



Funded by the European Commission

Seventh Framework Programme



CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. 607642

D2.3 Final Roadmap

Date of deliverable: 31/05/2016
Actual submission date: 06/06/2016

Start date of the Project: 1st June 2014. Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 1.0

Project funded by the European Commission under the Seventh Framework Programme		
Restriction Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission)	



D2.3 Final Roadmap

Funded by the European Commission under the Seventh Framework Programme

Page 1 of 91

Revision history

Version	Object	Date	Author(s)
0.1	Creation	23/05/2016	E. Frumento, F. Freschi
0.2-0.3	Internal versions	30/05/2016	D. Ariu, E. Frumento
1.0	Final version ready to be submitted to EC	06/06/2016	E. Frumento, F. Freschi, D. Ariu



D2.3

Final Roadmap

Responsible

E. Frumento, F. Freschi (CEFRIEL)

Contributor(s)

All the partners of the project

Note: To allow a proper understanding of the ranking process, the reference document is D2.2 which includes also in Appendixes two documents describing the roadmapping methodology developed in WP2

- "Creation of Roadmaps based on Scenario Analysis" (Slides)
- "Tutorial on Scenario Analysis & Roadmapping"

Summary: This deliverable is the companion document of the final roadmap of the project which has been released as an interactive web site linked in the project's home page and also available as a subdomain at the address <http://roadmap.cyberroad-project.eu>. The present document reports some insight into the process followed to rank the research topics and the roadmap details plus includes all the research topics developed by the partners. The present documents elaborated the results of the previous deliverable, especially:

- D5.6 Cybercrime research topics
- D6.6 Cyberterrorism research topics
- D3.3 Social economic Legal research topics
- D2.2 Risk assessment ranking methodology

Keywords: final roadmap



TABLE OF CONTENTS

1	INTRODUCTION	7
1.1	FROM THE SCENARIOS TO THE RESEARCH TOPICS	7
1.2	SCORING PROCESS USED FOR THE ROADMAP	10
1.3	RESULTS OF THE RESEARCH TOPICS PRIORITIZATION	11
1.3.1	Readiness of current risk mitigation solutions	13
1.4	CREATION OF THE INTERACTIVE ROADMAP	15
2	ANTI-MALWARE	20
2.1	ABSTRACT	20
2.2	RESEARCH ACTION #1 RESEARCH IN MALWARE ANALYSIS FIELD, ADVANCED MALWARE DEFENCE AND SHIELDING	20
2.3	RESEARCH ACTION #2 ADVANCED MALWARE DETECTION AND PREVENTION TECHNIQUES ON MOBILE DEVICES	21
2.4	RESEARCH ACTIONS GANTT	22
3	AUTHENTICATION AND ANONYMIZATION	23
3.1	ABSTRACT	23
3.2	RESEARCH ACTION #1 COUNTER MEASURES TO ABUSES OF ANONYMITY TOOLS AND PROTOCOLS	23
3.3	RESEARCH ACTION #2 IMPROVED INFORMATION SHARING BETWEEN PARTIES WITH STANDARDIZATION OF PROTOCOLS AND LEGAL FRAMEWORKS AT LOCAL AND INTERNATIONAL LEVEL	24
3.4	RESEARCH ACTION #3 IMPROVEMENTS TO THE STABILITY AND SECURITY OF SYSTEMS USING STRONG, INNOVATIVE AUTHENTICATION METHODS, ENCRYPTION AND DIGITAL FORENSICS	24
3.5	RESEARCH ACTIONS GANTT	25
4	BEHAVIOURAL SECURITY	26
4.1	ABSTRACT	26
4.2	RESEARCH ACTION #1 BEHAVIOURAL USER AUTHENTICATION AND NO-PASSWORD SYSTEMS	26
4.3	RESEARCH ACTION #2 BEHAVIOURAL ANALYTICS FOR IoT-EMPOWERED SYSTEMS	27
4.4	RESEARCH ACTIONS GANTT	28
5	CRYPTOGRAPHY AND PUBLIC-KEY INFRASTRUCTURES (PKIS)	29
5.1	ABSTRACT	29
5.2	RESEARCH ACTION #1 DEVELOPMENT AND SECURITY ANALYSIS OF LIGHTWEIGHT ENCRYPTION AND AUTHENTICATION SCHEMES AS WELL AS HASH FUNCTIONS FOR LOW-END MOBILE DEVICES	29
5.3	RESEARCH ACTION #2 SCALABLE KEY DISTRIBUTION AND MANAGEMENT SCHEMES FOR SECRET-KEY BASED CRYPTOSYSTEMS AND NETWORKS WITH HIGHLY DYNAMIC TOPOLOGIES	30
5.4	RESEARCH ACTION #3 DEVELOPMENT AND EVALUATION OF (LIGHTWEIGHT) QUANTUM-RESISTANT ENCRYPTION AND AUTHENTICATION SCHEMES AS WELL AS DIGITAL SIGNATURES	30
5.5	RESEARCH ACTIONS GANTT	31
6	CYBERCRIME AND THE ECONOMY	32
6.1	ABSTRACT	32
6.2	RESEARCH ACTION #1 PROVIDE A FRAMEWORK FOR THE AGGREGATION OF TRUSTED AND RELIABLE DATA ON THE COST OF CYBERCRIME	32
6.3	RESEARCH ACTION #2 IN DEPTH THREAT ANALYSIS AND STUDY OF PREVENTATIVE MEASURES ON THE TOPIC OF CRYPTOCURRENCIES	33
6.4	RESEARCH ACTIONS GANTT	34
7	FORENSICS	35
7.1	ABSTRACT	35
7.2	RESEARCH ACTION #1 FORENSIC METHODS FOR BIG DATA	36
7.3	RESEARCH ACTION #2 LIVE FORENSICS, AUDIT & CONTROL	36
7.4	RESEARCH ACTION #3 FORENSICS IN MOBILE AND DISTRIBUTED ENVIRONMENTS	37
7.5	RESEARCH ACTION #4 DATABASE FORENSICS AND DATA LEAK DETECTION	37
7.6	RESEARCH ACTIONS GANTT	38
8	HEALTHCARE	39
8.1	ABSTRACT	39



8.2	RESEARCH ACTION #1 BETTER HARMONIZATION OF HEALTH CARE PROTOCOLS AND BETTER TESTING OF EXISTING SOLUTIONS AGAINST SECURITY (ALSO USING SECURE SOFTWARE DEVELOPMENT SOLUTIONS) AGAINST REAL AND MODERN THREATS.	39
8.3	RESEARCH ACTION #2 PROTECT AND TRAIN THE HUMAN CAPITAL.	40
8.4	RESEARCH ACTION #3 JUNCTION OF CYBER AND REAL THREATS.	41
8.5	RESEARCH ACTIONS GANTT	42
9	INFORMATION EXCHANGE	43
9.1	ABSTRACT	43
9.2	RESEARCH ACTION #1 HARMONIZATION OF INFORMATION EXCHANGE INCLUDING SENSITIVE AND CLASSIFIED ACROSS PUBLIC, MILITARY, PRIVATE AND ACADEMIC SECTOR.	43
9.3	RESEARCH ACTION #2 COMBATING FRAUD AND THEFT IN FREIGHT TRANSPORT AND CUSTOMS BROKERAGE.	44
9.4	RESEARCH ACTIONS GANTT	45
10	LAW AND ORDER	46
10.1	ABSTRACT	46
10.2	RESEARCH ACTION #1 DEVELOPING AN ENHANCED, INTEGRATED GLOBAL RESPONSE FROM CRIME FIGHTING AGENCIES.	46
10.3	RESEARCH ACTION #2 ENHANCEMENT OF THE EUROPEAN LEGAL FRAMEWORK.	47
10.4	RESEARCH ACTION #3 STUDY PRACTICES AND PROCESSES OF INTERNET MONEY LAUNDERING.	48
10.5	RESEARCH ACTIONS GANTT	49
11	NETWORKING	50
11.1	ABSTRACT	50
11.2	RESEARCH ACTION #1 MONITORING AND INTRUSIONS DETECTION SYSTEMS TO IDENTIFY NETWORK INTRUSIONS THAT CAN UNDERMINE DATA INTEGRITY (E.G. CORRUPT OPERATIONAL DATA WITH TRAFFIC INJECTION) OR CONFIDENTIALITY (E.G. WITH A MAN-IN-THE-MIDDLE ATTACK).	50
11.3	RESEARCH ACTION #2 PROTOCOLS FOR UTILITIES, SMART GRIDS AND ADVANCED METERING INFRASTRUCTURES (AMI) WITH EMBEDDED SUPPORT FOR ENCRYPTION, SECURITY, AUTHENTICATION AND SCALABILITY.	50
11.4	RESEARCH ACTION #3 INNOVATIVE SOLUTIONS TO GUARANTEE DATA INTEGRITY WITHOUT RELYING ON ENCRYPTION.	51
11.5	RESEARCH ACTIONS GANTT	51
12	CYBER THREAT AWARENESS	52
12.1	ABSTRACT	52
12.2	RESEARCH ACTION #1 IMPROVEMENT OF AWARENESS MECHANISMS FOR DATA AND INFORMATION SHARING IN PERSONAL AND WEARABLE DEVICES AND IN THE TREND OF DISAPPEARING COMPUTER.	52
12.3	RESEARCH ACTION #2 IMPROVING THE AWARENESS OF CYBER THREATS FOR WORKFORCES IN CRITICAL INFRASTRUCTURES.	53
12.4	RESEARCH ACTION #3 DETECTION OF ATTEMPTS OF TAMPERING WITH MANUFACTURING PROCESSES IN INDUSTRIAL PLANTS.	53
12.5	RESEARCH ACTION #4 CREATION OF AD-HOC AWARENESS EXPERIENCES.	54
12.6	RESEARCH ACTIONS GANTT	55
13	NEW OBJECTS AND DISAPPEARING COMPUTING	56
13.1	ABSTRACT	56
13.2	RESEARCH ACTION #1 DIFFICULTY TO FIND UPDATING MECHANISMS THAT SCALE TO LARGE AND HETEROGENEOUS NETWORKS.	56
13.3	RESEARCH ACTION #2 ABSENCE OF A RELIABLE AND HOLISTIC SECURITY MECHANISM.	57
13.4	RESEARCH ACTION #3 ABSENCE OF A SYSTEMIC VIEW OF THE CORRELATION AMONG SECURITY, PRIVACY AND SAFETY.	57
13.5	RESEARCH ACTIONS GANTT	58
14	SCADA & CRITICAL INFRASTRUCTURES PROTECTION	59
14.1	ABSTRACT	59
14.2	RESEARCH ACTION #1 ADDRESSING ADVANCED SECURE MOBILE COMPUTING FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE.	60
14.3	RESEARCH ACTION #2 TRAINING PLATFORMS ABLE TO REPLICATE REAL CRITICAL INFRASTRUCTURES.	60
14.4	RESEARCH ACTION #3 INFORMATION SHARING SYSTEMS TO SUPPORT CRITICAL INFRASTRUCTURE PROTECTION.	61
14.5	RESEARCH ACTIONS GANTT	63



15	SOCIAL RESILIENCE	64
15.1	ABSTRACT	64
15.2	RESEARCH ACTION #1 ABSENCE OF A TRUSTED AUTHORITY FOR COMMUNICATION WITH PEOPLE AT RISK	64
15.3	RESEARCH ACTION #2 IDENTIFICATION OF POSSIBLE SECURITY AND SAFETY ISSUES	65
15.4	RESEARCH ACTION #3 ENSURE REDUNDANCY OF THE TRUSTED AUTHORITY	65
15.5	RESEARCH ACTIONS GANTT	66
16	SDLC & ARCHITECTURES	67
16.1	ABSTRACT	68
16.2	RESEARCH ACTION #1 DEVELOPMENT OF CODING STANDARDS FOR SECURE AND FAULT-TOLERANT CYBER-PHYSICAL SYSTEM DEVELOPMENT	68
16.3	RESEARCH ACTION #2 STANDARDIZED INTERFACES TO EXTERNAL MODULES AND SYSTEMS FOR PROVIDING IN-DEPTH SECURITY.	69
16.4	RESEARCH ACTION #3 COMPONENT AND SYSTEM LEVEL PENETRATION-TESTING PROCEDURES DURING DEVELOPMENT AND INTEGRATION OF COMPLEX SYSTEMS.	69
16.5	RESEARCH ACTION #4 EXTENDING CURRENT SECURITY ARCHITECTURES TO LARGE DISTRIBUTED SYSTEMS INCLUDING PLAYERS WITH DIFFERENT BACKGROUND KNOWLEDGE IN SECURITY. FURTHERMORE, NEW AUTHENTICATION MECHANISMS NEED TO BE DEvised THAT PROVIDE USABLE SECURITY AND CONTINUOUS AUTHENTICATION.	70
16.6	RESEARCH ACTION #5 METHODOLOGIES TO INCREASE PREPAREDNESS AND RESPONSIVENESS IN CASE OF ATTACK, INCLUDING ATTACKS TARGETING PRODUCTION PROCESS (E.G. TO INSERT MALWARE, BACKDOORS OR TROJAN IN FINAL PRODUCTS).	70
16.7	RESEARCH ACTION #6 INTELLIGENT IDS, HARDENING MECHANISMS AND AWARENESS.	71
16.8	RESEARCH ACTIONS GANTT	71
17	THREAT INTELLIGENCE AND ATTACK DETECTION	72
17.1	ABSTRACT	72
17.2	RESEARCH ACTION #1 THREAT AND ATTACK INTELLIGENCE IMPROVEMENT, BY DEVELOPING ATTACK SIMULATION INFRASTRUCTURES AND ADVANCED RISK ANALYSIS AND MODELLING.	73
17.3	RESEARCH ACTION #2 INTELLIGENT INTRUSION AND MALWARE DETECTION, SYSTEM HARDENING AND SITUATION AWARENESS ACROSS A COMPLEX ENVIRONMENT	73
17.4	RESEARCH ACTION #3 PROTECTION OF ORGANISATIONS FROM CRITICAL DATA LEAKS CAUSED BY INTENTIONAL OR UNINTENTIONAL INSIDER THREATS.	74
17.5	RESEARCH ACTION #4 UNDERSTANDING THE ECONOMIC IMPACT OF DIGITAL CURRENCIES AND THEIR ROLE IN ENABLING NEW FORMS OF CYBER AND ORGANISED CRIME.	75
17.6	RESEARCH ACTIONS GANTT	76
18	TRUST CHAINS AND IDENTITY	77
18.1	ABSTRACT	77
18.2	RESEARCH ACTION #1 TRUST CHAINS BETWEEN INDIVIDUALS	77
18.3	RESEARCH ACTION #2 TRUST CHAINS IN CYBER-PHYSICAL SYSTEMS, IOT, AND SUPPLY CHAINS.	78
18.4	RESEARCH ACTION #3 TRUST CHAINS IN FINANCIAL MARKETS.	79
18.5	RESEARCH ACTIONS GANTT	80
19	VULNERABILITY ASSESSMENT	81
19.1	ABSTRACT	81
19.2	RESEARCH ACTION #1 VULNERABILITY ASSESSMENT TOOLS AND PROCEDURES	81
19.3	RESEARCH ACTIONS GANTT	83
ANNEX I - TEMPLATE FOR THE DESCRIPTION OF THE RESEARCH TOPICS AND ACTIONS		84
ANNEX II - TEMPLATE FOR THE GANTT DIAGRAM ASSOCIATED WITH EVERY RESEARCH TOPIC		87
ANNEX III - TEMPLATE FOR THE PRIORITIZATION OF THE RESEARCH TOPICS		89



1 INTRODUCTION

The Cybercrime and Cyberterrorism research roadmap, is the final outcome of the CyberROAD project. The roadmap, has been prepared following the indications provided in the following two project deliverables:

- D2.1 – Roadmapping Methodologies and guidelines for information collection and assessment
- D2.2 – *Risk Assessment Ranking Methodology* and its annexed documents:
 - “*Creation of roadmaps based on scenario analysis*”
 - “*Tutorial on Scenario Analysis and Roadmapping*”

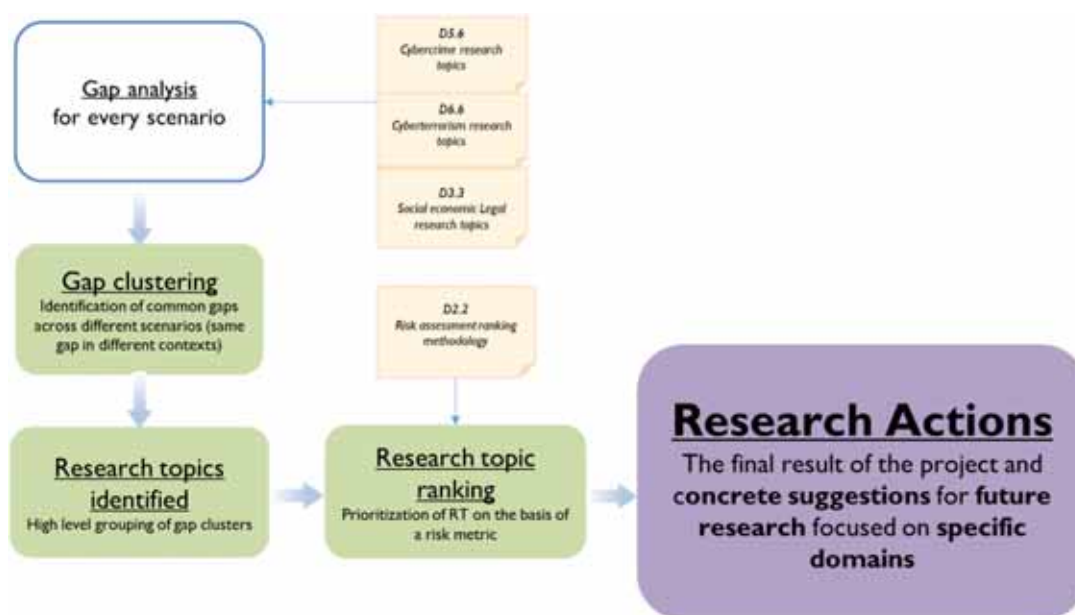


Figure 1 - Process for the preparation of the CyberROAD roadmap

The process consisted of the following fundamental steps, depicted in Figure 1:

- 1) The preparation of a set of scenarios pertaining Cybercrime and Cyberterrorism from which current and future research gaps have been identified;
- 2) The clustering of Research Gaps into coherent Research Topics;
- 3) The analysis of the Research Gaps and design of a set of Research Actions required to address them. Research Actions, organised into coherent Research Topics, prioritised, and finally represented in a user-friendly fashion, represent **the final CyberROAD roadmap**.

Details of the process which lead to the delivery of the roadmap will be provided in the rest of the Chapter 1 of this document.

1.1 FROM THE SCENARIOS TO THE RESEARCH TOPICS

A set of **Scenarios** (each one containing both the current and the future **Views**) has been defined. We refer the reader to “D2.2 – Risk Assessment Ranking Methodology” and its annexed “Tutorial on Scenario Analysis and Roadmapping” for the definition of *Scenario*, *View*, and of their structure. CyberROAD partners agreed on the list of Scenarios to address during the *CyberROAD workshop* (internal project workshop) which took place in Vienna on December 9th, 2015¹. For the sake of completeness, we report below here in Table 1 the list of Scenarios.

¹ Details of the Workshop and its outcomes are provided in “D7.8 – Second ARES Workshop Report”



Scenario	View	Partner
Social Sharing	(i) Social Network (CC and CT)	NASK & FORTH
	(ii) Life logging (CC and CT)	RHUL
	(iii) Wearable device (CC & CT)	SUPSI
Building Automation	(i) Smart Building and domotics	SBA
Energy	(i) Water Utilities	SM
	(ii) Gas Utilities	VITRO
	(iii) Smart Grid	VITRO
Transportation	(i) ICT Systems for Transportation	NCSRD
	(ii) Aviation	NCSRD
	(iii) Smart Roads	NCSRD
Healthcare	(i) Mobile Health and Augmented Humans	CEFRIEL
	(ii) Hospital 2.0	CEFRIEL
	(iii) P4 Medicine	SBA
Security and safety	(i) Fighting Cybercrime as a Service	CDF
	(ii) Attribution of cyber crime	NASK
	(iii) Trusted Components (SW and HW, supply chain)	TUD
Workforce	(i) Enterprise 2.0 (BYOD, ubiquitous connectivity)	CEFRIEL
Industry	(i) Industry 4.0	SM
	(ii) Just in time production	TUD
Financial Services	(i) Cryptocurrencies	CDF
	(ii) Online Banking	RHUL



Data Driven Economy	(i) Big Data (CC and CT)	SBA
	(ii) Control over data (includes privacy, data protection and leakage, OS/computer system logging, Software as a Service (SaaS))	SBA

Table 1 - List of Scenarios and of the corresponding Views identified during the CyberROAD Workshop in Vienna.

The aforementioned Scenarios, provided as an Annex to both deliverables “D5.6 – Cybercrime Research Topics” and “D6.6 – Cyber-terrorism Research Topics” have been analysed within the scope of tasks T3.3, T5.4, and T6.4, which have analysed them from the SEPL (Social, Economic, Political, Legal), from the Cybercrime, and from the Cyber-Terrorism perspective respectively.

From the analysis of each Scenario, and in particular from the comparison of the current against the future views, a list of **Research Gaps** has been identified that shall be addressed by the future research actions in Europe to mitigate the risk arising from Cybercrime and Cyberterrorism attacks. In total 209 research gaps have been identified:

- 7 of which emerged from the SEPL analysis in Task 3.3 and which are reported in D3.3;
- 105 of which emerged from the Cybercrime analysis in Task 5.4 and which are reported in D5.6;
- 97 of which emerged from the Cyberterrorism analysis in Task 6.4 and which are reported in D6.6.

Because of the nature of the problem, a clear separation between gaps affecting Cybercrime and Cyberterrorism has been not always possible. In order to cope with this aspect, for each gap it has been clearly specified if it affects only cybercrime, only cyber-terrorism, or both.

Coherent Research Gaps have been grouped together (independently from the originating scenario) into **Research Topics**, each Research Topic being a set of related **Research Actions** required to address the set of gaps. A number of 18 Research Topics has been identified which are those covered by the CyberROAD roadmap:

Research Topic #1.	ANTI-MALWARE
Research Topic #2.	AUTHENTICATION AND ANONYMIZATION
Research Topic #3.	BEHAVIOURAL SECURITY
Research Topic #4.	CRYPTOGRAPHY AND PUBLIC-KEY INFRASTRUCTURES (PKIS)
Research Topic #5.	CYBERCRIME AND THE ECONOMY
Research Topic #6.	FORENSICS
Research Topic #7.	HEALTHCARE
Research Topic #8.	INFORMATION EXCHANGE
Research Topic #9.	LAW AND ORDER
Research Topic #10.	NETWORKING
Research Topic #11.	CYBER THREAT AWARENESS
Research Topic #12.	NEW OBJECTS AND DISAPPEARING COMPUTING
Research Topic #13.	SCADA & CRITICAL INFRASTRUCTURES PROTECTION
Research Topic #14.	SOCIAL RESILIENCE
Research Topic #15.	SDLC & ARCHITECTURES
Research Topic #16.	THREAT INTELLIGENCE AND ATTACK DETECTION
Research Topic #17.	TRUST CHAINS AND IDENTITY
Research Topic #18.	VULNERABILITY ASSESSMENT

Research Topics have been assigned to CyberROAD partners involved in Task 2.3 (basically all the partners), which prepared them according to the template provided as **Annex I - Template for the Description of the Research Topics and Actions**). Based on the template provided, each Topic has been characterised by the means of:

- A short abstract, concisely describing the goals and the actions foreseen for the Research Topic;
- A number of **Research Actions**, each one addressing and filling a number of gaps concerning the Research Topic;
- **A set of data required for the prioritization of the Topics**, defined according to the *Risk Assessment Ranking Methodology* depicted in D2.2. Required data included the *Distance to the Market*, the *Cost of the Topic*, the *Availability of Competence in Europe*, the *Time Span for Addressing the Action*, and the *Actors involved*. An explanation of the meaning of such data and of the metrics used to measure them is provided in D2.2.



Research Actions corresponding to each Topic have been also displaced over a time period of 5 years using the template provided as **Annex II - Template for the Gantt Diagram Associated with Every Research Topic** of this document.

1.2 SCORING PROCESS USED FOR THE ROADMAP.

In order to proceed with the prioritization of the Research Topics, the Risk Assessment Ranking Methodology described in D2.2 required an additional set of information with respect to those already provided by the CyberROAD partners during the preparation of the Research Topics.

