – Grant Agreement. Project Starting Date: May, 1 st 2018
[Ref2]	RESISTO – D10.10 Exploitation Activities – first
[Ref3]	RESISTO – Consortium Agreement – V8.0