In particular, the proposed Risk Ranking methodology required for each Research Topic:

- To identify the Cyber Threats concerning the Topic;
- To identify the list of assets affected by each Cyber Threat;
- To calculate the risks using Boston Squares, that is providing likelihood for each threat and a measure of the impact of the threat itself.

Based on the information above, Research Topics have been ranked to.

In order to make the evaluations consistent among the 18 Research Topics, a common list of Cyber Threats² has been identified.

- **Accidental leak.** The agent is "friendly user" and intends to protect assets, but accidentally or mistakenly takes actions that result in harm.
- **Denial of Service.** Not only DoS but starvation in general at all the levels (NTW, system, service or storage)
- **Eavesdropping, Interception and Hijacking.** Secretly listening to the private conversation and intercepting data during their transferring (es. MITM)
- **Espionage.**
- **Financial Fraud.**
- **Misuse.** Benign shortcuts and misuse of authorizations, "pushed wrong button". Current employee with harmless intent but unknowingly misuses system or safeguards
- **Opportunistic data theft.** Opportunistic individual with simple profit motive.
- **Physical theft.**
- **Product/system alteration.** Incidental alteration of the products, not intentional like Sabotage.
- **Sabotage.** Abuse of privileges for sabotage, cyber or physical.
- **Violence.** Violent acts toward people.

Similarly, a list of assets³, which might be impacted by the Threats, was also identified:

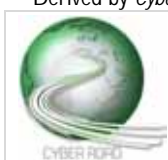
- **Access Data**
- **Business/Service**
- **Commercially Sensitive Data**
- **Intellectual Property**
- **Materials**
- **Money**
- **People**
- **Personal Data**
- **Plants and Equipment**
- **Procedures and Processes**
- **Reputation**

Threats and the corresponding affected Assets were listed in a template (**Annex III**) which has been distributed through the consortium for an evaluation of the risk associated with each Research Topic.

More details regarding Risk evaluation are provided in the following section.

² Derived by *Critical Infrastructure Readiness Report*, The Aspen Institute / INTEL Security, 2015

³ Derived by *Cyber-attacks: effects on UK companies*, Oxford Economics, 2014



1.3 RESULTS OF THE RESEARCH TOPICS PRIORITIZATION

The last step toward the final research roadmap was to assign a scoring to the risks of each research topic. This operation was done following the methods described in the deliverable D2.2 and led to the classification of the research topics along four dimensions of risk:

- *Data Breach Risk*, meant as the risk of losing control over the data or having a breach;
- *Health & Safety Risk*, meant as the risk of having health injuries or physical safety risk (e.g. killing people);
- *Financial Risk*, meant as the risk of having financial losses;
- *Intangible Risk*, as defined in D2.2.

The CyberROAD partners who originally compiled the Research Topics, were asked, for each threat and each corresponding Affected Asset to evaluate all the risks dimensions, assigning standardized risk values, using the template provided as **Annex III - Template for the Prioritization of the Research Topics**).

It is important to underline that each of the four risk dimensions have different ranges of values, according to the absolute importance of the risk axis (for example the Health & Safety risk is usually considered higher in terms of cost, because may affect human lives), as it can be easily seen from the **Annex III - Template for the Prioritization of the Research Topics**

At the end of this process a set of Excel files has been obtained, one for each research topic, each file containing the scores independently assigned by the experts.

The final stage was to collect these separated values in a unique datasheet file and to assign a final overall weighted rank. The result is a situation like the following:

Modify weighting factors	
Data Breach Risk	1
Health & Safety Risk	1
Financial Risk	1
Intangible Risk	1

Weighting factors	
Very high	1
High	0,75
Medium	0,5
Low	0,25
Negligible	0

Research topic	Value	Rank
RT04 Cryptography	8911,00	1
RT01 Anti malware	8685,00	2
RT12 New objects	8628,00	3
RT17 Threat intelligence	7428,00	4
RT08 Information exchange	7245,00	5
RT16 SDCL & Architectures	6927,00	6
RT07 Healthcare	6900,00	7
RT11 Awareness	6534,00	8
RT09 Law & order	6509,00	9
RT10 Networking	6321,00	10
RT15 Social resilience	6317,00	11
RT05 CyberCrime Economy	6312,00	12
RT02 Authentication	5851,00	13
RT14 SCADA & CIP	5650,00	14
RT19 Vulnerability assessment	5269,00	15
RT06 Forensics	5190,00	16
RT18 Trust chain & identity	3379,00	17
RT03 Behavioural security	2540,00	18

Rank #	Stars
1 Very high	5
1 Very high	5
1 Very high	5
1 Very high	5
2 High	4
2 High	4
2 High	4
2 High	4
3 Medium	3
3 Medium	3
3 Medium	3
4 Low	2
4 Low	2
5 Negligible	1
5 Negligible	1
5 Negligible	1
5 Negligible	1
5 Negligible	1



The tables above provide:

- The weights, or the relative importance of each single risk axis onto the overall risk score
- The list of the research topics and the calculated risk value
- The rank of the risk value, resulting from the Excel's formula RANK⁴.
- The grouping of the research topics in four categories of importance: *negligible, low, medium, high and very high*.
- The assigned number of stars (orange column)

The final result is a list of research topics, sorted by the rank of the calculated risk. The risk is a weighted sum of the four independent risks:

$$Risk = \sum_{i=0}^4 Weight[i] * Risk[i] * Importance[i]$$

Each $Risk[i]$ (one among the four risk axis identified) is multiplied for a $Weight[i]$ and an $Importance[i]$ whose value ranges from 0 to 1. The scoring for the final roadmap was calculated with $Importance[i] = 1 \forall i$.

The interesting possibility offered by this method of calculating the risk is that it is possible to modify the values of $Importance[i]$, tweaking the final risk rank for special situations. The most interesting analysis is to look what happens if we set $Importance[i]=0$ for $\forall i \neq j$ where j is one of the four risk axis. This, in other words, means that the model considers only one risk direction and ignores all the others. The rank is therefore modified accordingly.

For example, only considering the *Data Breach Risk* ($j=1$) the final scoring of the research topics becomes the following:

Modify weighting factors	
Data Breach Risk	1
Health & Safety Risk	0
Financial Risk	0
Intangible Risk	0

Weighting factors	
Very high	1
High	0,75
Medium	0,5
Low	0,25
Negligible	0

Research topic	Value	Rank
RT04 Cryptography	2109,00	1
RT08 Information exchange	2080,00	2
RT17 Threat intelligence	1776,00	3
RT05 CyberCrime Economy	1737,00	4
RT01 Anti malware	1554,00	5
RT09 Law & order	1544,00	6
RT16 SDCL & Architectures	1499,00	7
RT19 Vulnerability assessment	1449,00	8
RT06 Forensics	1430,00	9
RT11 Awareness	1350,00	10
RT07 Healthcare	1326,00	11
RT12 New objects	1304,00	12
RT14 SCADA & CIP	1304,00	12
RT10 Networking	1226,00	14
RT18 Trust chain & identity	1157,00	15
RT15 Social resilience	1028,00	16

Rank #	Stars
1 Very high	5
1 Very high	5
1 Very high	5
1 Very high	5
2 High	4
2 High	4
2 High	4
2 High	4
3 Medium	3
3 Medium	3
3 Medium	3
4 Low	2
4 Low	2
5 Negligible	1
5 Negligible	1
5 Negligible	1

⁴ Returns the rank of a number in a list of numbers.



RT02 Authentication	896,00	17
RT03 Behavioural security	257,00	18

5 Negligible	1
5 Negligible	1

Comparing the two situations reported the rank of “RT 01 Antimalware” for example, changes from 2 to 5.

1.3.1 READINESS OF CURRENT RISK MITIGATION SOLUTIONS

The **readiness** in general could be defined as the capability of the current defences or risk mitigation solutions to solve a today's risk. In other words, **the readiness is the opposite of the risk**. The higher is the risk associated to a Research Topic, the lower is the level or readiness of the current risk mitigation solutions. In other words, it can be an alternative way to interpret the risk rank value.

As an example, to a research topic that is ranked to a “negligible” level of risk corresponds very effective risk mitigation solutions, hence with a high level of readiness. The formula to convert the risk ranking to the readiness value is reported in Figure 2: the rank has been sampled in 5 values.



Figure 2 – Readiness as a discrete function of the risk rank

The concept of readiness is extremely interesting because it represents the estimated situation of today's defence solutions.

Let consider the readiness level of ne Research Topics at time (e.g., for some RTs) along the four risk axis (we cycle setting $j=1$ for all the risk axis). The result is as follows:

		Healthcare		SCADA & CIP		Anti malware		SDLC & Architecture
	Rank	Readiness	Rank	Readiness	Rank	Readiness	Rank	Readiness
Data Breach Risk	10	3 Medium	11	3 Medium	5	2 High	6	2 High
Health & Safety Risk	4	1 Very high	10	3 Medium	2	1 Very high	9	3 Medium
Financial Risk	12	4 Low	13	4 Low	7	2 High	10	3 Medium
Intangible Risk	10	3 Medium	10	3 Medium	4	1 Very high	7	2 High

Table 2 - relative rank of RT07, RT14, RT01, RT16 for each risk axis and the corresponding readiness levels

These values can be transported into a radar graph like the one reported in Figure 3, which shows the estimated areas of attention for each Research Topic.





Figure 3 – Readiness radar graph for RT07, RT14, RT01, RT16

1.4 CREATION OF THE INTERACTIVE ROADMAP.

The CyberROAD research roadmap has been made available online since May 25th 2016 on to the CyberROAD website, and it is reachable from the project homepage (see Figure 4). The roadmap, is also directly reachable from the address <http://roadmap.cyberroad-project.eu>.



Figure 4 – Link to the CyberROAD roadmap onto the project homepage

The roadmap, which is developed using the HTML5⁵ markup language, is interactive, user-friendly, and can be easily navigated as a standard website.

First, the user is presented a page (see Figure 5), which concisely explains the CyberROAD project, the roadmap, and how it has been built.

⁵ http://www.w3schools.com/html/html5_intro.asp





Figure 5 - The Home Page of the CyberROAD roadmap

As the user presses on the "START" button, instructions are provided which explain how the different parts of the roadmap can be accessed (Figure 6). Clicking on the "GOT IT" button the user finally enters the roadmap.



Figure 6 - The How-To page explains the users how the different parts of the roadmap can be accessed.

The roadmap (Figure 7) is represented by a street, which goes through 18 "skyscrapers", each one representing a different Research Topic.



Figure 7 - The CyberROAD Roadmap. Each research topic is represented by a skyscraper, which height is proportional

The height of each skyscraper is correlated with the importance of the Research Topic in the ranking: the higher the importance of a Topic, the higher the corresponding skyscraper. The same information is also represented by a number of stars associated to each skyscraper: the most relevant topics are marked with 5 stars, whereas the less relevant have only 1.

The overall ranking is also available clicking on the "LIST VIEW" button (the pop-up which appears when the button is clicked is displayed in Figure 8).

RESEARCH TOPIC	
RT04 Cryptography	★★★★★
RT01 Anti malware	★★★★★
RT12 New objects	★★★★★
RT17 Threat intelligence	★★★★★
RT08 Information exchange	★★★★
RT16 SDCL & Architectures	★★★★
RT07 Healthcare	★★★★
RT11 Awareness	★★★★
RT09 Law & order	★★★
RT10 Networking	★★★
RT15 Social resilience	★★★
RT05 CyberCrime Economy	★★
RT02 Authentication	★★
RT14 SCADA & CIP	★
RT19 Vulnerability assessment	★
RT06 Forensics	★
RT03 Behavioural security	★
RT18 Trust chain & identity	★

Figure 8 - Ranking of the Research Topics.



Details of each Research Topic can be accessed from the box in the top-left corner of the screen. The box contains two buttons: the “READ AN ABSTRACT” button actually opens a pop-up which contains the abstract (Figure 9), whereas the “DOWNLOAD FULL DOCUMENT” button allows to download a PDF file containing the whole description of the Research Topic.

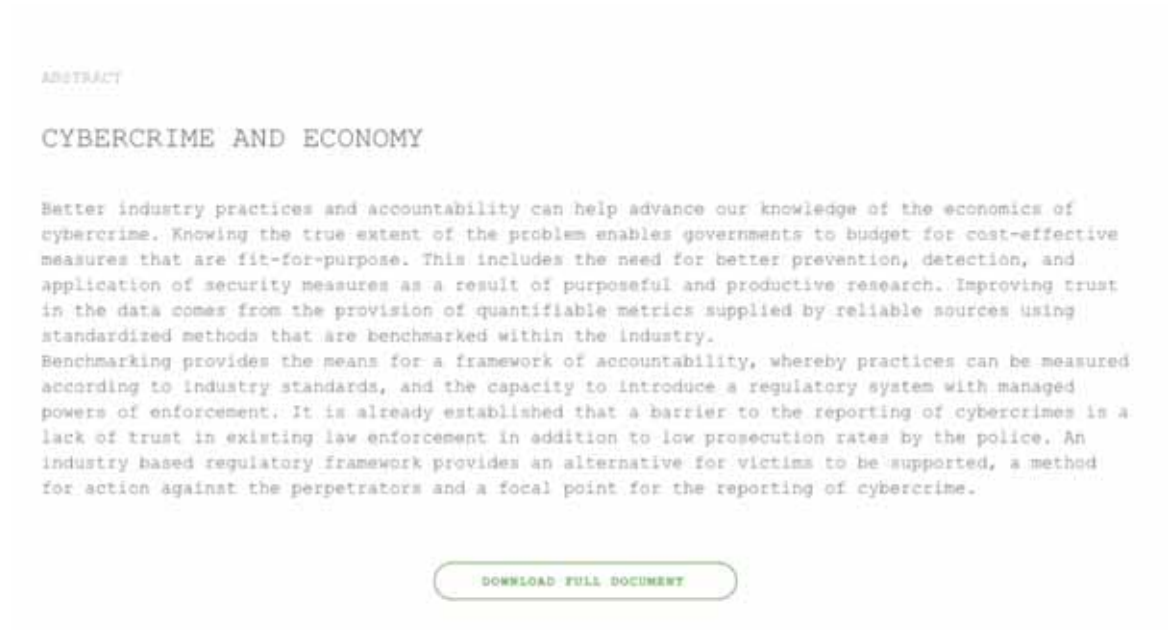


Figure 9 - An example of Abstract of a Research Topic

The description of the Research Topic is provided according to the template provided as Annex I - Template for the Description of the Research Topics and Actions) of this document, and also contains the GANTT diagram of the Research Actions (Annex II - Template for the Gantt Diagram Associated with Every Research Topic of this document). As an example, the frontpage of the “Cybercrime and the Economy” Research Topic is provided in Figure 10.



Figure 10 - Front-page of the Research Topic "Cybercrime and the Economy"

For each Research Topic, the GANTT diagram displaying the sequence of research actions over a time period of five years is also shown. Each Research Action, is represented by a horizontal green bar, which length is proportional to the time for the action being implemented.



Figure 11 - A GANTT diagram of the Research Actions is provided for each Research Topic. Each green bar corresponds to a Research Action, of which a small description is provided as the user passes over with the mouse.

When the user passes the mouse over a specific action, its title is displayed. Dependencies of the research actions are also, where existing, displayed by the means of a grey arrow connecting the actions.

2 ANTI-MALWARE

CT RG-55/34 and CC RG-2/8/35	Research in malware analysis field, advanced malware defence and shielding
CT RG-9 and CC RG-11	Design of advance malware detection, analysis and prevention tools and techniques for lifelogging
CT RG-94 and CC-RG-100	Advanced malware analysis tools and techniques and mitigation of infection techniques
CT RG-101 and CC-RG-105	Research on advanced malware detection and prevention techniques on mobile devices

2.1 ABSTRACT

Malicious Software (malware) has always been a vehicle of choice for cybercriminals and cyberterrorists to deliver their attacks. What was once started as an activity for fun has now consolidated into a well-established business model mostly driven by profit and political motifs. Malware is nowadays responsible for most of the malicious activities on the Internet (e.g., sensitive and financial information theft, DDoS, spam, click fraud), playing a fundamental role in more complex attacks. Despite the non-negligible research effort invested by the academic and industry community, statistics and trends provide a clear evidence that malicious software still represents one of the most pressing Internet threats undermining the security, privacy and safety of Internet users - an increasingly worrying concern that nowadays is not only confined to traditional computing devices, but that also spreads to mobile, critical infrastructure and Internet of Things at a very fast pace. Dealing with malware will be the challenge for the next decade.

2.2 RESEARCH ACTION #1 RESEARCH IN MALWARE ANALYSIS FIELD, ADVANCED MALWARE DEFENCE AND SHIELDING

DISTANCE TO THE MARKET: TRL 5

COST OF THE TOPIC: 5-10 Research and Innovation Actions, 1 CSA

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 5 years

ACTORS: security industry, SMEs, Universities, Research Centres

The analysis, classification and detection of malicious software has been the focus of a number of research efforts, in recent years. The problem space is large and requires a holistic approach geared towards building on sound techniques (e.g., machine learning, program analysis, software verification) that can be shown to work in real operational settings. To further exacerbate the problem, novel techniques must address the problem posed by evasive malware, engineered to hinder automatic analysis attempts represent; there is the need to develop techniques to automatically reason about behaviours or syntactic artefacts aimed at bypassing protections.

A holistic approach would require to research along the following dimensions:

- **Detection.** Find if the system is infected with malware. Develop novel mechanisms (beyond signature matching) that will evaluate the overall behaviour of the system and detect when malware is suspected to be present. Detection can be both passive and active in an effort to force the malware to reveal itself.
- **Prevention.** Prevent malware from entering the system in the first place. Take a whole-system-image approach to exploit information coming from several different sources over a long period of time.
- **Tolerance.** Operate in the presence of malware. Design systems that can function correctly (to a large extent) even when they are infected with malware that cannot be eradicated.



2.3 RESEARCH ACTION #2 ADVANCED MALWARE DETECTION AND PREVENTION TECHNIQUES ON MOBILE DEVICES

DISTANCE TO THE MARKET: TRL 5

COST OF THE TOPIC: 5-10 Research and Innovation Actions, 1 CSA

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 5 years

ACTORS: security industry, SMEs, NGOs, Universities, Research Centres

Over the past few years we have seen a rapid increase in the use and deployment of mobile devices. People are using their smartphones and tablets much more than they use their traditional computers; young people have also started to re-discover wristwatches in the face of devices that can do much more than tell the time: measure steps, measure heart rate, and comment on health status. In this exciting new world, smart mobile devices will be an attractive target for cybercrime and cyberterrorism. Remote possession and control of these devices, through malware, will provide a wealth of opportunities for an attacker: know the whereabouts of the target, know his/her vulnerable spots, provide them with faulty information, steal their data, steal their money, extort them, place bogus information in the device, interfere with all physical world structures it controls (smart cars, smart homes, etc.).

In this new environment we need a whole new approach to deal with malware:

- **Measuring and Monitoring.** Although traditional computers have extensive measuring, monitoring and logging facilities, smart devices have little, if any at all. We need research in order to develop mechanisms that will let us measure and monitor the behaviour of smart and embedded devices. Without being able to fully monitor a device, malware will always be able to slip between the cracks and hide.
- **Control.** Provide users with the ability to control their devices and their data. Provide more transparency in all actions and shed light into who is accessing what. Provide users with the ability to grant access to data and resources as well as the ability to revoke this access on-demand. Change the access model from a server-centric to a user-centric one.
- **Change the model.** Conduct research in alternative models of detection. Detect malicious behaviour even if no malicious executable (i.e. malware) can be detected. Develop novel ways to handle and tolerate malicious behaviour which may come from any type of interaction.



2.4 RESEARCH ACTIONS GANTT

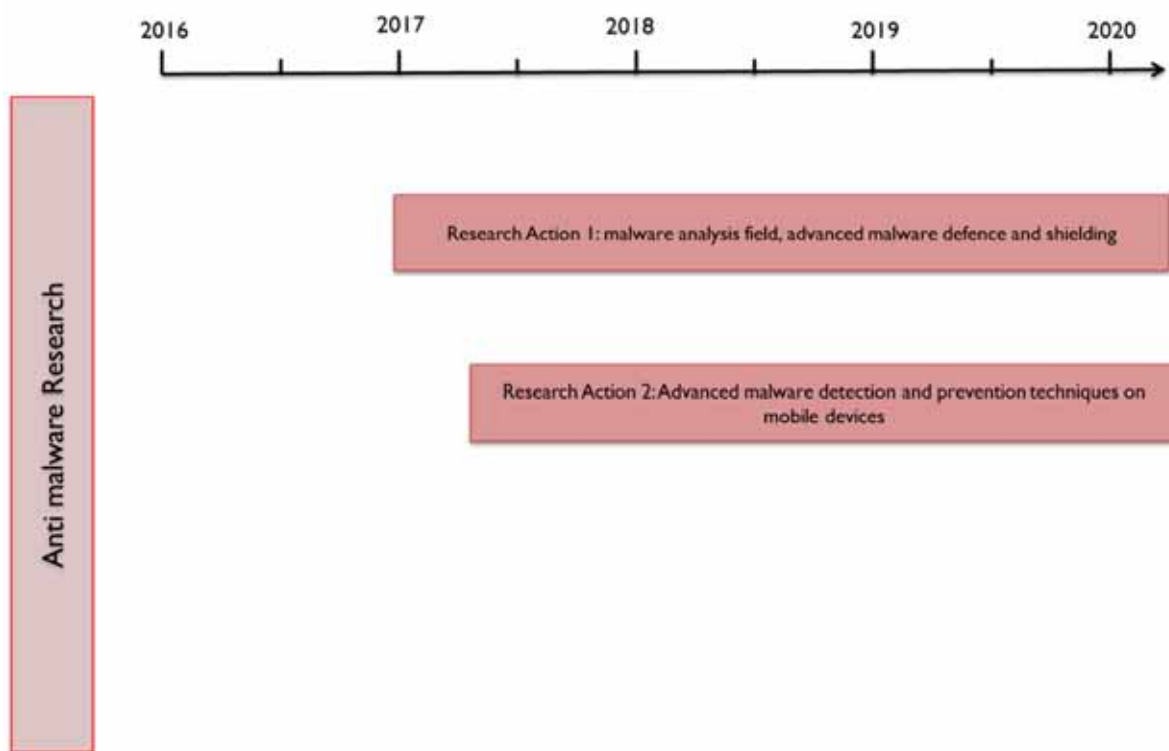


Figure 12 – Anti-malware RAs GANTT

3 AUTHENTICATION AND ANONYMIZATION

CC NO ID 01 & CT RG-65	De-anonymization of internet users
CC RG-17	Standardized Security measures with strong authentication.
CC RG-19	Innovative data leakage detection system capable to capture any anomalous path taken by sensitive data
CC RG-3	Improvement of the monitoring tools either for personal usage, as it is already happening of the credit card market
CC RG-4	Advanced research in security and privacy concerning virtual worlds
CC RG-59	Watermarks and Fingerprints that survive enrichments and aggregation
CC RG-60	Watermarks that are resilient against collusions and do only have a negligible impact on the results
CC RG-7 & CT RG-4	Advanced research in authentication and anonymization
CT RG-95	Novel techniques for access control

3.1 ABSTRACT

Low prosecution rates for acts of cybercrime and cyberterrorism are due, to some extent, to an inability to identify the actors involved. Without this knowledge the capacity for mitigation, prevention of future attacks and bringing perpetrators to justice is severely limited. The advent of Big Data and the Internet of Things will see anonymization increase with further pressures on authentication systems from both the inside and the outside. To stem this tide, appropriate measures are necessary to ensure that the safety and security of users is protected and enhanced in a world where social networks and wearable devices are commonplace and people are exposed to an increase in the dangers from phishing, identity theft, and information disclosure.

The goal is to design, formulate and create innovative solutions appropriate for a future where authentication is still possible and anonymization does not protect and give further advantage to cybercriminals and cyberterrorists.

3.2 RESEARCH ACTION #1 COUNTER MEASURES TO ABUSES OF ANONYMITY TOOLS AND PROTOCOLS

DISTANCE TO THE MARKET: TRL 3
COST OF THE TOPIC: 3 STREPs + 1 IP
AVAILABILITY OF COMPETENCE IN EUROPE: 3
TIME SPAN FOR ADDRESSING THE ACTION: 30 months
ACTORS: Research institutions, Industry

In anticipation of an increase in the number of personal and wearable devices in an IOT future measures are needed that protect the identity of users and militate against the theft of anonymized data.

Anonymity tools and protocols are easily abused for nefarious purposes and yet such tools provide an essential aid for legitimate reasons. Correlation of online and offline surveillance data can generate new insights, provide sources for measurement and information useful to the development of products and applications.



The right to be forgotten should be explored through novel approaches such as improved anonymization techniques that are safe from abuses. Areas for investigation include advanced psychological profiling and automated risk evaluation.

3.3 RESEARCH ACTION #2 IMPROVED INFORMATION SHARING BETWEEN PARTIES WITH STANDARDIZATION OF PROTOCOLS AND LEGAL FRAMEWORKS AT LOCAL AND INTERNATIONAL LEVEL

DISTANCE TO THE MARKET: TRL 5

COST OF THE TOPIC: 3 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 3

TIME SPAN FOR ADDRESSING THE ACTION: 36 months

ACTORS: Law enforcement, industry, research, cyber security professionals, legal

Evidences show that cybercrime is under-reported with prevalent reasons given as confusion over where attacks should be reported and lack of trust in the body to which the report is made or in anything worthwhile resulting from the of reporting incidents.

An important action is to improve information sharing between parties from the ground level to those correlating the data and up the governments and other bodies where future decisions are made.

Areas for improvement include clarity of information sharing, differences and misunderstandings relating to privacy, traffic monitoring, data storage & analysis. What can legally be shared is important for advances in cyber forensics and the question of attribution.

3.4 RESEARCH ACTION #3 IMPROVEMENTS TO THE STABILITY AND SECURITY OF SYSTEMS USING STRONG, INNOVATIVE AUTHENTICATION METHODS, ENCRYPTION AND DIGITAL FORENSICS

DISTANCE TO THE MARKET: TRL 5

COST OF THE TOPIC: 4 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 36 months

ACTORS: Industry, research

Novel techniques and tools are needed to improve the stability and security of systems without compromising authentications. Building systems with standardized security measures with strong authentication and sanity checks adds resilience against attack. Additionally, more research is needed into how system access controls can be customised including modular approaches that are easy to administer.

Advanced encryption techniques are needed across all user bases. Currently attackers have higher levels of encryption than ordinary users who may not understand how, when or why encryption is needed.

Improved techniques that lead to attribution will advance security through enhancement of cybercriminal and cyberterrorist identification. Areas for investigation include malware reverse engineering, stylometry and linguistic obscuration. Defeating attacker obscuration with advanced digital forensics tools aids cyber intelligence on malware and attack tool behaviour and signatures.

Other areas for research include watermarks and fingerprints used in the prevention of anonymized data theft.



3.5 RESEARCH ACTIONS GANTT

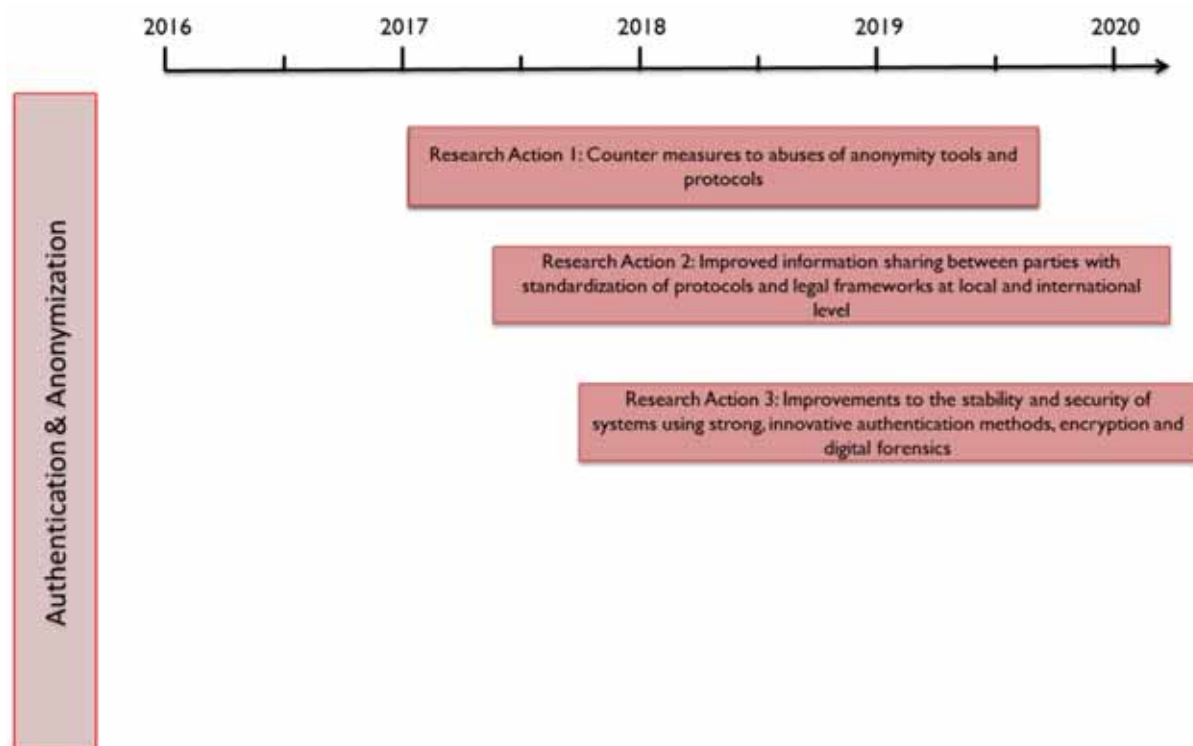


Figure 13 - Authentication and Anonymization RAs GANTT



4 BEHAVIOURAL SECURITY

CC RG-64 and CT RG-59	Novel techniques for access control that cannot be enforced through violence, real-time detection methods of attacks
CC RG-75 and CT RG-70	Next generation of analysis, fingerprinting tools with context
CC RG-78	Behavioural security
CT RG-18	Innovative process-aware behavioural-based intrusion detection system capable of identifying any deviation from normal activities for the processes being monitored
CT RG-77	Devise innovative technique for the detection of anomalous changes in the process activities and status
CT RG-80	Technologies to monitor and control the production process and detect deviations from acceptable behaviour

4.1 ABSTRACT

The widespread use of digital technologies in the private and working life of individuals led to a proliferation of online services that allow users to remotely store, access and share both personal and corporate sensitive data, from different physical places and from a variety of devices. This trend is re-shaping many aspects of individuals' life, such as people's working habits (e.g., through the bring-your-own-device - BYOD - policy) and healthcare services (e.g., automated collection of personal health data through wearable devices). Current authentication mechanisms for protecting the access to users' data, mainly based on passwords, are no more suitable to such novel usage scenarios, and to the corresponding security threats. This demands to strengthen current authentication systems, through:

- continuous authentication based on users' behaviour modelling and anomaly detection, for recognizing users' identity based on the dynamic and history of their interaction with a given service or device, as well as on the usage context
- no-password authentication techniques, like the ones based on biometrics, that can also be used together with continuous authentication

The behavioural security paradigm is also desirable in complex IoT-empowered systems, like industry and utilities, in which the increasing automatization opens the way to novel attack opportunities that cannot be properly dealt with using current signature-based detection techniques. In this context, behavioural approaches can enable the detection of anomalous changes in the normal activities of processes being monitored.

Additionally, behavioural analytics can also provide additional, useful tools to forensic investigators for cybercrime attribution.

4.2 RESEARCH ACTION #1 BEHAVIOURAL USER AUTHENTICATION AND NO-PASSWORD SYSTEMS

DISTANCE TO THE MARKET: TRL 4

COST OF THE TOPIC: 5 STREPs

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: universities, research institutions, online service providers, companies specialized in biometric authentication systems



Password-based user authentication mechanisms currently used in most online services exhibit well-known limitations, e.g., passwords are often easy to guess, they can be sniffed, revealed through social engineering (e.g., by phishing attacks), or automatically stolen by malware. Moreover, password-based solutions are suited to isolated systems, whereas the current landscape of digital technologies and their use cases (e.g., mobile devices, wearables, cloud computing, social media, BYOD policy) is increasingly made up of highly interconnected systems characterized by the possibility of accessing different kinds of online services from different devices and with different delivery models. It is therefore necessary to strengthen current authentication systems and access policies. To this aim, the behavioural paradigm is the most promising one. Behavioural authentication is based on exploiting several, soft identity cues related to users' behaviour in accessing and using online services, possibly taking into account also the usage context. In particular, the following issues need to be addressed:

- developing continuous authentication systems based on the analysis of users' behaviour, exploiting different "input signals" or "pieces of evidence" including, e.g., soft biometrics like keystroke dynamics, and contextual factors like the specific service being used, the device used to access it, and user's location
- developing anomaly detection techniques based on the history of past interactions and on behavioural analytics to detect suspect deviations from normal user activities, as cues of compromised accounts or systems
- developing fuzzy logic and machine learning techniques to effectively combine the different authentication signals
- securing users' behavioural data collected for authentication purposes against the risk of being in turn stolen or misused
- exploiting behavioural analytics in forensic tools as a further source of evidence for cybercrime attribution

No-password authentication systems based on biometrics can also be used in certain application contexts, possibly in combination with behavioural-based, continuous authentication. Current biometric authentication systems are however not yet mature for a widespread adoption; further research is needed to address issues like the following:

- performance improvement in uncontrolled environments
- security improvement against "spoofing" attacks, that consist of using falsified biometric traits

4.3 RESEARCH ACTION #2 BEHAVIOURAL ANALYTICS FOR *IoT*-EMPOWERED SYSTEMS

DISTANCE TO THE MARKET: TRL 4

COST OF THE TOPIC: 4 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 3

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: universities, research institutions, industries

IoT and related technologies are deeply transforming the industry, infrastructure and utility landscape. For instance, industrial production processes are evolving toward the Industry 4.0 paradigm, that exploits the benefits of cyber-physical systems and the Internet of Services, beside IoT. The Just-in-Time-Production paradigm is also going to transform factories into a network of highly-interconnected, decentralized and self-organizing "smart" devices, in which the IoT trend will play a leading role. Similarly, increasing automation and remote, centralized control systems are being adopted in utilities (e.g., for water process management). Beside their benefits, such technologies also offer new opportunities of attack to cybercriminals and cyber terrorists. For instance, the lack of authentication features in most used control systems protocols allow intruders to access and compromise control processes, forcing field equipment to misbehave.

Current security solutions mostly rely on signature-based IDSs, which aim at detecting attacks by recognizing specific patterns in network data streams or process behaviour. They are however doomed to fail in scenarios like the ones above, due to the increasing sophistication and customization of future attacks.

Future solutions to enforce security have to include strong authentication schemes, access control systems and improved attack detection systems. To this aim:

- behavioural analytics solutions based on anomaly detection approaches are required, to exploit their ability to detect deviations from a baseline behaviour, thus naturally including unknown and previously unseen attacks



- such solutions must be capable of continuously monitoring utilities and industrial processes, detecting suspicious activities that can be due to attacks (e.g., changes in the manufacturing process and activities), as well as detecting compromised components
- solutions to limit the number of false alarms, which is a drawback of anomaly-based techniques, have also to be developed
- behavioural analytics can be exploited in forensic tools also in the above contexts, as a further source of evidence for cybercrime and cyber terrorism attribution

4.4 RESEARCH ACTIONS GANTT

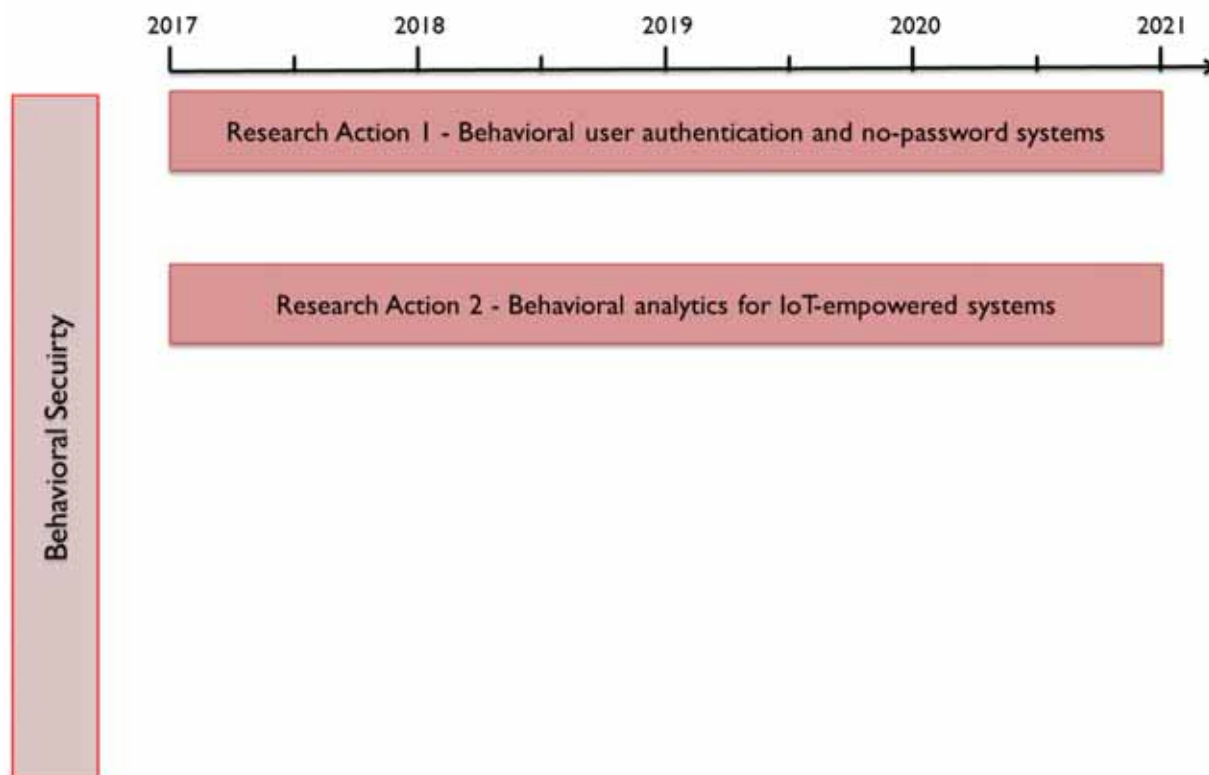


Figure 14 - Behavioural Security RAs GANTT

5 CRYPTOGRAPHY AND PUBLIC-KEY INFRASTRUCTURES (PKIs)

CC RG-11, CC RG-13, CC RG-85 and CT RG-8, CT RG-12, CT RG-76	Strong and efficient cryptographic primitives for low-end embedded devices and sensors
CC RG-15, CC RG-25, CC RG-26 and CT RG-25, CT RG-26	Simple and efficient key distribution mechanisms and Public-Key Infrastructures
CC RG-66, CC RG-03 and CT RG-61, CT RG-83	Preserving future resilience of encryption and authentication schemes

5.1 ABSTRACT

This document summarizes main research gaps regarding cryptographic protocols as well as key distribution and management schemes in order to ensure appropriate levels of security in future technologies. In particular, due to the massive deployment of low-end devices, either in the form of ‘smart’ Internet-of-Things technology or as sensors to make up Industry 4.0 infrastructure, a new class of lightweight crypto primitives is required. They must adhere to new requirements such as low energy consumption, minimal hardware footprint and easy synthetization in hardware. Securing vastly deployed devices is of utmost importance as they are considered as the building blocks of upcoming technological trends such as smart city, car-to-X scenarios and more. Furthermore, technologies to distribute and manage cryptographic keys in a way that allows for efficient scaling and preserves the security of the overall system are required for secure interaction with distributed devices. Lastly, those schemes and cryptographic primitives must provide sufficient usability for the end-user and further must remain resilient against attacks in the future. Thus, post-quantum secure encryption and authentication schemes must be considered.

5.2 RESEARCH ACTION #1 DEVELOPMENT AND SECURITY ANALYSIS OF LIGHTWEIGHT ENCRYPTION AND AUTHENTICATION SCHEMES AS WELL AS HASH FUNCTIONS FOR LOW-END MOBILE DEVICES.

DISTANCE TO THE MARKET: TRL 6

COST OF THE TOPIC: 2 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 18 months

ACTORS: Research Institutions, Industry, Policy-makers

New lightweight cryptographic primitives must be found, including encryption schemes, hash functions as well as authentication schemes that are optimized towards area, energy consumption, throughput as well as latency.

With mobile devices becoming smaller, the importance of minimized area consumption on the silicon (usually measured in Gate Equivalents, GEs) is growing. If future cryptographic primitives do not meet the requirements of industry and the markets, security levels of mobile devices will decrease or cryptographic means will not be implemented at all.

Considering the vast amount of mobile devices that will be embedded in various elements of everyday life, energy consumption of each individual device will become a critical factor. Thus, it is reasonable to consider the energy consumption imposed by cryptographic elements and subsequently optimize them towards low-energy.

With low-end devices being used as sensors and actuators in industrial facilities, the importance of low latency in the context of real-time operations is increasing.

While some candidates exist for block ciphers, i.e. PRINCE, KATAN, SIMON and SPECK that are optimized towards area and speed, there is a lack of comparative studies as those block ciphers have been implemented using different technologies. Thus, common test cases with identical interfaces must be established, as already proposed by the ECRYPT project. Further, although there are first efforts towards



proving security of lightweight ciphers, it is an open question to what extent they are vulnerable against side-channel analysis. Especially in the case of using low-end devices (such as sensor node in the context of smart cities), these devices will be likely much more physically exposed compared to current device classes, which makes them more vulnerable against side-channel attacks. Also, considering that devices are sending sensor measurements in order to control parts of the infrastructure of a smart city, integrity and authentication of the sensor values will become an important security objective. Thus, authenticated encryption (i.e. AES-GCM/ AES-GCC) must be examined towards its compatibility with resource-constrained devices. Subsequently, the implementation of secure and lightweight cryptographic primitives in mission-critical low-end devices must be guaranteed by defining standards, policies and/or laws.

5.3 RESEARCH ACTION #2 SCALABLE KEY DISTRIBUTION AND MANAGEMENT SCHEMES FOR SECRET-KEY BASED CRYPTOSYSTEMS AND NETWORKS WITH HIGHLY DYNAMIC TOPOLOGIES.

DISTANCE TO THE MARKET: TRL 7

COST OF THE TOPIC: 2 STREPs

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 12 months

ACTORS: Research Institutions, Industry

Considering the vastly growing numbers of embedded devices, that will be part of smart cities, the smart metering grid of the future and industrial facilities as well as those which will be used as wearables and in the context of the quantify-yourself trend, a critical point in maintaining security of those devices is whether one would be able to efficiently distribute and maintain cryptographic keys and certificates. From the perspective of the end-user, complex systems like PKIs must be made transparent and understandable. Nowadays, most often PKI-based errors are ignored which corrupts the PKI and its security properties as a whole. Thus, the PKI must be appropriately used and trusted by all users in order to make it work. Additionally, maintenance of Registration Authorities must be made easy enough for human operators. Interesting questions arise when considering the scenario where a hardware device (i.e., smart grid) must be rekeyed due to compromise of the private key, such as how to choose a methodology or standard according to which the party that revokes or re-certifies the device can be authorized. Also, there remain open questions regarding large-scale revocation, i.e., in case of a compromise of a CA that is responsible for a complex PKI.

Furthermore, with mobile devices forming networks with highly dynamic topologies, i.e. Vehicular Ad-Hoc Networks (VANETS) or mesh networks, new approaches to distributing, updating or revoking keys are required. Additionally, considering the autonomous sensor networks which lack a central coordinating instance, traditional PKI-based approaches or hierarchical Key Management Systems in general are not applicable.

Regarding highly resource-constrained devices that usually only support symmetric key cryptography, there are open research challenges with respect to key distribution approaches that scale sufficiently.

5.4 RESEARCH ACTION #3 DEVELOPMENT AND EVALUATION OF (LIGHTWEIGHT) QUANTUM-RESISTANT ENCRYPTION AND AUTHENTICATION SCHEMES AS WELL AS DIGITAL SIGNATURES.

DISTANCE TO THE MARKET: TRL 4

COST OF THE TOPIC: 2 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: Research Institutions, National Institutions

In order to preserve security provided by encryption schemes in the future, it is not sufficient to rely on encryption schemes whose security is based on hardness assumptions. Rather, the (currently theoretical) construction of a quantum-computer must be considered, as its realization would make obsolete any cryptosystem that bases security on the hardness of factoring integers or the discrete-log problem. Thus, finding post-quantum secure (PQS) encryption and authentication schemes as well as hash functions are subject to current research.

Numerous subsequent questions arise, such as whether potential PQS cryptosystems are efficient enough



to be used by highly-occupied systems (i.e., webserver or resource-constrained devices such as IoT platforms or wireless scenarios. Currently the public keys of PQS systems are rather large. Generally, as for any cryptosystem, trust must be established in potential PQS candidates by providing security proofs or conducting extensive cryptanalysis. The same holds for other cryptographic primitives such as digital signatures. This challenge also asks for new security models and exhaustive studies of the underlying algorithmic problems in general. Furthermore, there is a lack of knowledge regarding the resistance of PQS schemes against side-channel attacks due to the limited number of actual implementations, in software as well as hardware.

Another important aspect with respect to PQS schemes is the complexity of their implementation. As many crypto-related security incidents of the past suggested, the secure implementation of a theoretically secure cryptographic system often is the weak point. Finally, in order to make actual usage of quantum-resistant cryptosystems they must provide sufficient usability such that the average end-user is able to interact with it conveniently. Without broad user adaption such algorithms will remain theoretical concepts that do not contribute to actual security in our digital communication.

5.5 RESEARCH ACTIONS GANTT

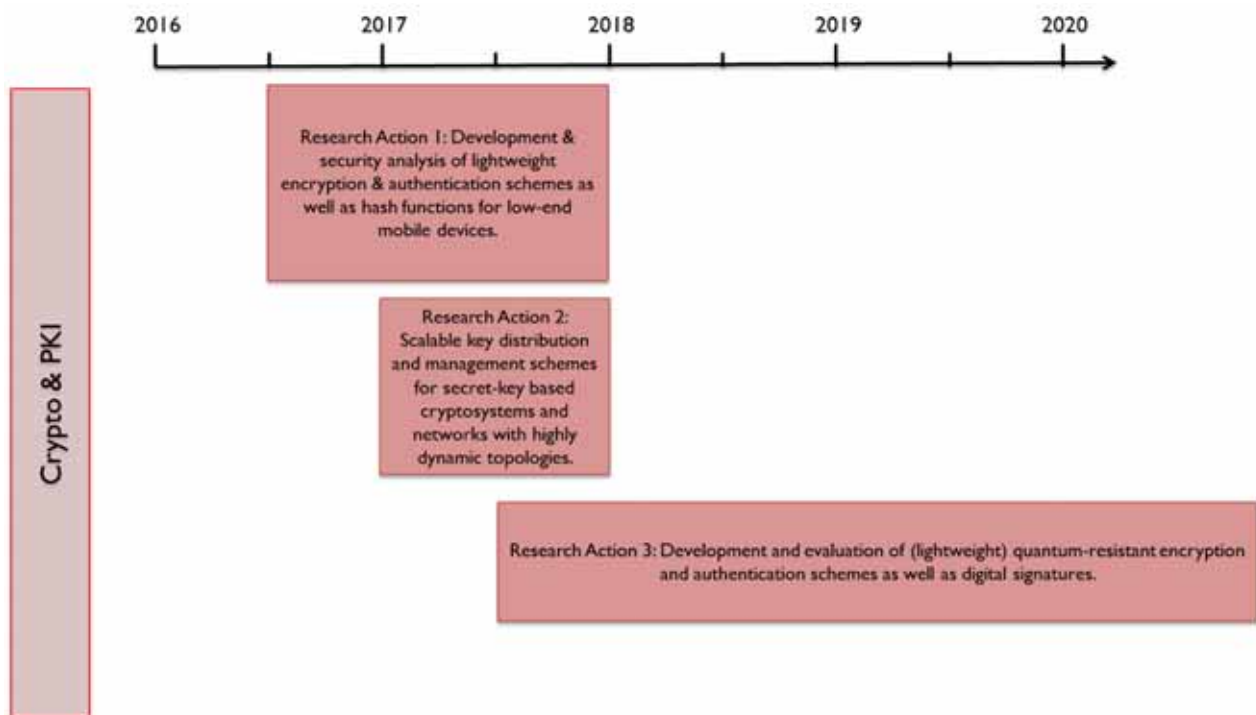


Figure 15 - Cryptography and Public-Key Infrastructures RAs GANTT

6 CYBERCRIME AND THE ECONOMY

CC RG-68	Research on cybercrime economics is patchy and requires more standardization with better practices and accountability
CC RG-69	Analysis of the threat that can be generated e.g. by new markets driven by crypto currencies

6.1 ABSTRACT

Better industry practices and accountability can help advance our knowledge of the economics of cybercrime. Knowing the true extent of the problem enables governments to budget for cost-effective measures that are fit-for-purpose. This includes the need for better prevention, detection, and application of security measures as a result of purposeful and productive research. Improving trust in the data comes from the provision of quantifiable metrics supplied by reliable sources using standardized methods that are benchmarked within the industry.

Benchmarking provides the means for a framework of accountability, whereby practices can be measured according to industry standards, and the capacity to introduce a regulatory system with managed powers of enforcement. It is already established that a barrier to the reporting of cybercrimes is a lack of trust in existing law enforcement in addition to low prosecution rates by the police. An industry based regulatory framework provides an alternative for victims to be supported, a method for action against the perpetrators and a focal point for the reporting of cybercrime.

The introduction of regulatory systems at an early stage of a newly developing cryptocurrency economy would benefit the process of cyber threat analysis and contribute towards greater accuracy in data evaluation. A system of structured regulatory measures with established cyber threat control mechanisms in place helps promote the type of environment in which an emerging cryptocurrency economy can confidently grow. An additional level of assurance is provided for consumers and the advancement of trusted and safe environments leads to the conditions in which new crypto-markets are able to flourish.

6.2 RESEARCH ACTION #1 PROVIDE A FRAMEWORK FOR THE AGGREGATION OF TRUSTED AND RELIABLE DATA ON THE COST OF CYBERCRIME

DISTANCE TO THE MARKET: TRL 3

COST OF THE TOPIC: 4 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 30 months

ACTORS: Industry, Standardization Body, Research Institute

What cybercrime actually costs is not yet known. Reliable data is essential for policy-making and revenue allocation from the top (governments) downwards (individual stakeholders) in order to meet the challenges of the future.

Challenges that need to be met in order to achieve this include resolving issues of trust, confusion over definitions of cybercrime, unreliable data sources, a lack of standards and benchmarks, and better information sharing.

Improved trust is co-dependent upon resolving current issues. Building upon The Budapest Convention on Cybercrime, the only international treaty to-date on cyber (enabled) crimes, would provide a first step to better definitions.

Improved methods of measurement of cybercrime for costing purposes is reliant upon the availability of accurate data. Who should provide this data and what steps are needed to ensure its accuracy?



The lack of international standards and benchmarking in the cyber security industry undermines efforts to provide consistency of data. Fast-paced innovations eclipse the processes of traditional standard-setting; fit-for purpose practices are needed.

Confusion over where and how to report cyber-attacks means incidents are under-reported which acts as an impediment to rigorous data analysis. Cross-border offending obstructs police action and adds to already low reporting rates of cybercrime.

In future scenario governments, boards and individual stakeholders can have a high level of awareness of the value of data. This is achievable through mandatory reporting of cybercrimes to a trusted entity with the data used to provide accurate analysis of the true cost of cybercrime.

6.3 RESEARCH ACTION #2 IN DEPTH THREAT ANALYSIS AND STUDY OF PREVENTATIVE MEASURES ON THE TOPIC OF CRYPTOCURRENCIES.

DISTANCE TO THE MARKET: TRL 4

COST OF THE TOPIC: 5 STREPs + 0 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 36 months

ACTORS: Industry, Research Institute

Different challenges are both presented and provided as new markets emerge to meet the needs of an evolving digital era. The rise of cryptocurrencies offers opportunities for better defences driven by advanced encryption and good entropy within the random number generation process.

Anticipating future threats arising out of cryptocurrency technologies is a pre-requisite with actions needed such as the early introduction of a regulatory framework for cryptocurrency operators and exchangers, which can limit the advance of decentralization.

Cybercriminals can use the lack of industry standards and best practices to their advantage as evidenced in the current situation where the true extent of cybercrime is still unknown. A framework for industry regulation of the cryptocurrency industry at an early stage of its development would ensure that challenges are faced as they unfold.

Early cross-border agreement on cryptocurrency regulations would bring legitimacy to developing systems evolving out of the virtual market. The anonymity afforded by cryptocurrencies is attractive to cybercriminals: regulation can help limit the fraud and help protect consumers.

In a future scenario cryptocurrencies are an essential feature of a vibrant economy that is trusted and secure. A regulatory framework provides a level of assurance for consumers using cryptocurrencies across a range of devices. Fraud is controlled through a number of fit-for-purpose defences aided by the provision of accurate data from trusted sources operating within a legitimate regulatory system.



6.4 RESEARCH ACTIONS GANTT

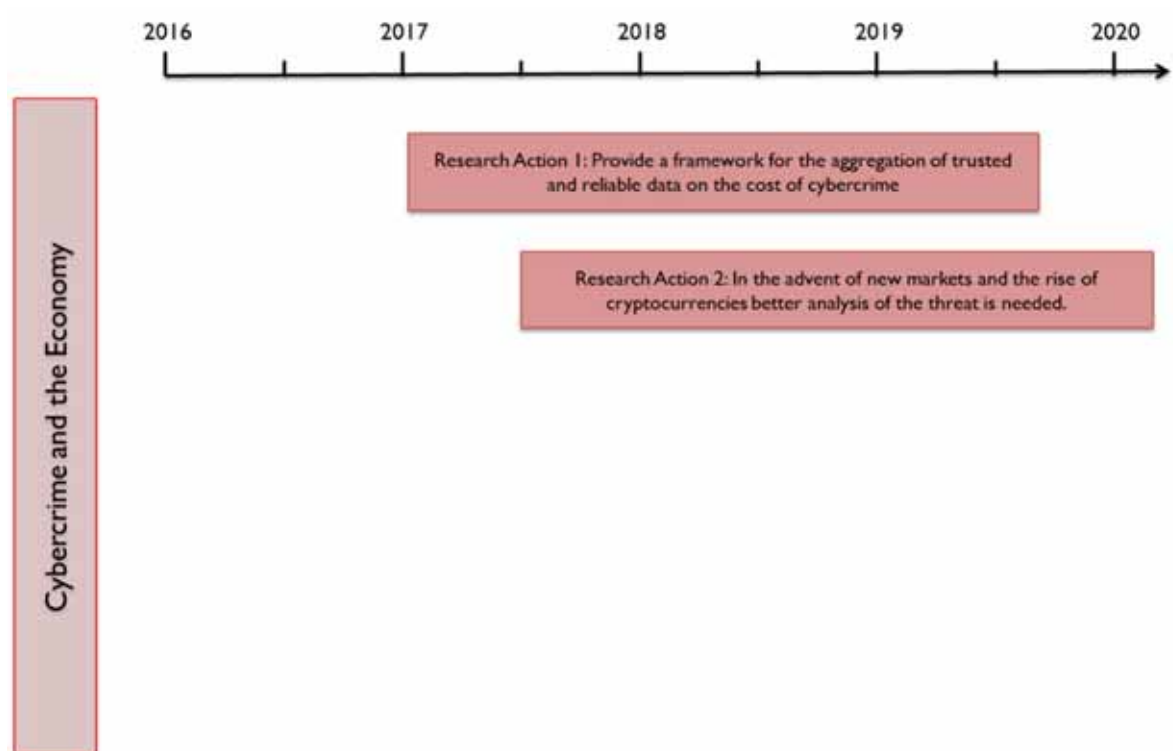


Figure 16 - Cybercrime and the Economy RAs GANTT

7 FORENSICS

CT RG-58 and CC RG-62	There is a huge research gap regarding database forensics in general, especially considering the detection of manipulation by users with higher privileges and even database administrators.
CT RG-71	Intelligence has access to great volume of information but lacks of tools to identify the most meaningful
CT RG-72	Research on cyberterrorism motivations/root cause
CT RG-79	Improve Incident Response
CT RG-93 and CC RG- 98	Methods for forensics and crosschecking. Methods for assessing the sensitivity of data aggregates and linked data sets.
CC RG- 101 and CC RG-103	Watermarks and Fingerprints that cannot be spotted easily and is resilient to collusion attacks and inferences.

7.1 ABSTRACT

Digital Forensics is often solely associated with the areas of attribution in the aftermath of a cyber-attack, as well as the discovery of hidden and the restoration of deleted files, either due to malicious attempts or simply because of errors by a legitimate user.

Still, digital forensics possesses many aspects that are not covered by current large-scale research and could be useful in order to thwart acts of cyberterrorism and cybercrime. Efficient methods for enabling cheap and fast digital investigations could not only lead to a much faster attribution of attacks with subsequent countermeasures (reactive, as well as proactive with respect to follow-up attacks), which would in itself be a valuable issue in order to reduce the expected motivation and increase the danger for cybercriminals. Accessible forensic methods could also be used in order to even detect attacks, especially considering instances of data and system manipulation. With respect to data theft and industrial espionage, methods for data leak detection and comprehensive audit & control mechanisms could help reduce the danger of espionage and exfiltration attacks by making the data thief more easily detectable.

Digital forensics and its methods is always considered to be a mixed blessing, blurring the line between rightful and lawful investigation and the protection of user rights. This is especially important in case of comprehensive auditing of access patterns and employee work: Here, research into the harmonization of European law will be needed, allowing for solutions that provide a certain level of detection of data theft and manipulation, as well as protecting the privacy of the innocent. While this legal work is of course of great importance, it needs a strong relation to technological research in the area of digital forensics, in order to make laws that can be related to the technological reality.

With the advent of cheap sensors that allow the wide adoption of new paradigms like IoT, new challenges for forensic methods have appeared: Opportunistic networks and ad hoc connections increase the difficulty of forensic investigation drastically. Still, new technologies in the area of machine learning and data mining will also open up new doors with respect to real-time forensics (live forensics) based on patterns and behaviour. Furthermore, the introduction of principles like industry 4.0 and personalized/participatory medicine introduced completely new classes of equipment and environments that need new solutions: For example, industry lanes might not be capable of shutting down several days for an investigation as it is currently done in the more traditional IT-world, without causing huge losses.

Summarized, the introduction of new technologies poses a large amount of new challenges to the field of digital forensics, which need further development in order to answer these challenges.

7.2 RESEARCH ACTION #1 FORENSIC METHODS FOR BIG DATA.

DISTANCE TO THE MARKET: TRL 2

COST OF THE TOPIC: 3 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 36 months

ACTORS: Big Data providers, LEAs, Machine Learning specialists, Security experts

Big Data is one of the major emerging topics of the last years, especially considering the multitude of related issues: Big sensor networks in the IoT-world that generate large amounts of data in real time with complex linkage, as well as data driven science and economy, ranging from biomedical research in the area of personalized medicine based on genomics to providing added services in large industrial environments within the new industry 4.0 paradigm.

Manipulations of such big data streams are currently very hard to detect, especially in case of unspecified sources. Here, machine learning algorithms can help to detect changes in the delivered data, or irregularities in the data provisioning.

Another big challenge for data driven environments with respect to Privacy is the question on detecting (singular) sensitive data particles within the large amount of data. This is especially important in environments where the data is not derived by one or a few well-defined sources, but rather form an agglomeration of data provided by different sources with variable content. In case of overlapping source information, this can pose even more important questions, as most anonymization strategies in use are susceptible to de-anonymization through collusion attacks, i.e. the anonymization can often be endangered by aggregating different versions of the same data set. Thus, in order to pursue the goal of guaranteeing the protection of sensitive data, we propose to use machine learning techniques that are able to 1) detect sensitive information in large data streams and 2) rate the combination of different data sources with respect to linkage possibilities.

7.3 RESEARCH ACTION #2 LIVE FORENSICS, AUDIT & CONTROL.

DISTANCE TO THE MARKET: TRL 7

COST OF THE TOPIC: 2 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 32 months

ACTORS: industry, IoT-experts, Security experts

Traditional forensic investigations are set up as ex-post analysis in post-mortem or post-incident investigations, often based on a detected or assumed irregularity in the system. This approach comes with some deficits with respect to the new environments introduced within the industry 4.0 paradigm or large IoT-structures:

1. The analysis happens ex ante, i.e. the damage is already done. Modern environments need the detection of attacks and manipulations to be much faster, in order to avert damage. A possible improvement is the development of methods for generating a complete and reliable overview on the health status of each endpoint in the system.
2. Typically, the system under investigation is either shut down for normal operation, or an exact copy of the system is generated, where the analysis is then conducted on. Both approaches are completely unfeasible in more complex production systems, as a shutdown of the system typically results in large financial damages, in case of some applications like steel furnaces, even in a complete shutdown of the factory. On the other hand, since large IoT or industrial systems are extremely expensive and highly proprietary in nature, the production of an exact copy is not feasible.

Based on these problems, forensic investigations need to enable infrastructure owners to efficiently monitor their systems and conduct forensic investigations directly on the running system.

Thus, the results of this research action shall include:

- The development of modern audit & control applications that monitor the overall health status of systems, including access to resources and system components. This also includes the development of working solutions that can be introduced into standard of the shelf IoT-structures.



- The development of tools and processes for introducing live forensics into industrial environments, i.e. enabling the forensic analyst to analyse complex systems without shutting them down: critical information needs to be protected in order to be used during the analysis, while the investigation process must not interfere with the system stability. This will also include methods for efficiently generating forensic clones of industry systems.

7.4 RESEARCH ACTION #3 FORENSICS IN MOBILE AND DISTRIBUTED ENVIRONMENTS.

DISTANCE TO THE MARKET: TRL 5
 COST OF THE TOPIC: 4 STREPs + 2 IP
 AVAILABILITY OF COMPETENCE IN EUROPE: 5
 TIME SPAN FOR ADDRESSING THE ACTION: 36 months
 ACTORS: mobile services providers, Industry, IoT-Provider

With the rise of smartphones, mobile platforms gained increasing popularity, which also had drastic effects on the area of forensics: nowadays, these devices are one of the main targets during forensic investigations, often in course of analysing traditional scenarios of crime and terrorism (see also the discussion regarding decryption of iOS-based devices by the FBI).

Still, there are many technological issues to overcome, especially with respect to the new device-side encryption technologies that are currently increasingly implemented. While the smartphone arena is receiving increasing attention, the widespread implementation of IoT-devices like integrated sensors relates to new issues in the area of forensics: due to some features characterizing opportunist ad-hoc networks (e.g., energy saving and mobility of the sensors) traditional methods for network forensics, as well as network observation, are not suitable anymore. Thus, a key step of future research concerns the development of new techniques that allow to analyse the network structure at the exact time when the attack was carried out, even during an ex-post analysis, including monitoring features and the possibility to gather all network changes.

One of the main issue in mobile forensics lies in the area of legal exploitability: while many techniques exist that can be used in order to gain forensic information on system manipulation and disruption, close to none of them hold in front of court. Most often the problem lies in the complexity of the forensic tools and methods at hand that make the trustworthiness of the gathered results hard to determine, i.e. whether the evidence was not fabricated by the forensic investigators. Thus, it is of paramount importance to develop technologies, processes and especially tools that fulfil all the legal requirements in order to be acceptable as proof in front of court.

Following these principles as much as possible during forensics will diminish incidents regarding the authenticity of evidence, and augment the transparency of the whole forensic process.

7.5 RESEARCH ACTION #4 DATABASE FORENSICS AND DATA LEAK DETECTION.

DISTANCE TO THE MARKET: TRL 5
 COST OF THE TOPIC: 4 STREPs + 2 IP
 AVAILABILITY OF COMPETENCE IN EUROPE: 5
 TIME SPAN FOR ADDRESSING THE ACTION: 36 months
 ACTORS: Security researchers, data driven domains, industry 4.0, big data analysts

The large data dependent systems that are currently in use everywhere are unimaginable without the use of databases. Most of the data stored in all kinds of applications and systems is stored in some kind of database management system (DBMS). Furthermore, data has become a resource and thus a (monetary) asset in many modern, often service driven, environments: starting from research labs in the bionics sector up to data driven industrial services, data nowadays not only needs protection due to privacy concerns, but simply as a valuable resource.

Data manipulation and data theft are therefore important attack vectors for cyberterrorists and cybercriminals respectively. While for data stores on file systems bases there exists a multitude of different approaches for manipulation detection, file recovery and other techniques typically utilized during a forensic investigation, the field of database forensics has been left rather unattended during the last decades.



Furthermore, most recent works solely concentrate on attacks carried out by “normal” users or even outsiders, missing attacks that are carried out by an administrator, either due to a malicious insider, or in the course of stolen credentials through either a previous technical attack or social engineering. These attacks are far more dangerous, since database administrators typically have the possibilities to conceal their tracks (e.g. in log files and audit mechanisms) effectively and can stay undetected for a very long time. Another issues lies in the release of data sets in order to conduct joint projects with other (often industrial) partners. As this data is only shared for a certain cause with a strictly limited amount of partners, it must not be passed on. While passing on might not be an issue with respect to privacy, even insensitive data (e.g. sensor measurements) can possess a huge value. Thus, methods that allow to detect leaking parties even in case of incomplete data sets are needed. Current approaches typically rely on the introduction of marker data that either introduces slight errors in case of analysis, which can cause problems in case of data driven analysis, or rely on finding large portions of the leaked set. The aim of this action is to develop techniques for quick and unambiguous detection of data leaks based on single records or attribute subsets.

7.6 RESEARCH ACTIONS GANTT

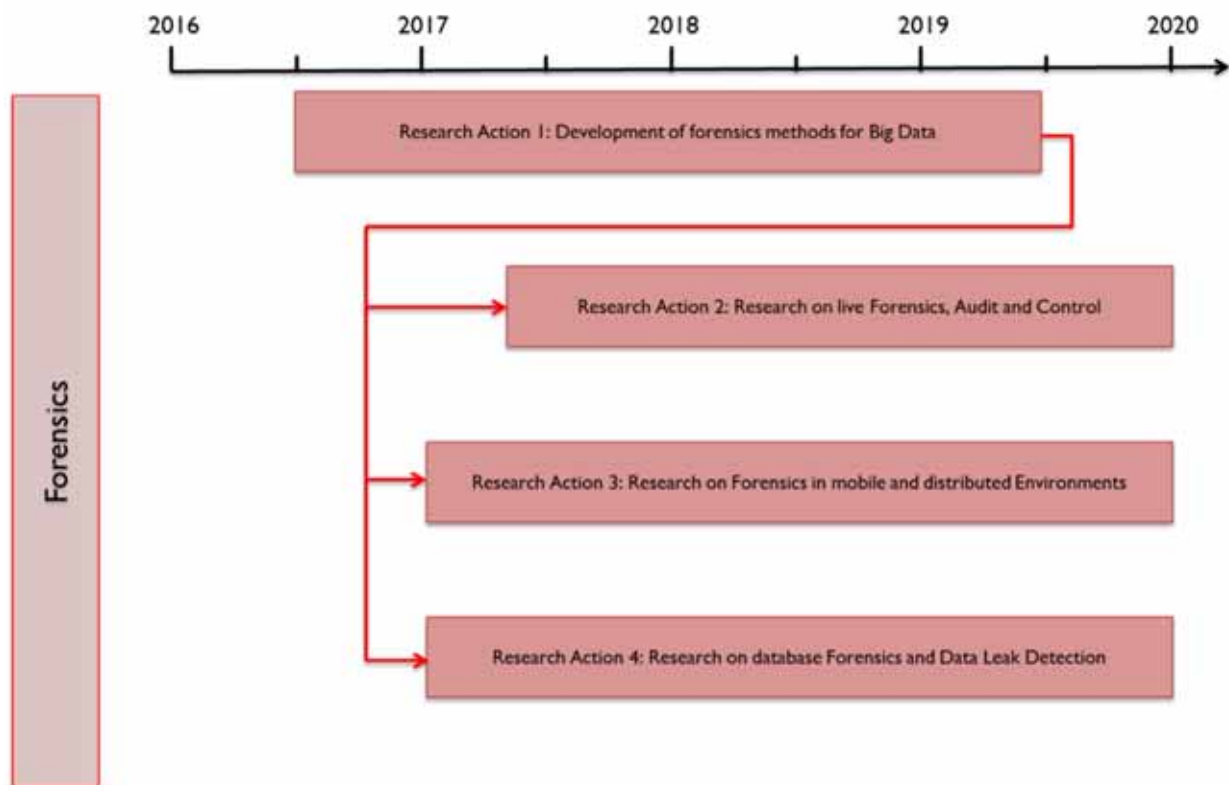


Figure 17 - Forensics RAs GANTT

8 HEALTHCARE

CC RG-55 and CT RG-55	Better harmonization of health care protocols and better testing of existing solutions against security (also using Secure Software Development Solutions) against real and modern threats.
CT RG-57	New ways to protect health records that goes beyond encryption and access control. Monitoring solutions that can track the data either in storage and transmission and detect misuses, breaches and deny of services.

8.1 ABSTRACT

Healthcare is increasingly becoming a service-oriented ecosystem. This is based on solid market trends in the wearable industry, social needs of an ageing society and economic sustainability of the healthcare services.

The digital revolution of healthcare started several years ago with the introduction of informatics into hospitals. Nowadays, healthcare operators and patients' worlds are definitely highly digitalized, modifying how healthcare operators and patients offer and use services respectively. Since a few years, healthcare is migrating to an ecosystem logic which consists in the evolution of the hospital, typically seen as a physical place of care, to a distributed network of services for patients, provided in home environments through different channels and technologies. Today's most common style of living in the western-world is to blend working and private lives, largely using digital ecosystems in which personal and professional services coexists and exchange data. One of the most important challenges for healthcare is hence to evolve its services to match these new societal trends. Furthermore, Cybercriminals are adopting corporate best practices and establishing professional businesses in order to increase the efficiency of their attacks against enterprises and consumers. This also implies a major rethink of most of the security solutions adopted in the past years in healthcare.

Today, healthcare is one of the most attacked and promising areas of exploitation for cybercriminals and cyberterrorists due to the overabundance of valuable information and for its nature as a critical infrastructure. The modern healthcare ecosystems can be abused in different ways. As a matter of fact, hospitals became incrementally digitalized often with complex and still largely unsolved security problems, tied to the standards used, the lack of harmonization of services and problems with different roles in the hospitals and harmonizing laws among different countries (especially in Europe). On the other side, advanced attack techniques are becoming extremely flexible, ready to catch all the possible economic advantages.

The solutions for these trends are complex because the problem does not only involve the owner of the data (the user) and the official handler (the health services), but also external actors (e.g. insurances), in some cases also based in foreign countries (e.g. companies selling health monitoring services through wearable bracelets, which are hosting data abroad).

8.2 RESEARCH ACTION #1 BETTER HARMONIZATION OF HEALTH CARE PROTOCOLS AND BETTER TESTING OF EXISTING SOLUTIONS AGAINST SECURITY (ALSO USING SECURE SOFTWARE DEVELOPMENT SOLUTIONS) AGAINST REAL AND MODERN THREATS.

DISTANCE TO THE MARKET: TRL 3-4

COST OF THE TOPIC: 3-5 STREPs + 3- IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 42 months

ACTORS: healthcare operators, research centres specialized in security, security market leaders, healthcare device/solution providers, standardization bodies.

The cyber threats that evolved, as well as targeted attacks that appeared during the last few years, can be considered as one of the main worrisome trends, especially for high value organizations like hospitals. On



one side, the usage of proprietary solutions and the specificity of the used protocols (e.g., DICOM, HL7) kept specialized threats away so far (typically hospitals fell for opportunistic threats, not specifically created for healthcare). On the other side, the increasing number of targeted attacks allows to foresee a change of direction.

Due to the ground-breaking innovative and business driven approaches of latest attacks, most of the previously installed defence solutions do not suffice anymore. A new set of protection mechanisms, going under the names of “threat intelligence” and “analyst-driven solutions” appeared on the market. These mechanisms involve a mixture of human experts and Artificial Intelligence (AI) at different degrees. These new defence systems are often complex enough to require a service oriented approach (often offered as SaaS) and involve AI, trained by humans, where heuristics were used in the past (e.g. the future of antiviruses is foreseen to involve AIs more than heuristics).

Beside these problems, modern hospitals still suffer from another class of issues, that has been addressed for decades: the existing security standards in the eHealth world lack on-field testing against complex real world attacks. Standards specified by SDOs (Standard Developing Organizations) are in use and their robustness has still often not been proven against real modern attacks. After spending millions to upgrade and protect the existing hospital information services. new upgrades to face a completely new set of threats will become necessary. It is important hence to:

1. Protect the data along its whole lifecycle (creation, storage, transmission and destruction) and across all security relevant layers (network, application, device, physical, human).
2. Test the effectiveness of the new defence solutions in the healthcare world.
3. Coordinate and update the existing specific health standards with respect to latest trends and attack techniques.

8.3 RESEARCH ACTION #2 PROTECT AND TRAIN THE HUMAN CAPITAL.

DISTANCE TO THE MARKET: TRL 3-4

COST OF THE TOPIC: 2 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 42 months

ACTORS: healthcare operators, research centres specialized in security, security market leaders, healthcare device/solution providers, sociologists, cognitive scientists, psychologists, HCI experts, medical staff

Healthcare is one of the few critical infrastructures whose services could largely survive even in case of a big technological disruption: one of the most important assets of an hospital is the human capital (e.g., physicians and nurses) while technology's main role is to support and increase their overall efficiency. Technology must hence be protected and kept stable because, simplifying, it is the enabling factor through which the hospitals “serve” a large population, but very few energy has been devoted to the protection of people. Today's cybercriminals and cyberterrorists largely use Social Engineering tactics to exploit the human side of security: modern Social Engineering is the crucial step involved in almost all the attacks. This is especially critical, since data protection is not only a matter of privacy protection, but hospitals are increasingly depending on the availability of their data for their daily business of helping patients. With this background, the increasing danger of becoming a paying victim of ransomware is further increased. Thus, not only awareness on the users' side must be increased, but also on the side of HIS-developers,

Nevertheless, solving the problem of Social Engineering is not simple, since, beside the new defence technologies, the only available solution is “awareness”. However, generating awareness is still an open problem. However, it is recognized that the best approach should be based on a concrete and profound collaboration among different competences (e.g. psychologists, HCI experts, sociologists, medical staff, cognitive sciences, security experts, ...).

Nevertheless, the most interesting recipes for new awareness strategies in security are all involving the following three elements:

- Gamification: traditional ICT security trainings do not present particular appealing characteristics. In contrast, gamification frames such trainings as hacking games of different formats (e.g., attack-defence capture the flag, jeopardy), fostering competitiveness and promoting problem-solving activities.



- Incidental learning: partial yet continuous learning and knowledge improvement, for example through mini-sessions during the day, trying to avoid monolithic tracks.
- Personalization: adapt the learning experience to individuals' attitudes, habits and mind-sets.

The healthcare sector, more than others, is a special test area for improving awareness strategies, because of the specific mind set of healthcare operators which makes them particularly vulnerable to Social Engineering attacks. The natural predisposition of healthcare operators to support others (second opinions and collaborations are an everyday best practice in medicine), together with their continuous exposure to different technologies and at the same time their relatively low training in security, makes them the perfect victims of cyber threats.

8.4 RESEARCH ACTION #3 JUNCTION OF CYBER AND REAL THREATS.

DISTANCE TO THE MARKET: TRL 5

COST OF THE TOPIC: 4 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 42 months

ACTORS: healthcare operators, research centres specialized in security, Law Enforcement Agencies, security market leaders, healthcare device/solution providers

Cybercrime and Cyberterrorisms are converging to the same strategies and business models as traditional crime and terrorisms, thus resulting in an increased blending of cybercrime and crime and a commonality of interests between cyberterrorism and terrorism. What is starting to appear, in the evidences collected, is a multi-staged approach to threats and a coordination of efforts aimed at reaching a final goal: for example, disrupting the Hospital Information Services (HIS) through ransomware in conjunction with a terrorist attack, could be used to increase the ensuing social "chaos" and to reduce the hospitals efficiency when it would be needed most.

Healthcare is double exposed to these problems because of its nature as a critical infrastructure and the extreme value of its assets (the Personal Healthcare Information –PHI– and Personal Identifiable Information –PII–) for either citizens and the black market. It will be beneficial to investigate the exposure of the critical infrastructures and especially healthcare with respect to the following topics:

1. Conjunction of cybercrime and traditional crime, for example the increasing probability of cyber-murders through e.g. exploitation of life-support devices. The objective could be:
 - a. Investigation: understanding the economic and strategic plans of criminals and terrorists from an attackers' point of view.
 - b. Mitigation: fostering the adoption and adaptation of e.g. secure code development best practices at all the technological levels in healthcare and promoting official certifications in order to reduce the attack surface.
2. Coordination of efforts between cyber threats and terroristic acts in order to amplify the effects of a terrorist attack. Mitigation means:
 - a. Improving the investigation efforts and the inter-force coordination among LEAs and healthcare operators.
 - b. Further studying the possible blending of real and cyber threat models (either by an economic or strategic point of view).



8.5 RESEARCH ACTIONS GANTT

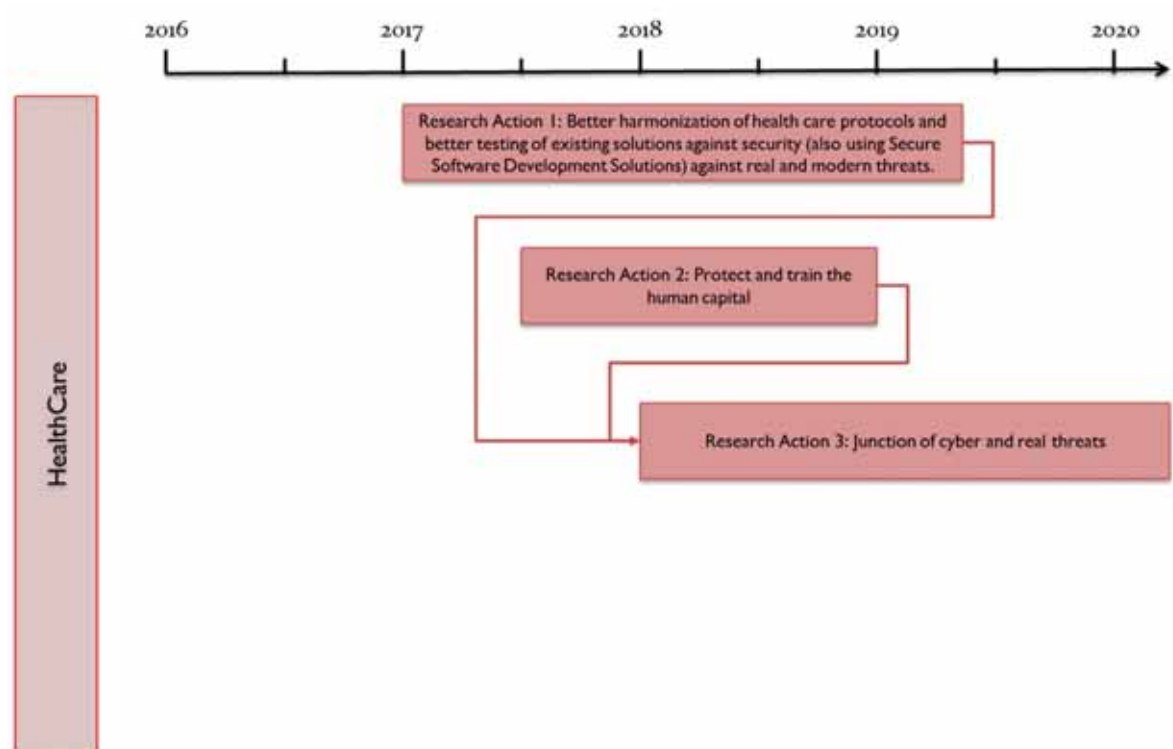


Figure 18 - Healthcare RAs GANTT

9 INFORMATION EXCHANGE

CC RG-51	Secure Signed Documents
CT RG-52	Secure Signed Documents
CC RG-52	Secure and Interoperable EDI
CT RG-82	How to engage operators/exchangers in information exchange
CC RG-34 and CT RG-34	Data mining for fraud detection
CT RG-53	Data analysis and Intelligence in customs brokerage
CT RG-54	Early detection of supply chain attacks

9.1 ABSTRACT

Electronic Data Interchange (EDI) is the process of electronic communication of formatted, structured data (documents, invoices, etc.). Through EDI, document and information exchange can be more secure and easy to monitor. Use of EDI can thus help combat crime such as fraud, tax evasion etc. Furthermore, there is an increased need for interoperable EDI that is certified to handle classified or sensitive material, often needed for information between law enforcement agencies, government, etc.

Although there is a multitude of Electronic Data Interchange solutions available in the market, they are based on a variety of different standards leading to a lot of fragmentation and thus creating barriers in the adoption of this technology. A multitude of businesses or organisations that require paper document handling fail to adopt EDI or are unwilling to change business processes. Furthermore, the cost of the initial setup of EDI solutions, the multitude of different standards and the cost of training employees to a new process also hinder the adoption of EDI. Thus, there is a pressing need for interoperable, easy to use and easy to deploy EDI solutions, for a variety of different stakeholders ranging from small business owners to government to military etc.

9.2 RESEARCH ACTION #1 HARMONIZATION OF INFORMATION EXCHANGE INCLUDING SENSITIVE AND CLASSIFIED ACROSS PUBLIC, MILITARY, PRIVATE AND ACADEMIC SECTOR.

DISTANCE TO THE MARKET: TRL 5-7

COST OF THE TOPIC: 2 STREP + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 42 months

ACTORS: government, law enforcement, customs, border guard, military, IT security industry, high-tech industry, research/academia

Information exchange is a critical factor for effective cyber security. Actionable information can be used by organizations to enhance their security measures, update their controls and protect by threats that have been recognized and identified elsewhere.

This saves time and effort and contributes to the improvement of the overall security posture. However, it is quite usual that such information falls under classification or sensitiveness rules that prevent further sharing with relevant stakeholders.

Specific operational requirements and communication channels have to be established in order to facilitate the information exchange process, overcome unnecessary approval constraints, and at the same protect any unintentional disclosure.

An official framework should be developed describing the specific content and context of cyber security information that needs to be shared across all relevant national and international stakeholders.



9.3 RESEARCH ACTION #2 COMBATING FRAUD AND THEFT IN FREIGHT TRANSPORT AND CUSTOMS BROKERAGE.

DISTANCE TO THE MARKET: TRL 5-7

COST OF THE TOPIC: 2 STREP + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: government, law enforcement, customs, border guard, IT security industry, freight forwarders, customs brokers, research/academia

Freight transport within and across borders is a vital part of modern economy. The high value of transported cargo makes freight forwarders an attractive target for cybercriminals who use illicit techniques and tools to enable crimes such as cargo theft, customs fraud, excise or VAT fraud, smuggling etc.

Furthermore, transporting cargo through international borders requires clearing through customs. The massive amount of documents and data that are processed through customs can lead to errors in handling and loss of revenue for importers/exporters who are fully exposed to this risk. Monitoring the vast amount of documents to detect suspected cases of fraud or smuggling, is a very difficult task and not sufficiently automated.

Thus, customs are vulnerable to ransomware and DDOS attacks that can disrupt normal operations and require intelligent, secure and interoperable solutions to handle and authenticate massive amounts of documents. Freight forwarders are often the victims of identity theft leading to cargo high-jacking, fuel fraud etc.

This action aims to combat cybercrime in freight transport by:

- Providing tools to prevent and detect identity theft,
- Providing tools to prevent and detect document forgery,
- Providing interoperable and mobile Electronic Data Interchange solutions and promoting their adoption,
- Enabling Real-time cargo tracking across different transport modalities,
- Introducing improved data analysis and intelligence in customs brokerage, and
- Ensuring that information flow is safe, secure and uninterrupted.



9.4 RESEARCH ACTIONS GANTT

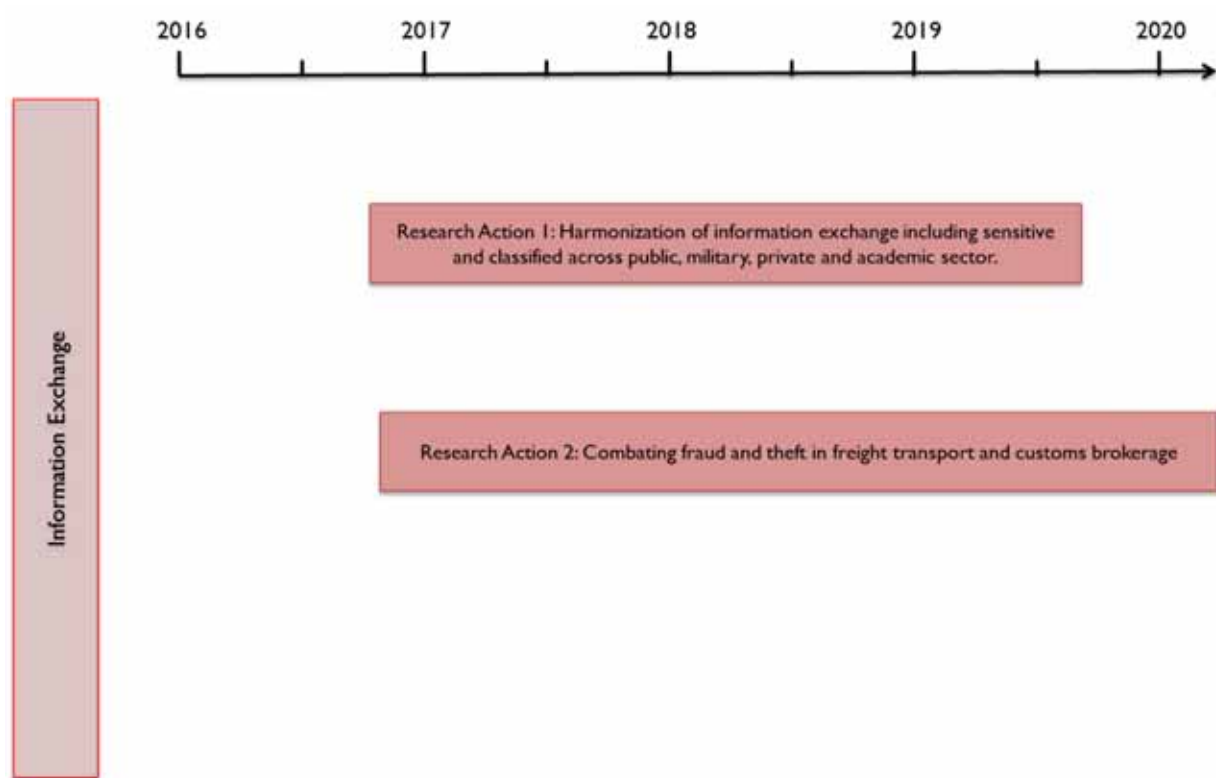


Figure 19 - Information Exchange RAs GANTT

10 LAW AND ORDER

CC RG-92	Training of law enforcement officers and legal authorities on laws relating to the new paradigm. Development of new laws and research on strengthening of old laws dealing with online cybercrime and cyber terrorism.
CC/CT LEG-6	Research to better understand how to extend the EU legal framework in response to cybercrime and, at the same time, preserve the privacy of the citizen.
CT RG-92	Research to better understand infrastructures on the Internet that support underground flow exchange of using online means.

10.1 ABSTRACT

The gaps identified by the social, economic political and legal research stream within Cyber ROAD are categorised within two clusters: social resilience and law and order. The following gaps have been prioritised for research action because they are representative of the three law and order main themes to emerge from the Cyber ROAD analysis. These three themes are: development of an integrated and well-coordinated global approach to fight cybercrime and cyber terrorism, privacy-aware tools and legal frameworks for cybercrime fighting and enhanced identification of internet-enabled money laundering practices at both the social and data network levels.

The research to develop an integrated and well-coordinated global approach to fight cybercrime and cyber terrorism is focused on the training of law enforcement officers and legal authorities to respond to cybercrime and cyber terrorism and the development of new laws and research on strengthening of old laws responding to cybercrime and cyber terrorism.

The research to develop an improved legal framework research explores the practicalities of developing and deploying a European cybercrime fighting framework. The research gap also examines the practicalities of remote access, develops improved methods of remote access to digitally stored evidence and analyses the tensions between individual privacy and the data access needs of the crime fighting agencies.

The research to enhance identification of internet-enabled money laundering examines the topic from both the social and data network perspectives and enhances the understanding of how money laundering is manifested on the internet and the social and technical infrastructures used to support internet-enabled money laundering.

10.2 RESEARCH ACTION #1 *DEVELOPING AN ENHANCED, INTEGRATED GLOBAL RESPONSE FROM CRIME FIGHTING AGENCIES.*

DISTANCE TO THE MARKET: TRL 3

COST OF THE TOPIC: 2 STREPs and 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: Law enforcement agencies, academics, law makers, government

This research action addresses the following research questions:

- What education programme is most effective in training law enforcement officers in responding to cybercrime and cyber terrorism?
- What is the structure and contents of the legal paradigm needed to respond to cybercrime and cyber terrorism?
- What are the effective means of communicating the new legal paradigm to law makers?

A research programme is needed to co-ordinate existing expertise and develop effective methods of



communicating the new legal paradigm to law makers so that prompt, effective legislation change becomes possible in every legal jurisdiction. This research action aims to develop an integrated and well-coordinated global approach to fight against cybercrime and cyberterrorism. It is focused on the training of law enforcement officers and legal authorities on laws relating to cybercrime and cyber terrorism, the development of new laws and research on strengthening of old laws dealing with online cybercrime and cyber terrorism. One of the main outputs of this research will be a new legal paradigm for responding to cybercrime and cyber terrorism. Research is necessary to determine the most effective way of teaching law enforcement officers so that their expertise in responding to terrestrial crime can be transformed into new expertise in responding to cybercrime.

Research is necessary to identify the new laws necessary to respond to cybercrime. In particular, research is needed to build a picture of the new legal paradigm necessary to respond to cybercrime and cyber terrorism, examine where the new legal paradigm converges and diverges from the current legal paradigm and identify gaps in legislation that is necessary to respond to cybercrime and cyber terrorism. As part of the design of the new legal paradigm, the conceptualization of legal jurisdiction will need to be examined.

This research action comprises the following stages:

- 1) Review of current legal paradigm and gap analysis of capabilities in the context of cybercrime and cyber terrorism.
- 2) Stakeholder consultation as input to the design of new legal paradigm
- 3) Public policy updates and proposals

10.3 RESEARCH ACTION #2 ENHANCEMENT OF THE EUROPEAN LEGAL FRAMEWORK.

DISTANCE TO THE MARKET: TRL 1

COST OF THE TOPIC: 2 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: Crime fighting agencies, governments and law makers

This research action explores how the European Legal Framework might be enhanced to better respond to cybercrime and at the same time preserve the privacy of the EU citizen.

The research questions that this research action addresses are:

- What constitutes an effective cross-border data sharing framework for cybercrime fighting that preserves the privacy of the citizen?
- How can effective remote access to digital data stores for cybercrime evidence gathering be facilitated?
- How can the relationships between digital evidence data stores best be visualized in order to support cybercrime fighting?

This research action seeks to extend and standardise the legal framework in order to enable the crime fighting agencies to more rapidly investigate cybercrime.

An enhanced legal framework needs to have the following capabilities:

- a) communicate privacy issues to the public;
- b) visualise the relationships between data stores that contain the evidence necessary for a cybercrime investigation;
- c) provide effective remote access to digital data stores for evidence; and d) safeguard privacy and human rights when accessing digital data stores for cybercrime investigation

There is strong motivation for such a programme - without their being clear legal consequences for cybercrime, the perceived chance of being identified or brought to justice is small. At the same time, EU citizens use cryptography to protect their personal data on social media platforms that use data storage outside of the EU. This means that the EU does not have sovereignty over the critical data necessary to deter, prevent, investigate and prosecute criminals. This also means that the EU has to redefine traffic data as a legal concept that moves beyond simply identifying the IP address and to make the content of this traffic available to law enforcement agencies during an investigation.

This research action comprises the following stages:

1. Review of the existing framework for digital evidence access and identification of gaps in capability.
2. In partnership with the stakeholder communities, design of revised frameworks of digital evidence access and identification of privacy tensions for citizens.
3. Development, deployment and assessment of tools and methods to support the legal framework and to respond to the identified privacy tensions.



10.4 RESEARCH ACTION #3 STUDY PRACTICES AND PROCESSES OF INTERNET MONEY LAUNDERING.

DISTANCE TO THE MARKET: TRL 3

COST OF THE TOPIC: 1 STREP

AVAILABILITY OF COMPETENCE IN EUROPE: 2

TIME SPAN FOR ADDRESSING THE ACTION: 24 months

ACTORS: Academics, industry and government, consumer and citizen representatives

This research action examines infrastructures that support internet enabled money laundering.

This research action addresses the following research questions:

- What are the most effective ways to study the flow of internet-based money laundering transactions?
- What internet infrastructures support money laundering?
- In what ways has the Internet influenced money laundering practices?

This research action aims to derive a better understanding of how the internet has influenced the nature of money laundering. In particular, this research action will look at how money laundering transactions flow across the internet. This research will also explore how the internet has resulted in changes to money laundering practices. The research will further develop our understanding of the internet infrastructures that are currently used in money laundering and how these might evolve in the future.

The research action will bring together both social and computational science researchers. The social research will focus on the historical practices of money laundering and examine how these have been influenced by the use of the Internet for money laundering. The social research will also examine to what extent the use of the internet has affected the take-up of money laundering services, the roles of money laundering within crime networks and the ability of traditional interventions to disrupt money laundering activities. The computational research will examine how money laundering transactions can be identified on the data network, the transaction patterns generated by internet-enabled money laundering and the traceability of the transaction patterns.

This research action would comprise the following stages:

1. Survey of existing academic and practitioner literature on money laundering practices.
2. Field research to identify the impact of the Internet on money laundering practices and the communities that both carry out and consume money laundering services.
3. Lab research to examine how money laundering transactions manifest themselves on the data network.
4. Development, deployment and assessment of new techniques to identify and trace internet-enabled money laundering.



10.5 RESEARCH ACTIONS GANTT

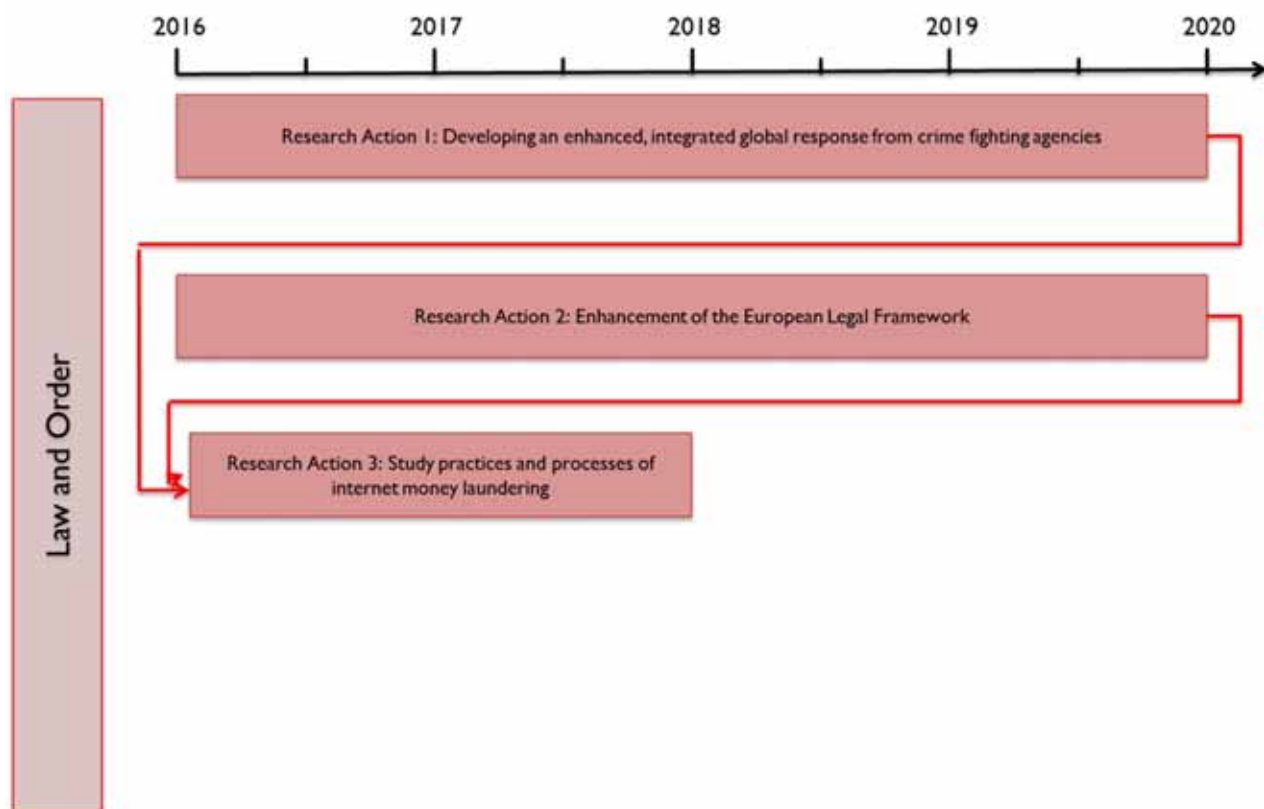


Figure 20 - Law and Order RAs GANTT

11 NETWORKING

CC RG-22	Improving integrity and confidentiality of heterogeneous utilities networks.
CC RG-23 and CT RG-23	Improve trade-off between protocols security and latency.
CC RG-27	Improve efficiency and security of communication protocols for wide area power systems.

11.1 ABSTRACT

The clear advantages in terms of cost reduction and efficiency gain that is offered by the adoption of new technologies such as the Internet of Things (IoT) and smart grids, is pushing many systems (including utilities) to move from closed environment to open IP-based communication networks. This trend opens up a new range of risks to data integrity and confidentiality that can be compromised by network attacks such as data injection, man-in-the-middle, spoofing, impersonation, or denial of service. Therefore, it is important to improve the security of communication networks such as those in use in systems such as utilities, smart grids and power systems and Advanced Metering Infrastructure (AMI).

11.2 RESEARCH ACTION #1 MONITORING AND INTRUSIONS DETECTION SYSTEMS TO IDENTIFY NETWORK INTRUSIONS THAT CAN UNDERMINE DATA INTEGRITY (E.G. CORRUPT OPERATIONAL DATA WITH TRAFFIC INJECTION) OR CONFIDENTIALITY (E.G. WITH A MAN-IN-THE-MIDDLE ATTACK).

DISTANCE TO THE MARKET: TRL 5
COST OF THE TOPIC: 3 STREPs + 0 IP
AVAILABILITY OF COMPETENCE IN EUROPE: 5
TIME SPAN FOR ADDRESSING THE ACTION: 36 months
ACTORS: Industry, Critical Infrastructures, Research Institute

Monitoring and intrusion detection systems can identify intrusions and signs of possibly compromised devices before the threats they pose to utilities and critical infrastructure materialize, thus minimizing their negative consequences. In particular, it is important to design novel network intrusion detection technologies that, aware of the specific communication protocols adopted and aware of the possibly limited access to the data due to cryptographic schemes or legislation, can still be effective in detecting increasingly complex attacks. Specifically, monitoring solutions for critical infrastructures should meet the following requirements:

- 1) Pose a minimal impact on utilities network that typically have limited resources.
- 2) Capabilities of detecting new emerging complex targeted attacks.
- 3) Capabilities of performing monitoring and detection even in the presence of encryption schemes.

11.3 RESEARCH ACTION #2 PROTOCOLS FOR UTILITIES, SMART GRIDS AND ADVANCED METERING INFRASTRUCTURES (AMI) WITH EMBEDDED SUPPORT FOR ENCRYPTION, SECURITY, AUTHENTICATION AND SCALABILITY.

DISTANCE TO THE MARKET: TRL 5
COST OF THE TOPIC: 3 STREPs + 0 IP
AVAILABILITY OF COMPETENCE IN EUROPE: 3
TIME SPAN FOR ADDRESSING THE ACTION: 48 months
ACTORS: Industry, Standardization Body, Research Institute

Industrial Control Systems (ICS) are typically used to regulate industrial processes (e.g. in utilities). ICS are

exposed to the same security vulnerabilities associated with enterprise networks. To overcome these risks, cryptography can be used; however, applying cryptographic algorithms to ICS environment introduces communication latency that violates operational requirements. Thus, it is important to improve existing cryptography techniques (or devise innovative methodology) that can support encryption by respecting real time constraints. Recently, IETF has standardized RPL (routing protocol for low power networks), which is expected to be the standard routing protocol for the majority of applications including advanced metering infrastructure (AMI) networks. Although the RPL protocol provides optimal routing performance, it does have numerous security flaws that should be addressed prior to its use in critical infrastructure. Especially, it is important that protocols in use in critical infrastructure exhibit the following features:

- 1) Being robust to complex attacks aimed at disrupting functional operations or violating data integrity.
- 2) Support encryption and authentication with a reduced latency, so that operational time constraints posed by critical environments can still be respected.

11.4 RESEARCH ACTION #3 INNOVATIVE SOLUTIONS TO GUARANTEE DATA INTEGRITY WITHOUT RELYING ON ENCRYPTION.

DISTANCE TO THE MARKET: TRL 3

COST OF THE TOPIC: 3 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 60 months

ACTORS: Industry, Research Institute

Typically, encryption is adopted to guarantee data integrity. However, in critical environments, the extra latency required by cryptography techniques often makes it impossible to respect operational time constraints. This may lead to a situation where encryption cannot be adopted at all. To solve this issue, it is important to devise innovative techniques capable of data integrity verification without relying on encryption. For instance, an alternative to encryption could be to check data integrity by verifying that data is in line with process status and sensors' measurements.

11.5 RESEARCH ACTIONS GANTT

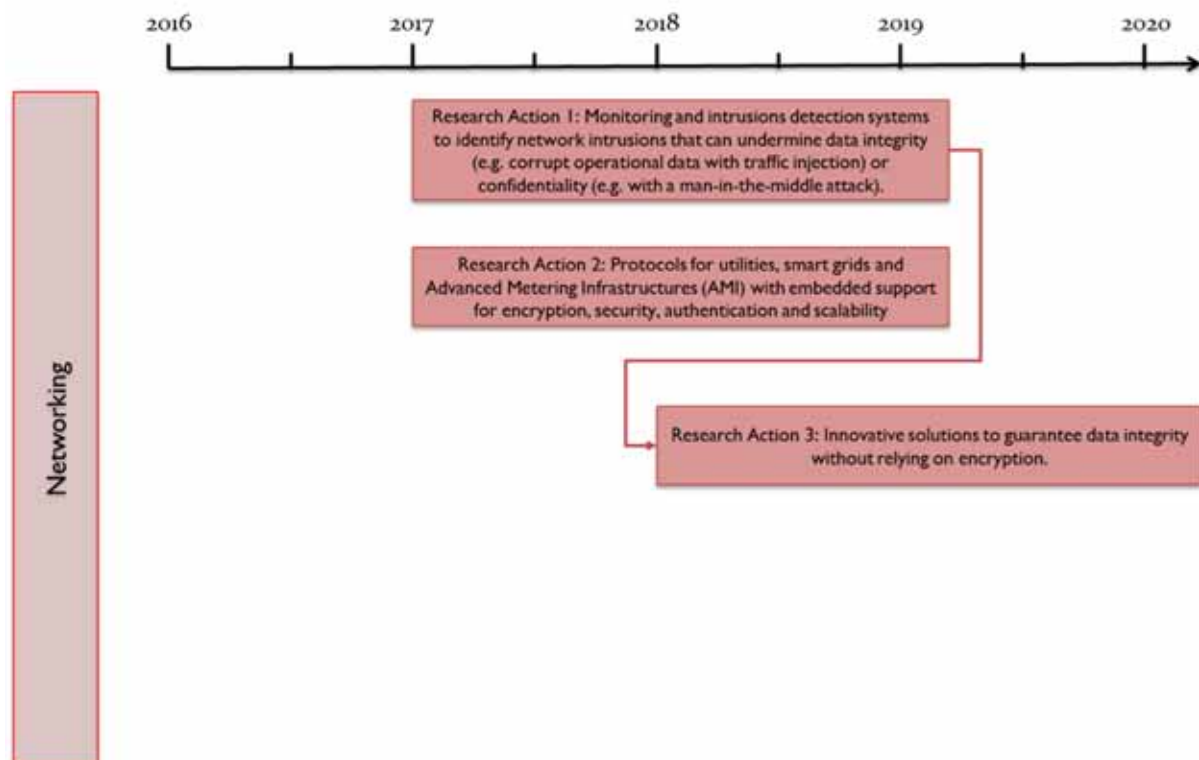


Figure 21 - Networking RAs GANTT



12 CYBER THREAT AWARENESS

CC RG-5 & CT RG-2	New awareness methodologies with a human touch
CC RG-20 & CT RG-17	Training methodology (anti-phishing and social engineering) to increase security awareness for critical infrastructures.
CC RG-56 & CT RG-56	New ways to alert users of ongoing attacks or increased risks because the device become a disappearing device and thus perceiving the related threats is also difficult.
CC RG-58	Techniques and strategies for raising user awareness towards the sensitivity of health data. Methods for providing the social component of such networks, while still providing anonymity.
CC RG-63	Research into effective awareness training methods
CT RG-68	Process awareness embedded in security tools


12.1 ABSTRACT

Nowadays, Social Engineering (SE) attacks are posing one of the most significant risks for cybersecurity. Indeed, the analysis of the new attack strategies clearly shows how cybercriminals increasingly tend to exploit vulnerabilities introduced by human factors to perform cyber-attacks. While SE is a well-known method for deception used for a very long time, its evolution in the past years has been dramatically changing the current attack landscape, and it will heavily influence future scenarios. The evolution of SE attacks is rooted in socio-economic and technological factors. On the one hand, current society transformations are characterized by a model of “immersed humans”, where physical and virtual meetings seamlessly merge, thanks to mobile and ubiquitous terminals. In working contexts, employees can complete a task in any possible place, leading to an inevitable blending between private and professional lives. Furthermore, the advent of online social networks has been heavily affecting people-sharing habits, creating a proliferation of digital identities available on the Internet. On the other hand, new technologies have been enabling more sophisticated SE attacks, i.e. advanced automatic methods to gather and elaborate information needed to carefully select the “victims”. All these factors contributed to the evolution of SE into a new multifaceted phenomenon that goes under the name of Social Engineering 2.0, which increases the number of potential victims directly exposed on the Internet.

People’s vulnerability to SE attacks is based primarily on their naivety and lack of cybersecurity awareness. Hence, SE attacks (e.g. stealing bank codes and passwords) exploit the behavioural habits and trusting nature of users. The unsafe behaviour of users is also worsened by the poor design in many human-computer interfaces that do not provide any feedback on the increased exposure to cyber threats. Since the crucial phase of these attacks leverages on vulnerabilities introduced by users’ behaviour, it is of the utmost importance to extend the governance of security to include human element among the risk factors in order to implement appropriate and effective countermeasures. The most effective measure against SE attacks is the development of awareness through specific training courses. Such training should be aimed at increasing the security culture within a specific domain. The crucial point is to create awareness programs that have a real impact on people's attitudes with the result of an effective increase in the level of security to be maintained over time. In general, it is necessary to develop intervention strategies that encourage the active involvement of people, where security features are not perceived as an “enemy”, but as an ally to cooperate with in avoiding the bad consequences of falling victims of SE attacks.

12.2 RESEARCH ACTION #1 IMPROVEMENT OF AWARENESS MECHANISMS FOR DATA AND INFORMATION SHARING IN PERSONAL AND WEARABLE DEVICES AND IN THE TREND OF DISAPPEARING COMPUTER.

DISTANCE TO THE MARKET: TRL 3

	D2.3 Final Roadmap
	Funded by the European Commission under the Seventh Framework Programme
	Page 52 of 91

COST OF THE TOPIC: 5 STREPs + 1 IP
 AVAILABILITY OF COMPETENCE IN EUROPE: 3
 TIME SPAN FOR ADDRESSING THE ACTION: 36 months
 ACTORS: Research institutions, Industry

Personal devices, such as smartphone, wearables, and the whole category of disappearing computer, are capable to sense, store, and share a large variety of environmental, physical, and health data, as well as textual and visual information. Often this happens without users' awareness and knowledge. The new European General Data Protection Regulation (GDPR) legislation foresees to radically change most of these problems, but the awareness of the users in terms of understanding what the systems propose or want to do with the data is still lagging behind.

For these reasons, there are some important directions that should be investigated to improve the informed use, and the market penetration of these solutions.

- Raising user's awareness through effective feedback mechanisms from the connected devices that let the user clearly perceive privacy and security risks related to improper data sharing behaviour.
- Interactive and adaptive alerting mechanisms that allow users to cooperate with the machine in detecting the characteristics of potentially unsecure websites, cloud and online social services.
- Informed processing of data along its lifecycle, so that users can control the whole chain, from the acquisition phase, to data storage and destruction, with the possibility for the users to revoke permissions.

12.3 RESEARCH ACTION #2 IMPROVING THE AWARENESS OF CYBER THREATS FOR WORKFORCES IN CRITICAL INFRASTRUCTURES.

DISTANCE TO THE MARKET: TRL 4
 COST OF THE TOPIC: 3 STREPs + 1 IP
 AVAILABILITY OF COMPETENCE IN EUROPE: 4
 TIME SPAN FOR ADDRESSING THE ACTION: 30 months
 ACTORS: Industry, research institutions

- Effective detection of phishing web sites, and spear phishing emails based on the correlation of open source intelligence, textual and visual analysis.
- Enable the user to naturally interact with the phishing and spear phishing detection mechanisms in a feedback loop to iteratively improve the detection capabilities, and raise the awareness level of the workforces.
- Threat modelling paradigms for critical infrastructures that include indirect threats based on social engineering attacks.
- Involvement of users in defence solutions, by keeping the humans in a feedback loop with the modern learning-bases threat intelligence systems, to match the users' awareness tracks with the learning curves of the defence system. Despite some early products appeared on the market the research is still at its beginning. For example, a crowd idea generation based approach that rewards humans to participate into human sensors networks signalling phishing samples, could be used to feed analyst-driven predictive analysis.

12.4 RESEARCH ACTION #3 DETECTION OF ATTEMPTS OF TAMPERING WITH MANUFACTURING PROCESSES IN INDUSTRIAL PLANTS.

DISTANCE TO THE MARKET: TRL 3
 COST OF THE TOPIC: 5 STREPs + 1 IP
 AVAILABILITY OF COMPETENCE IN EUROPE: 5
 TIME SPAN FOR ADDRESSING THE ACTION: 36 months
 ACTORS: Industry, Research Institutions

- Novel paradigms for security information and event management to correlate network and computer system events with process control events.

- SCADA devices and algorithms to self-detect any modifications in manufacturing process execution.
- Encryption and obfuscation mechanisms for the exchange of data and command and control instructions in the internal network connecting the remote controlled production systems.
- Insertion of humans in the loop: most of nowadays threats involve humans as their main vector of infection. Humans became a relevant and integrated part both in the attack and protection mechanisms: this changed the landscape of IT security, because the humans have been added in the protection mechanisms as sensors (sensing what is happening in the enterprise, via for example human sensors networks), or feeding the machines (for example analyst-driven solutions). Integrated human-technological protection systems are appearing on the market, but the research area is still evolving.

12.5 RESEARCH ACTION #4 CREATION OF AD-HOC AWARENESS EXPERIENCES.

DISTANCE TO THE MARKET: TRL 4

COST OF THE TOPIC: 4 STREPs + 0 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 30 months

ACTORS: Industry, Research Institutions

The number of awareness mechanisms available in the ICT Security market for training users is increasing, ranging from printed leaflets, courses, infographics, videos, audio courses, and gamification. However, each of the available method showed its effectiveness in specific environments (e.g., video and posters in enterprises, gamification with citizens etc.), but there is neither a winning approach, nor some guidelines to allow the selection of the best approach for a given scenario. Nevertheless, the most interesting recipes for new awareness strategies in security are all involving the following three elements:

- Gamification: traditional ICT security trainings do not present particular appealing characteristics. In contrast, gamification frames such trainings as hacking games of different formats (e.g., attack-defence capture the flag, jeopardy), fostering competitiveness and promoting problem-solving activities.
- Incidental learning: partial yet continuous learning and knowledge improvement, for example through mini-sessions during the day, trying to avoid monolithic tracks.
- Personalization: adapt the learning experience to individuals' attitudes, habits and mind-sets.

What is important to investigate is how to tailor the awareness experience around each single person, according to his/her psychological profile and personality and match these findings against the costs to produce the material.



12.6 RESEARCH ACTIONS GANTT

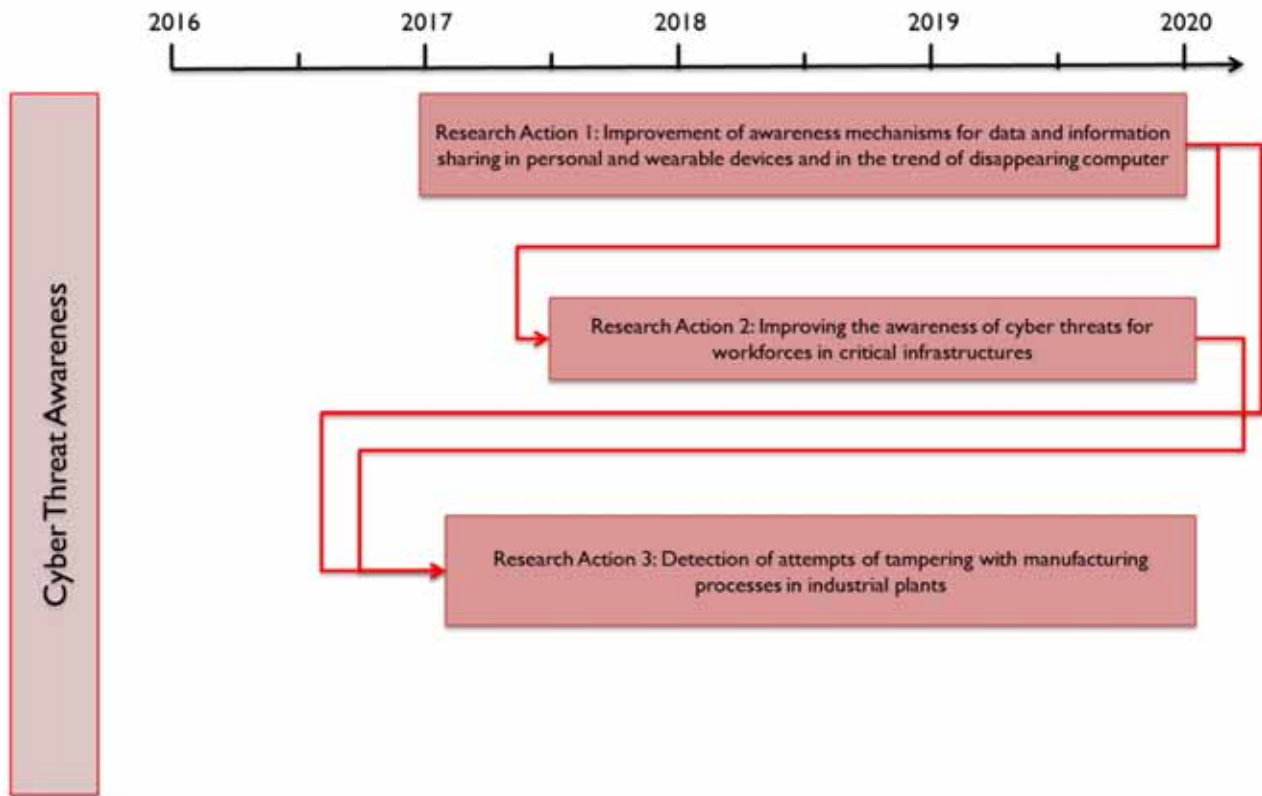


Figure 22 - Cyber Threat Awareness RAs GANTT



13 NEW OBJECTS AND DISAPPEARING COMPUTING

CC RG- 31 and CT RG- 31	Difficulty to find updating mechanisms that scale to large and heterogeneous networks
CT RG-90, CC RG-93, CC RG-10, CT RG-11, CT RG-81	Absence of a reliable and holistic security mechanism
CC RG- 8, CT RG- 16, CT RG-44	Absence of a systemic view of the correlation among security, privacy and safety

13.1 ABSTRACT

Since the proliferation of the Internet of Things (IoT) paradigm, the use of tiny and interconnected devices has seen an enormous growth in several fields. Examples of application areas are monitoring systems and e-banking services.

Networks that are established on the basis of such devices differ from traditional ones, which makes them difficult to secure. Here we identify three key research gaps:

- 1) difficulty to find updating mechanisms that scale to large and heterogeneous networks
- 2) absence of a reliable and holistic security mechanism
- 3) absence of a systemic view of the correlation among security, privacy and safety.

13.2 RESEARCH ACTION #1 DIFFICULTY TO FIND UPDATING MECHANISMS THAT SCALE TO LARGE AND HETEROGENEOUS NETWORKS.

DISTANCE TO THE MARKET: TRL 4

COST OF THE TOPIC: 0 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 12 months

ACTORS: Universities and academic actors; electronic industry

The use of IoT devices is increasingly pervasive. Their adoption is common in several areas, ranging from wearable health-care devices to tiny sensors that monitor the level of water poisoning.

The scenarios where IoT networks work are continuously evolving, both in terms of computational requirements and in security complexity. Thus, it is of paramount importance to define hardware and software upgrading mechanisms that are as simple as possible.

Devices must be built in order to ease extension in memory, computation capabilities and performance in general. The same applies for software components, for which a reliable updating/patching mechanism has to be clearly defined (and standardized).

While the replacement/upgrade of hardware components requires a physical access to the network, this is not necessarily true as far as software is concerned. In fact, the feasibility of a remote upgrading mechanism which is secure and reliable is worth investigating.

More specifically, an ideal updating mechanism should discover and provide patches to new security flaws in a way that notifies the owner of the devices in a timely manner or that, alternatively, is automatic.

The former option is not always possible, since the interaction between users and devices is not as user-friendly as in a traditional scenario (e.g., devices often do not have a input/output capabilities).

As far as the latter option is concerned, it is necessary that some trusted authority (e.g., the manufacturer) get constantly notified about the status of the network, i.e., the type of devices and the software they



currently run.

This requirement is difficult to meet due to two main reasons:

- 1) these network are heterogeneous and continuously evolve (i.e., it is easy to add and remove devices)
- 2) devices have generally limited connection capabilities, which make the interaction with an external entity harder.

Additionally, limited resources prevent a traditional updating mechanism to be properly implemented, since firmware and patches should be distributed with minimal overhead and stored in a very limited memory. A possible approach consists in optimizing the distribution of the updates, for example by proposing peer-to-peer solutions (i.e., a small set of nodes initially receive the updates and then deliver them to the rest of the network). Other security requirements (e.g., integrity, updates authentication, etc.) have to be satisfied in the IoT scenario. The aforementioned constraints force researchers to find lightweight solutions.

13.3 RESEARCH ACTION #2 ABSENCE OF A RELIABLE AND HOLISTIC SECURITY MECHANISM.

DISTANCE TO THE MARKET: TRL 3

COST OF THE TOPIC: 0 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 24 months

ACTORS: Research institutes and security related industries

The presence of a centralized mechanism that distributes patches to the network nodes opens the door to the definition of a reliable IoT network management system. The goal is to implement monitoring/reaction procedures, in order to realize security mechanisms, analogous to those used in traditional networks (e.g., intrusion detection systems, firewalls, etc.).

The adoption of techniques commonly used in traditional network requires significant reengineering to address the constraints posed by resource-limited devices. For instance, if the processing power is limited, it is not possible to implement robust encryption and alternative lightweight solutions must be found. Analogous considerations hold as far as authentication mechanisms are concerned: due to the highly dynamism that characterize IoT networks, it is necessary to find a way to easily authenticate the sensors.

Generally, in IoT networks it is possible to identify very simple devices connected to a more powerful device, which often acts as a gateway. Being the gateway the most powerful device within the IoT ecosystem, it may be used to implement several monitoring functions that give a global view of the network. The global view also allows to correlate the events observed in all the devices, helping to identify malicious activities better than an approach based on single devices. Moreover, this approach is also more feasible due to the well-known energy issues (i.e., most of the security operations are off-loaded to the gateway). Thus, a completely distributed approach in realizing, for example, an intrusion detection system, seems to be not possible. However, it is possible to investigate hybrid solutions, where the network is divided in clusters for which head nodes are defined. The role of the cluster-head is to monitor the nodes under its supervision, measuring, for instance, their energy consumption. If the consumed energy is above a given threshold, security countermeasures should be triggered (e.g., because flooding attacks have likely happened).

Moreover, given that IoT devices are often used to gather very personal information, another key issue is the definition of mechanisms and procedures through which it is possible to understand when there is leakage of sensitive information. Thus, a holistic approach that can face both security and privacy issues in a centralized fashion seems to be a viable route to take.

Finally, an extensive standardization on how things should be secured by design is urgently required.

13.4 RESEARCH ACTION #3 ABSENCE OF A SYSTEMIC VIEW OF THE CORRELATION AMONG SECURITY, PRIVACY AND SAFETY.

DISTANCE TO THE MARKET: TRL 4

COST OF THE TOPIC: 3 STREPs + 0 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 18 months
ACTORS: Research institutes and security related industries

Information gathered by IoT devices can be very different in nature. Some examples are: very sensitive and context-dependent information, such as those collected by wearable health-care devices; information vital for a community, such as those collected by sensors that monitor the level of poisoning of the water-supply network or information that are extremely important for an industrial process, such as those collected by generic monitoring sensors employed in a factory.

In all the aforementioned scenarios security has an impact on privacy, safety (these devices may act also in physical space) or both. Thus, a necessary step in the definition of reliable IoT system is the creation of a framework with the goal of assessing in a systemic way the correlation among these three key aspects, namely security, privacy and safety. The framework should include the definition of suitable metrics, which must measure security/safety potential risks, as well as the level of sensitiveness of the gathered information. In this way it will be easier to evaluate the type of network, and consequently implement ad-hoc design principles.

In fact, Security, Privacy and Safety by design principles must be followed and adapted to the particular situation. For example, if a network that monitors a mine field is compromised, safety of people is the first concern. If a home IoT network is compromised, the main concern is shifted to privacy. A possible design principle could be the automatic disabling of the devices that collect the most sensitive information whenever an intrusion is detected (i.e., disable certain sensors as soon as the environment is under attack).

13.5 RESEARCH ACTIONS GANTT

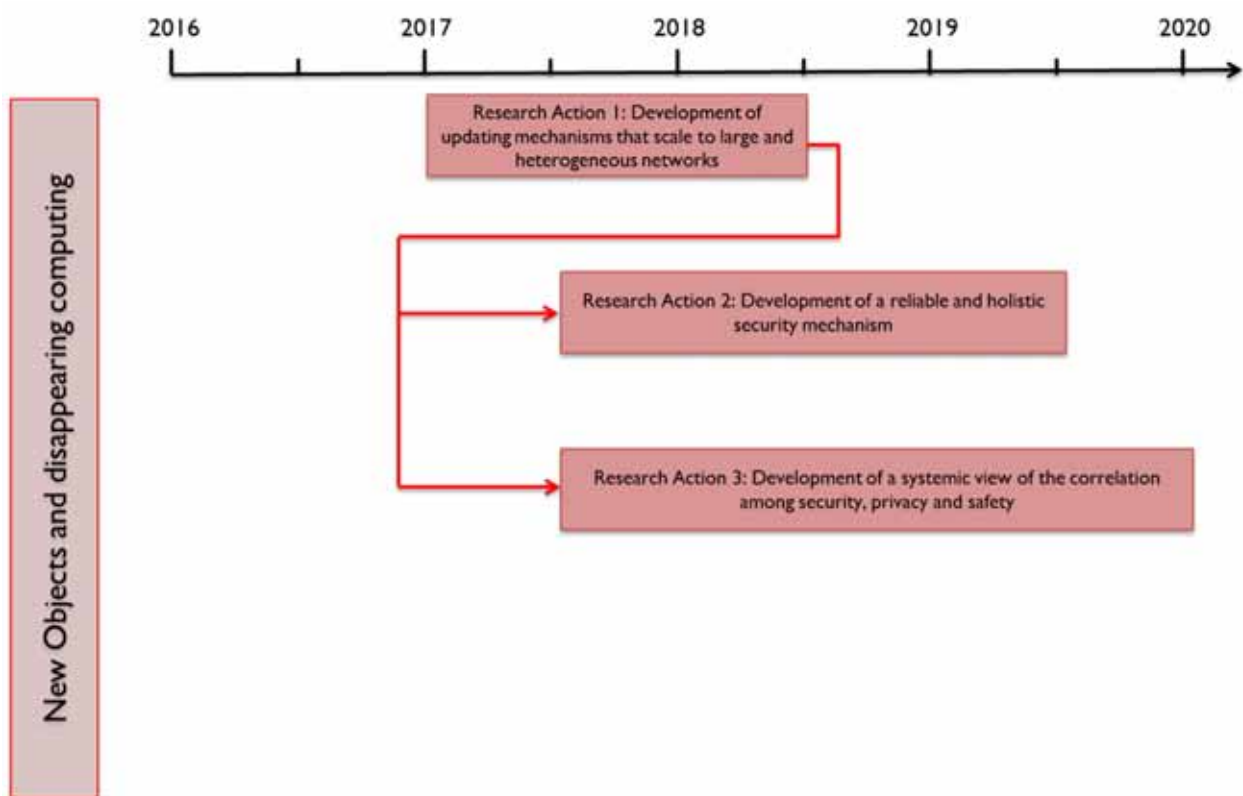


Figure 23 - New Objects and disappearing computing RAs GANTT

14 SCADA & CRITICAL INFRASTRUCTURES PROTECTION

CC RG- 14 and CC RG- 16	Tamper-proof sensors and controllers
CT RG-21	Develop techniques for monitoring and control of parameters and status of pipeline in order to detect deviations and misbehaviour
CT RG-22	Research into improving integrity and confidentiality of heterogeneous smart grid networks.
CT RG-24	Physical-layer authentication
CT RG-27	Research on efficient and secure communication protocols for wide area power systems
CC RG- 28 and CT RG-28	Research on secure routing and aggregation protocols
CC RG- 30 and CT RG-30	Research into securing large scale (Open) Demand Response environments
CC RG- 35 and CT RG-35	Challenging to provide protection to a large number of components in the entire railway/aviation system
CC RG- 37 and CT RG-37	Identify integrity of messages, support designated capacity per radio link, identify jammers
CC RG- 45 and CT RG-46	Enhance robustness in existing geo-localization systems
CT RG-49	Assess the performance of GNSS receivers in a broad range of channels under different attack schemes to provide a framework for risk and vulnerability assessment
CC RG- 90 and CT RG-86	Design of banking system solutions that are resilient to DDoS attacks

14.1 ABSTRACT

The modernization, interconnectedness and increasing complexity of Critical Infrastructure and the underlying technology have made that new attack vectors are available for offenders. Thus, in order to protect Critical Infrastructures effectively is mandatory to leverage various new approaches. This challenge is especially relevant in national security and the fight against cybercrime and cyber terrorism.



14.2 RESEARCH ACTION #1 ADDRESSING ADVANCED SECURE MOBILE COMPUTING FOR THE PROTECTION OF CRITICAL INFRASTRUCTURE.

DISTANCE TO THE MARKET: TRL 4-5

COST OF THE TOPIC: 3 STREPs + 3 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 1

TIME SPAN FOR ADDRESSING THE ACTION: 50 months

ACTORS: Governments, Critical Infrastructure Organizations, Research Institutes

Smart phones and other types of smart devices, such as wearables, IMD (Implantable Medical Devices) and Internet-enabled appliances are now widely adopted. They offer pervasive user connectivity through various wireless communication means, powerful sensing capabilities and easy install-and-use of third party applications. Altogether, it is reasonable to think that they will become the main user platform for managing Critical Infrastructure in near future.

The architecture of smart devices, the existing security models and the prolific mobile malware market make current commercial solutions highly ineffective. Recent studies show that traditional signature-based antimalware techniques for smart phones detect only between 20.2% and 79.6% of analysed malware. Other approaches, such as dynamic analysis, seem promising but are unaffordable when executed on the device due to resource consumption rates.

On the other hand, the inherent architecture of the smart phones, enables potential attacks at device or application level by subverting the security of “goodware” installed on the device. To deal with these threats, completely novel approaches that consider the whole ecosystem of apps installed on the device are required. Such approaches should highlight the level of security the apps exhibit, to support making informed decisions about whether executing certain actions (e.g. managing power plants, water treatment plants, etc.) that might have an impact not only on the citizens but also at business level.

Ensuring a secure execution environment brings a number of challenges that are particular to smart devices:

- Efficient and effective real-time, dynamic risk assessment for making informed decisions with a clear impact on personal and business assets. Recent advances suggest that the optimal approach lies in a combination of market, platform and cloud-based defensive strategies that overcome the inherent limitations of current devices. Transforming this into practical, cost-effective solutions remains an open challenge for the industry.
- Identifying and detecting polymorphic and metamorphic malware, as well as repackaged malware apps (the most common distribution and infection vector) regardless the presence of any security measure implemented at market level (open/unofficial markets).

None of the above will succeed against our adversaries if the human analyst still plays a role in the process, neither when supported by automated tools. Fully automation becomes a must-have requirement, both for malware/attack detection and remediation/response actions. Considering the figures of the malware market and its daily growth, it is obvious that the human analyst must move from a link in the operational chain to a valuable asset in pre and post operational phases, such as the design of new tools (analysis strategies, expert knowledge, algorithms, patterns) and the post-analysis of automatically-generated information.

14.3 RESEARCH ACTION #2 TRAINING PLATFORMS ABLE TO REPLICATE REAL CRITICAL INFRASTRUCTURES.

DISTANCE TO THE MARKET: TRL 6-7

COST OF THE TOPIC: 3 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 1

TIME SPAN FOR ADDRESSING THE ACTION: 42 months

ACTORS: Governments, Universities, Critical Infrastructure Organizations

Although figures vary between reports, there is a general agreement over the fact that current and former employees are amongst the main causes of cybersecurity incidents suffered by the Critical Infrastructures. Their lack of awareness is one of the most significant threats any organisation has to face. Likewise, the lack of qualified and trained IT/security staff aggravates the situation.

It has been largely proved that conducting training and awareness activities is a winning bet for reducing exposure to cyber threats at a reasonable cost.

Traditional training approaches, namely class-room sessions, e-learning and b-learning (as we know them today) do not suffice to keep our workforce up-to-date and ready to respond in such an overwhelming



changing scenario. Punctual training sessions, however they are provided, continue to lag behind the rapid rate of change of technology and cyber threats. But, worst of all, current approaches cannot accommodate, in a cost-effective and timely manner, the particularities of a customer's security problem, neither the technologies nor networks they use in their operational environments. In other words, the effectiveness of the training is very limited.

Even though training is currently considered a fundamental prerequisite for the adequate protection of Critical Infrastructures, there is still a need for innovative technology capable of providing realistic, flexible, evolutionary and tailored training able to reach a large-scale audience in a cost-effective way. As of today this remains a great challenge both for the academy and the industry.

In recent years, the training concept has been reshaped with the introduction of cyber ranges. A cyber range is a virtual environment typically built on top of standard hardware and used for multi-tenant hands-on training, experimentation, test and research in cybersecurity.

Some of the aforementioned required properties (realism, flexibility, etc.) are already met by current cyber range solutions. For example, a standard cyber range is usually designed to provide realistic settings where the user interacts with real (virtual) systems and networks that may, to some extent, reproduce real-world scenarios with real-time feedback and operation.

However, much research and innovation is still needed to accommodate and combine in a single solution all of the properties above. For instance, combining the capability to tailor a hands-on training course for a specific customer is, considering current cyber range solutions, impractical if large-scale and cost-effective properties also need to be provided. With this regard, a smart and automated trainee supervision and assessment system that guided them through the exercise, providing automated hints when needed, would permit to deploy the solution for thousands of trainees concurrently without the need of a single instructor. Also, a cyber range capable of easily deploying on-demand configurations of new tailored exercises would provide a significant improvement to better tackle with particular needs, specific situations, and representing new and emerging threats.

If there is one common limitation in current cyber ranges is that, even when commercialised under the label of training platforms, they support test, experimentation and research activities (even capture-the-flag competitions) but without any pedagogical features. Current solutions hardly incorporate metrics and functionality to measure the actual performance of the trainee and manage their progress along the time. At the most, we observe that some solutions incentivize and motivate the trainee using quantitative scoring systems or gamification approaches. A more comprehensive and systematic view is needed. The foundations underlying the learning process should be considered by design. This may imply implementing different and complementary approaches, such as formal learning, observational learning, trial and error approach, etc. Related to this, the complexity of the training exercises should be scaled to the trainee's level, customising the level of automated guidance and support in each exercise. This is particularly important when targeting individuals at introductory level. A significant break-through innovation would be that this adaptation – including the difficulty of the training – is automatically readjusted along the lifespan of the training, an even dynamically during an exercise, according to the trainee's performance. The system could, for example, propose new challenges/objectives, reinforce certain attitudes or improve the adversary skills for highly proficient trainees.

Expected Impact:

- 1) Increased competitiveness of European Critical Infrastructure security to the needs of citizen, national public administrations and organizations.
- 2) Increased resilience against widespread cyber security threats facing Critical Infrastructure Organizations.

14.4 RESEARCH ACTION #3 INFORMATION SHARING SYSTEMS TO SUPPORT CRITICAL INFRASTRUCTURE PROTECTION.

DISTANCE TO THE MARKET: TRL 6-7

COST OF THE TOPIC: 4 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 3

TIME SPAN FOR ADDRESSING THE ACTION: 36-45 months

ACTORS: Governments, Critical Infrastructure Organizations



The efforts and initiatives towards encouraging the information sharing amongst the stakeholders in Critical Infrastructure protection are significant and continue to grow in number and intensity. The European Cybersecurity Strategy and the NIS Directive are possibly the most relevant examples at European level, identifying information sharing as one of the main pillars for building cohesive and resilient infrastructures and services in Europe.

However, in spite of the achievements made so far, which were undoubtedly necessary, there is still a long road ahead if we really want to fight cyber threats effectively and be at the forefront of this never ending battle. Cyber-attacks execute and succeed in computer time, so we need information sharing mechanisms that operate within the same order of magnitude. Contrary to this, we regret to observe that current real-life implementations for information sharing still heavily depend on the human factor.

In addition to this, the intrinsic flawed and highly vulnerable nature of technology leads us to conclude that absolute trust cannot be achieved in Critical Infrastructure. We should not rely, in absolute terms, on any information independently of who is the source. This demolishes the principle which current real-life implementations are based on, mandating full trust in the peers that are part of an information sharing community. This problem is aggravated by the fact that we cannot foresee who will have the knowledge needed to prevent or respond to certain incident. So, it seems that creating rather static, rigid procedure-based information sharing communities, as suggested by current political and industry initiatives, will not work as effectively as we require.

In order to really make information sharing a truly useful tool that eventually redresses the imbalance between attackers and defenders we need an urgent shift in the way we approach it. In particular, we need (near) real-time information sharing that relies on suitable trust and risk-aware models at the same time that leverages existing standards (data formats, exchange protocols) and infrastructures. Creating novel mechanisms and models for information sharing would benefit the whole community. We recognize that the human-factor is possibly the main impediment for the wider adoption of not only novel ways of sharing information automatically without the human intervention, but also "de facto", more traditional information sharing practices that have not managed to prosper.

Expected Impact:

- 1) Improved cooperation among Critical Infrastructure Organizations across the EU and Associated Countries.
- 2) Lower cyber operating costs for European CERTs teams
- 3) Improved description of incidents and characteristics of the various types of cyber-attacks frequently carried out by cyber terrorist.



14.5 RESEARCH ACTIONS GANTT

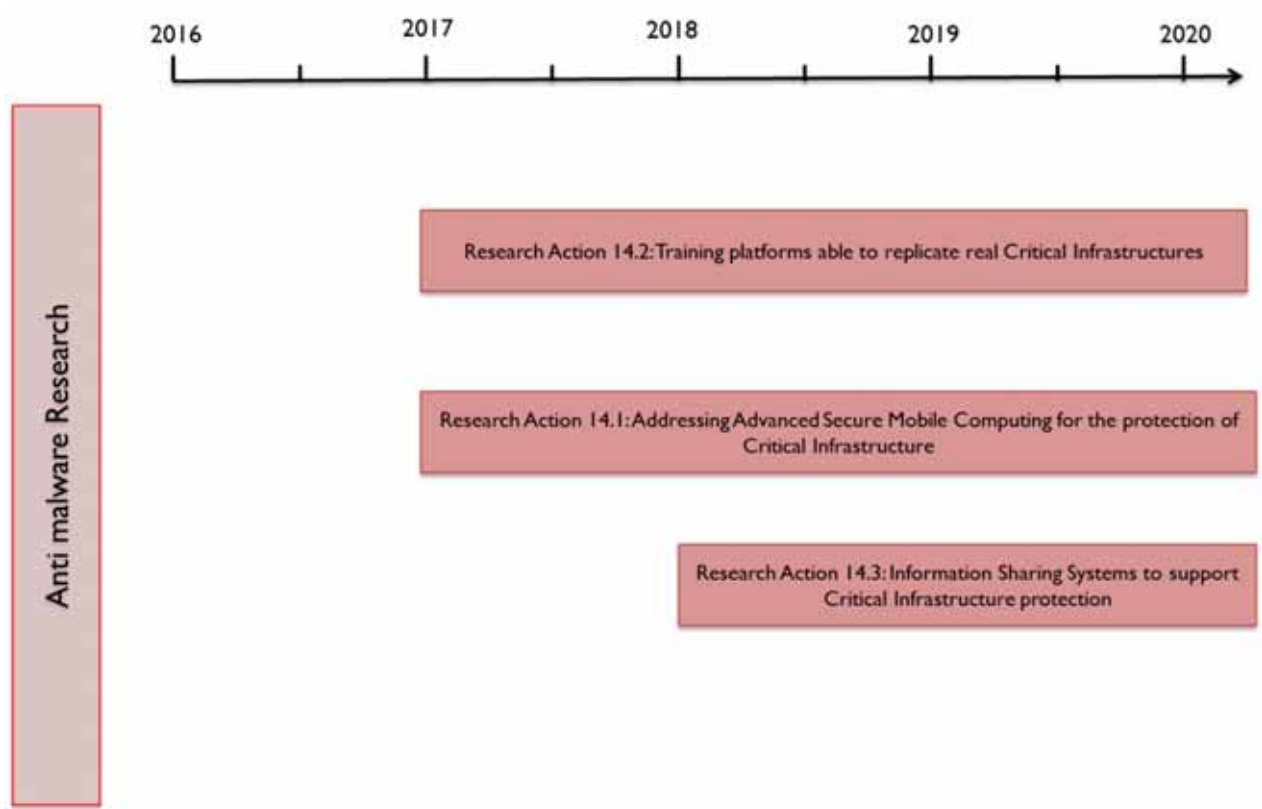


Figure 24 - SCADA and Critical Infrastructures Protection RAs GANTT

15 SOCIAL RESILIENCE

CC/CT LEG 2	Absence of a trusted authority for communication with people at risk
CC/CT LEG 3	Identification of possible security and safety issues
CC/CT LEG 1 and CC/CT LEG 2	Ensure redundancy of the trusted authority

15.1 ABSTRACT

Research on social resilience focuses on social responses to cybercrime and cyber terrorism. Leveraging on social resilience provides the basis of a potential programme of intervention that helps to both prevent cybercrimes from taking place and reducing the impact of cybercrime when it does take place. A key aspect of a social resilience system is the presence of a reliable mechanism that is able to spread awareness about some dangerous situation. The idea suggested here consists in the definition of a trusted authority that is in charge of communicating with the potential victims. Implications of the use of such a system are discussed (e.g., security and safety issues).

15.2 RESEARCH ACTION #1 ABSENCE OF A TRUSTED AUTHORITY FOR COMMUNICATION WITH PEOPLE AT RISK

DISTANCE TO THE MARKET: TRL 3

COST OF THE TOPIC: 2 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 24 months

ACTORS: Institutional bodies, Security responsible actors, Police, Government, Law enforcement, Research bodies, Cybercrime forces, Police, Research bodies, Private industry

Telecommunication infrastructures and services are used to communicate in time of crisis; this includes when a terrorist attack has taken place. Two main drawbacks of the current approach are distinguishable: first, people have to proactively tune in to hear about the dangerous situation; second, telecommunication systems only too rarely take into account the issues that could arise following a crisis (e.g., lines jammed because their capacity becomes saturated, routes down lowering this very capacity).

Thus, a mechanism that delivers timely and effective alerts to all the people that are at risk is required. Such a system should be based on a trusted authority (e.g., police/intelligence organization) that is able to certify the presence of a genuine danger. Then, the notification system has to be location-based, i.e., it has to deliver alerts messages to all the people that stay within an area that is considered at risk. For example, all the people within the cellular cell where a terrorist attack occurred could be notified by SMS, or by an automatic call.

It is needed to understand how the trusted authority receives information about the dangerous situation that is happening. In light of the following, we present two options:

- 1) the first one is that a "trusted authority" which handles the dangerous situation is also responsible of informing the broader public. An illustrative scenario could be: a water plant gathers data collected by its sensors that monitor the quality of water in the supply networks. If the quality of the water is under a threshold, the authority acts as a "trusted authority" and sends alert messages to all the people that reside within the involved areas.
- 2) the second one is about situations that are more chaotic and difficult to predict (e.g. terrorist attacks). Here it is needed that the "trusted authority" understands that something dangerous is happening, and is in measure to verify that the danger is real. False alarm must be put aside. This can be done with the help of the victims. Research must be done in order to find an easy way to communicate the danger, and then to verify that this is indeed not a false alarm.

The goal is to develop services that help people in danger to find solutions. For example, map of the safe areas can be distributed (e.g., via e-mail) to those who are in the crisis area.

15.3 RESEARCH ACTION #2 IDENTIFICATION OF POSSIBLE SECURITY AND SAFETY ISSUES

DISTANCE TO THE MARKET: TRL 3

COST OF THE TOPIC: 2 STREPs + 0 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 12 months

ACTORS: law enforcement agencies and their crisis centre, telecommunication providers, research institutes

The system has to be reliable and secure. For example, it must be able to disambiguate true from false alarms (including when people genuinely mistakenly over-react thinking a crisis is about to burst when it is not) and it must prevent manipulation activities. One possible malicious activity is described: the attacker could impersonate the trusted authority and provide people with a fake map of safe areas, thus urging people to go to a place where something dangerous would then be happening.

If messages coming from a fake authority are a concern that must be taken into account, the reverse is also true. In fact, the trusted authority should understand where some dangerous situation is really happening, and should do it in a timely manner. To do this, the trusted authority can for instance rely on messages received by people who feel they are at risk (e.g., because gunfire is taking place somewhere). Before sending alarm messages to any involved victims, the authority must be sure that this was a true danger and not, for example, a bad joke.

In order to evaluate the effectiveness of the alerting system, suitable metrics should be properly defined. For example, the time needed to notify potential victims of the occurring danger must be below a given threshold. Also the implication of any security compromise of such a system on human safety has to be quantitatively assessed.

15.4 RESEARCH ACTION #3 ENSURE REDUNDANCY OF THE TRUSTED AUTHORITY.

DISTANCE TO THE MARKET: TRL 3

COST OF THE TOPIC: 2 STREPs + 0 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 12 months

ACTORS: law enforcement agencies and their crisis centre, telecommunication providers, research institutes

When a crisis emerges, it may be difficult for authorities to ensure their message reach out to the victims. Telecommunication providers plan for a “normal” usage of their lines; a crisis event is however all but “normal”. People’s usage pattern changes. Traffic becomes saturated. On top of that, as in the case of a terrorist attack, an explosion may have very well physically damaged part of the telecommunication infrastructure. People within the crisis situation may not have signal. And as a consequence, the information may not reach its target audience in time.

To remedy such a situation, the trusted authority will need to be creative on how to reach out to people. This does not have to be via technological innovation. It will need to ensure that different telecommunication providers have agreements in place to jump in to support each other when such unlikely-but-with-high-safety-risk emerges. It will also need to ensure that it relies on a diverse strategy, using several mediums at the same time. Technology and creativity should allow to replace what otherwise was very effective albeit less convenient to deploy: good old analogous loudspeakers.

An example of such a creative solution could be with the use of drones. If part of the telecommunication infrastructure is down, a few drones could be dispatched to the crisis area, spread out and flown stationary: they could in so doing act as relay to other still-operating telecommunication towers, or transmit information via satellite link. Facebook is famously working on such a system to extend internet offers to developing countries, notably in Africa. Drones could furthermore act as a modern but easier-to-deploy version of the analogous loudspeaker.

Lastly, once such a system has been well-thought, tested and implemented, it should be set as a standard for



cities and countries. This implies that the goal is naturally to be able to deploy the system as widely as possible: such a system would ideally be cheap, easy to implement, and not be culture-sensitive. This newly developed system will also need to be mapped to economic models, thus be scalable and adequate for different societal models.

15.5 RESEARCH ACTIONS GANTT

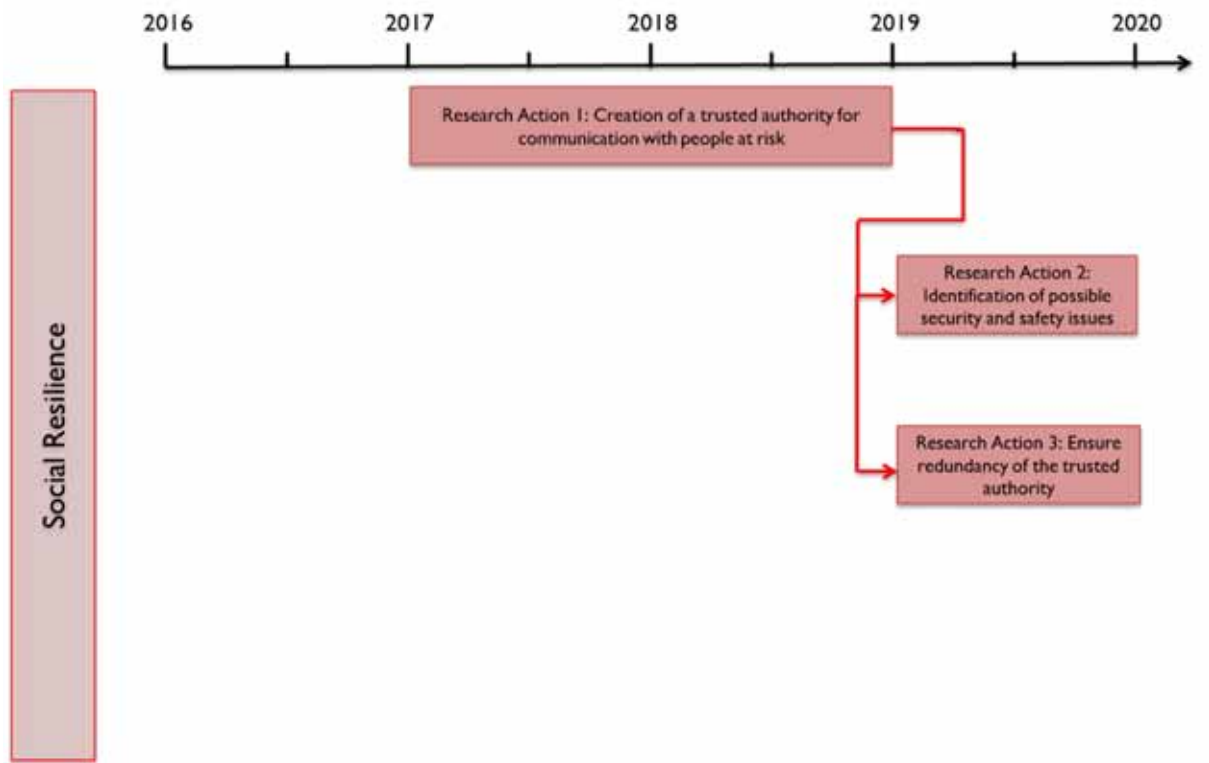


Figure 25 - Social Resilience RAs GANTT

16 SDLC & ARCHITECTURES

CC RG-41 and CT RG-41	Development of coding standards for secure and fault-tolerant cyber-physical system development
CT RG-14	Standardized interfaces to external modules and systems for providing in-depth security.
CT RG-40	Component and System level penetration testing procedures during development and integration of complex systems.
CC RG-97 and CC RG-100	Extending current security architectures to large distributed systems including players with different background knowledge in Security. Furthermore - CC RG-57 (for Cybercrime) - new authentication mechanisms need to be devised that provide usable security and continuous authentication.
CC RG-81	Methodologies to increase preparedness and responsiveness in case of attack, including attacks -
CT RG-75	targeting production process (e.g. to insert malware, backdoors or Trojan in final products).
CT RG-94	Intelligent IDS, hardening mechanisms and awareness.



16.1 ABSTRACT

Insecure software, even when executed in trusted computing environments, still represents a potential enabling factor for cybercrime and cyberterrorism scenarios. At the same time, even the most secure and bug-free software when run in untrusted execution environments, represents an important and often underestimated risk. Hence, the adoption of threat modelling techniques is to be considered fundamental in order to implement a Secure Software Development Lifecycle (SDLC) enabling the implementation of risk management best practices and the usage of well-known metrics. Other promising and interesting techniques aiming at protecting programs even if they contain vulnerabilities are still considered not mature and further research efforts needs to be spent in order to let them being effective. The efficiency of the threat modelling process is also an important factor affecting the security of developed software: all threats should be modelled, understood and properly rated as relevant (or not) considering the large degree of subjectivity involved in this process.

Some areas of improvement and suggested strategies are listed below:

- Support the widely adoption of SDLC and threat modelling techniques - especially for mobile app development - by simplifying management frameworks (CMMs), reducing the time-to-market for application development and the cost for developers' education.
- Improve support to, and encourage the adoption of management frameworks (CMMs) and SDLC for novel environments and paradigms such as IoT and wearables
- Simplify the existing techniques for SDLC and reduce the dependency by specific vendors
- Integrate threat modelling and risk management focusing on how to transform threats in the final risk metrics
- Increase the awareness on the attack techniques of whoever is involved into software products' development
- Create a certification of quality for SDLC
- Improve mechanisms for automatic generation of exploits for software vulnerabilities in order to ideally automate discovery and exploitation tasks

Secure application architectures are another big topic to keep in mind while developing software. Secure design principles must be taken into account since the early development stages, facing the big challenges raised by the usage of distributed, complex systems and by the novel paradigms (e.g. cyber-physical systems, swarms, grids, clouds, etc.) each with its own uniqueness and challenges.

16.2 RESEARCH ACTION #1 DEVELOPMENT OF CODING STANDARDS FOR SECURE AND FAULT-TOLERANT CYBER-PHYSICAL SYSTEM DEVELOPMENT

DISTANCE TO THE MARKET: TRL 7

COST OF THE TOPIC: 4 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: manufacturing industries, smart factories, machine-to-machine connectivity, smart sensors, smart tags, industrial control systems, autonomous cyber-physical systems, IoT devices, Internet of Services (IoS)

Cybercriminals (and Cyberterrorists too) are showing to have cyber-physical systems in their sights, even if driven by different motivations.

Hacking Cyber-Physical/Industrial Systems controlling gas pipelines or energy grids, shutting down national transportation critical infrastructures or gaining complete control of the on-board systems of an airplane, enable modern terrorism scenarios that have the potential to inflict massive damages affecting hundred thousands of lives, having a considerable psychological impact while granting at the same time total anonymity.

The opportunity to steal intellectual property or acquire sensitive data from Industry 4.0 companies, is being more and more exploited by Cybercriminals in order to monetize information on the dark web, or to limit competitive advantage of a competitor maybe sabotaging its production chain.

New threats that will affect cyber-physical systems can be faced through:

- High-level categorization of control systems to enable cyber awareness and readiness
- Advanced Risk analysis should be performed and model-based (formal) approach to system development needs to be adopted.
- Industries have to increase their responsiveness and preparedness developing proper methodologies to face the possibility of a successful attack in place.
- At the same time innovative monitoring and detection techniques must be put in place in order to attempt the detection of suspicious activities in the factory (e.g. detect change in the manufacturing processes and activities).
- Use goal-based programming instead of programming for specifications

16.3 RESEARCH ACTION #2 STANDARDIZED INTERFACES TO EXTERNAL MODULES AND SYSTEMS FOR PROVIDING IN-DEPTH SECURITY.

DISTANCE TO THE MARKET: TRL 7

COST OF THE TOPIC: 3 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 42 months

ACTORS: home automation systems, cyber-physical systems, interacting SW/HW modules

Trusted and standard software interfaces as well as secure hardware interfaces are the building blocks upon which we have to build Trusted Computing in a highly automated environment. The main goals of trusted software/hardware components are to guarantee a standard level of security and to increase usability of components while accessing services offered by untrusted modules or systems (e.g., services offered by third parties). Furthermore, standard trusted components facilitate maintenance of the overall system, allowing focusing most of securing efforts on single systems/components and easing preventive-monitoring activities.

To enhance systems' security, we should promote a key principle of design that provides for denying full access to available resources by default. Access to resources should be always brokered by interfaces providing well-defined entry-points. Providing direct access to untrusted/uncontrolled modules/systems, could lead to disastrous results in terms of integrity and availability of highly automated components/services. Development and usage of property management gateways is strongly suggested so as that interacting subsystems and modules could be more reliable, secure and safe.

16.4 RESEARCH ACTION #3 COMPONENT AND SYSTEM LEVEL PENETRATION-TESTING PROCEDURES DURING DEVELOPMENT AND INTEGRATION OF COMPLEX SYSTEMS.

DISTANCE TO THE MARKET: TRL 6

COST OF THE TOPIC: 3 STREPs + 2 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 42 months

ACTORS: penetration testers, software developers, ICT Security industry, cyber-physical systems, swarms, grids, clouds, complex environments

The development and integration activities related to components and systems parts of complex and heterogeneous environment (e.g. cyber-physical systems, swarms, grids, clouds, etc.), should always include systematic penetration-test activities. As well as unit and integration tests are executed during software development in order to fulfil functional and non-functional requirements and to detect unpredicted behaviours, component and system level penetration-tests should always be run as a mitigating action against possible future attacks brought either at system or at module/component level. Proper supporting methodologies, tools and techniques needs to be developed.

16.5 RESEARCH ACTION #4 EXTENDING CURRENT SECURITY ARCHITECTURES TO LARGE DISTRIBUTED SYSTEMS INCLUDING PLAYERS WITH DIFFERENT BACKGROUND KNOWLEDGE IN SECURITY. FURTHERMORE, NEW AUTHENTICATION MECHANISMS NEED TO BE DEvised THAT PROVIDE USABLE SECURITY AND CONTINUOUS AUTHENTICATION.

DISTANCE TO THE MARKET: TRL 3

COST OF THE TOPIC: 6 STREPs + 4 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 2

TIME SPAN FOR ADDRESSING THE ACTION: 54 months

ACTORS: ICT Security industry, research centres specialized in security, software developers, standardization bodies

Developing secure application architectures in large distributed systems is surely a big challenge. Secure design principles and well-known best-practices must be taken into account since the early design stages facing the big issues raised by the usage of distributed, complex systems and by the novel paradigms (e.g. cyber-physical systems, swarms, grids, clouds, etc.) each with its own uniqueness and challenges. The adoption of security-by-design principles, of design/coding standards and standardized interfaces to access resources/services, should also aim to reduce any issue related to potential security skill-gaps of the different stakeholders involved in the development of systems or components. Authentication mechanisms (also between modules/components when applicable) must be improved and adapted to novel, complex environments: they have to be also simpler, more effective and usable. Continuous authentication techniques should also be further developed and widely adopted.

16.6 RESEARCH ACTION #5 METHODOLOGIES TO INCREASE PREPAREDNESS AND RESPONSIVENESS IN CASE OF ATTACK, INCLUDING ATTACKS TARGETING PRODUCTION PROCESS (E.G. TO INSERT MALWARE, BACKDOORS OR TROJAN IN FINAL PRODUCTS).

DISTANCE TO THE MARKET: TRL 6

COST OF THE TOPIC: 6 STREPs + 3 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 3

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: cyber-physical systems, software, hardware, IoT, IoS, system developers, integrators, importers, stockists

In recent years, software and hardware manufacturers - even some of the smallest one in the value chain – have been affected by attacks to their production line and processes. Mainly motivated by espionage purposes or by criminal lucrative intents, these attacks aimed at compromising the integrity of legitimate software/firmware injecting malware, backdoors or Trojans in final products. The potential impact of such kind of attacks is huge: imagine what could happen if the tampered firmware of a PC's motherboard would be replicated in hundred thousands of copies and sold in tens of different countries of the world.

New methodologies and tools to mitigate the risk of such kind of attacks happening need to be developed.

Software production lines must be considered an attractive target and an asset to defend from potential insiders and cyberattacks. The integrity of software and production processes should be monitored and granted at all times. Incident management procedures (including proper countermeasures) should be in place and personnel should be properly trained.



16.7 RESEARCH ACTION #6 INTELLIGENT IDS, HARDENING MECHANISMS AND AWARENESS.

DISTANCE TO THE MARKET: TRL 5

COST OF THE TOPIC: 8 STREPs + 4 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 3

TIME SPAN FOR ADDRESSING THE ACTION: 52 months

ACTORS: ICT professionals, ICT Security vendors, ICT vendors, standardization bodies, educators

When facing novel threats, current signature/rule-based IDS systems show their limits: it is necessary to develop a new generation of autonomous, intelligent, adaptive IDS systems that for example should be able to learn new ways to mitigate or counter previously unknown attacks by experience and by inference and logic.

While keeping them effective, system hardening techniques must be simplified and proper tools and techniques developed (e.g. driven procedures to reduce the attack surface without the need to own deep security skills). Hardening should be taken into account in system design, development and delivery phases.

While struggling to counter increasingly sophisticated attacks, according to statistics the most effective techniques are still relatively simple and well-known. That's why awareness campaigns, tools and methodologies must be further developed for professionals implied in software development and system design.

16.8 RESEARCH ACTIONS GANTT

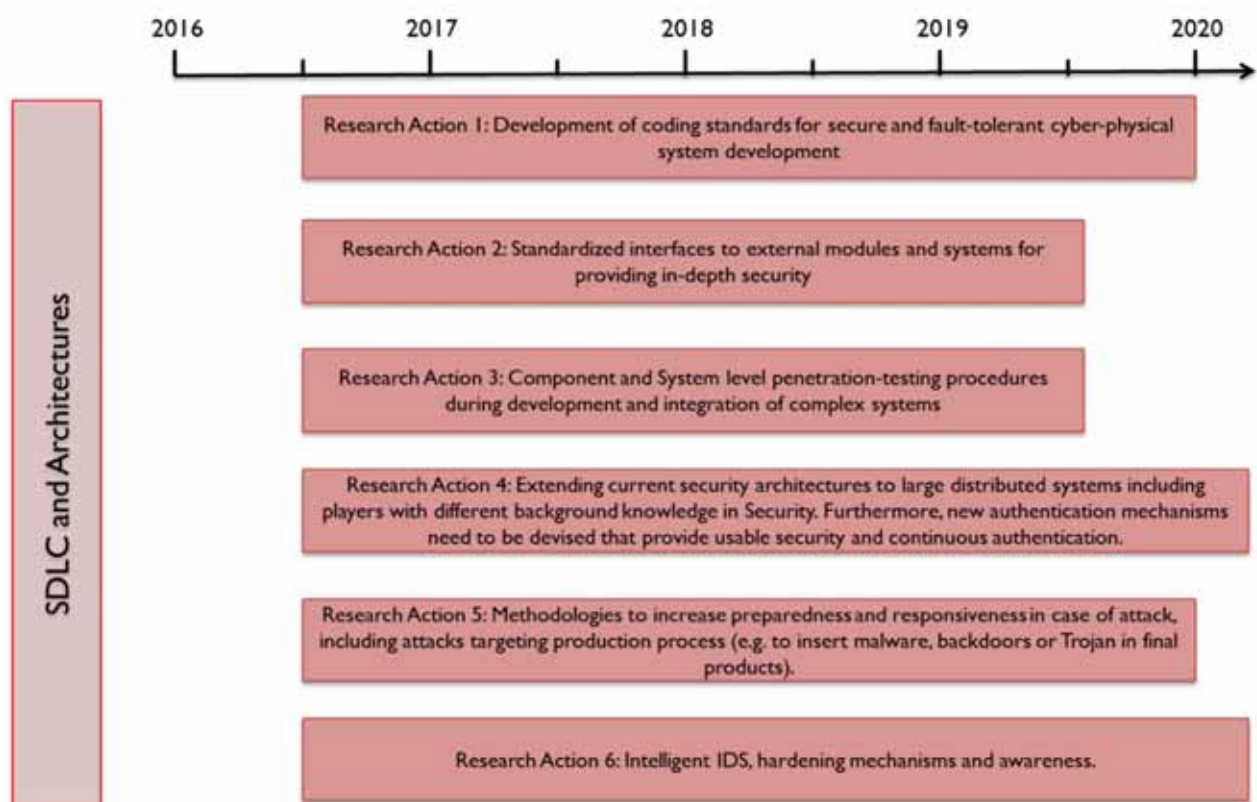


Figure 26 - SDLC & Architectures



17 THREAT INTELLIGENCE AND ATTACK DETECTION

CC RG-1 and CT RG-1	Threat and attack intelligence, attack simulation infrastructures
CC RG 2	Automatic malware research, advanced automatic malware defence and shielding
CC RG-5	Research on information propagation in non-centralized media (available research is available on state-controlled media)
CT RG-13	Develop realistic threat model for wearable devices
CC RG-18	Innovative process-aware behavioural-based intrusion detection system capable of identifying any deviation from normal activities for the processes being monitored
CT RG-32	How to engage operators/exchangers in information exchange
CC RG-32, CC RG-54, CT RG-54	Early detection of supply chain attacks
CC RG-38, CT RG-38 and CT RG-50	Gathering knowledge about attack statistics per critical component
CC RG-39, CT RG-39 and CT RG-10	Infrastructures for attack simulations
CC RG-84	Technologies to monitor and control the production process and detect deviations from acceptable behaviour
CC RG-89	Advanced anti-phishing solutions
CC RG-96	Research on advanced malware detection and prevention techniques on mobile devices
CC RG-99	Intelligent IDS, hardening mechanisms and awareness
CC RG-105	Advanced techniques for DDOS detection

17.1 ABSTRACT

The increasing use of ICT in more areas of human activity has created new possible threats and attack modalities compromising a variety of different targets. New technologies such as IoT, Wearables etc. are not hardened against cyber-attacks. Critical Industrial Systems are targets of new malware. DDOS and phishing attacks have become more common than ever, while new threats and new types of malware (such as ransomware, mining malware etc.) prove difficult to combat. It is, therefore, an imperative need to further improve threat intelligence and gain a better understanding of how threats develop and what makes them persist. Therefore, actions are expected to lead to improved threat intelligence and threat modelling, solutions to simulate attacks, design of component- and system-level penetration testing, intrusion and attack detection and overall improved protection of a variety of targets, be it desktop/mobile devices, wearables, individuals, IoT etc.



17.2 RESEARCH ACTION #1 THREAT AND ATTACK INTELLIGENCE IMPROVEMENT, BY DEVELOPING ATTACK SIMULATION INFRASTRUCTURES AND ADVANCED RISK ANALYSIS AND MODELLING.

DISTANCE TO THE MARKET: TRL 5-7

COST OF THE TOPIC: 2 STREPs + 1 IPs

AVAILABILITY OF COMPETENCE IN EUROPE: 3

TIME SPAN FOR ADDRESSING THE ACTION: 42 months

ACTORS: government, military, IT security industry, research/academia, critical infrastructure operators, law enforcement, CERTs/CSIRTs

The evolution of cyber-attacks and the continuous development of more sophisticated tactics, techniques and procedures usually overcomes most traditional security measures. Therefore, in order to better understand where are the weakest points that are being exploited and to test current or future protection solutions, we need to develop attack simulation structures. This will help to create the more specific conditions where an attack can take place and design or adjust security measures focused on specific needs and requirements.

Realistic attack simulation will contribute to the advanced threat modelling that will result in a more efficient dynamic risk analysis of current and near future attacks. It will also feed with valuable information the intelligence lifecycle that will produce more reliable and accurate threat intelligence.

The great value of an attack simulation infrastructure will improve the knowledge of attack context improving significantly the quality of threat intelligence and detection operations. It is also expected to lead to the design of solutions for component- and system-level penetration testing.

17.3 RESEARCH ACTION #2 INTELLIGENT INTRUSION AND MALWARE DETECTION, SYSTEM HARDENING AND SITUATION AWARENESS ACROSS A COMPLEX ENVIRONMENT.

DISTANCE TO THE MARKET: TRL 5-7

COST OF THE TOPIC: 2 STREPs + 2 IPs

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 52 months

ACTORS: government, military, IT security industry, research/academia, critical infrastructure operators, law enforcement, CERTs/CSIRTs

Attack detection currently relies mainly on known attack patterns and techniques. There is also a behavioural analysis and reputation model but with not sufficient results especially in avoiding false positives.

Although it is commonly accepted that protective measures have limited efficiency and more effort should be put in reactive – response measures, proactive defence still remains the first layer of security and needs continuous update and improvement.

The main objective of preventive security operations remains the block of intrusion attempts. This combined with advanced hardening and situation awareness can deliver better results in preventing cyber-attacks before being executed at the targeted environment.

Current intrusion and malware detection technologies need to be further improved by integrating advanced intelligence mechanisms, big data analytical procedures, prediction techniques in order to address threats and on-going attacks in a timely and efficient way.

The biggest challenge in the future will be to handle and manage a complex cyber environment with many different devices and technologies that keep growing (e.g. IoT, wearable devices, social media offering data as a commodity etc.)



17.4 RESEARCH ACTION #3 PROTECTION OF ORGANISATIONS FROM CRITICAL DATA LEAKS CAUSED BY INTENTIONAL OR UNINTENTIONAL INSIDER THREATS.

DISTANCE TO THE MARKET: TRL 5-7

COST OF THE TOPIC: 1-2 STREPs + 2 IPs

AVAILABILITY OF COMPETENCE IN EUROPE: 3

TIME SPAN FOR ADDRESSING THE ACTION: 56 months

ACTORS: government, military, IT security industry, research/academia, critical infrastructure operators, law enforcement, social media companies

Leaks of sensitive or even classified material is a major and growing concern among a variety of different organisations. An employee might commonly disclose important information unintentionally due to misuse of social media, lost or stolen personal devices containing sensitive material, falling victim to cyber-attacks such as phishing, click-jacking or other social engineering attacks etc. In other cases, a person might willingly disclose information for malicious purposes, sometimes even after termination due to poor administration of personal accounts.

In order to minimise the risk of critical data leaks, organisations require cost-effective and socially acceptable solutions for:

- Employee pre-screening processes that are compliant with EU legislation on privacy and non-discrimination,
- Proper device management,
- Social Media management,
- Employee training and tools to protect against phishing, click-jacking and social engineering attacks,
- Accountability processes that can uncover erratic behaviours indicating a possible insider threat,
- Proper employee termination processes that minimise the risk of leaked data.

Social acceptance of such solutions is also a major factor that could hinder their adoption. Proposed solutions should take into account the EU legislation on privacy and non-discrimination and be respectful to the employees' dignity and human rights. Furthermore, solutions should be as less intrusive and disrupting to everyday workflow as possible.

17.5 RESEARCH ACTION #4 UNDERSTANDING THE ECONOMIC IMPACT OF DIGITAL CURRENCIES AND THEIR ROLE IN ENABLING NEW FORMS OF CYBER AND ORGANISED CRIME.

DISTANCE TO THE MARKET: TRL 5-7

COST OF THE TOPIC: 2 STREP + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 3

TIME SPAN FOR ADDRESSING THE ACTION: 42 months

ACTORS: law enforcement, research/academia, ICT industry, government

Digital currencies have recently arisen as Internet-based services that enable on-the-spot, cross-border, irreversible exchange of money or ownership, illustrating similar properties as physical/national currencies. In the past few years, hundreds of digital currencies have been created, following either more stable/centralised or volatile/decentralised architectures.

The rapid and irreversible use of such currencies along with improved anonymity and have created a new market sector and have enabled new business models to flourish. Law enforcement, however, has also recognised that they enable criminal activity ranging from money laundering and tax evasion to illegal immigration and trafficking. Furthermore, new forms of cybercrime have appeared such as:

- New forms of malware: Digital currency processes are often computationally intensive. Digital currency users might voluntarily offer use of their own systems' processing power in exchange for compensation, a process known as mining. This has lead cybercriminals to mining malware that installs on desktop or mobile devices and utilises their processing power to generate illicit revenue.
- Currency Mixing: Mixing is the process of obfuscating the source of a transaction by mixing different currencies and funds, usually for a transaction fee.
- "Crime-as-a-Service": Europol warns that digital currencies enable cybercriminals to come together in an ad-hoc, per-project basis thus forming a new "Crime-as-a-Service" business model.

Law enforcement thus faces novel challenges related to digital currencies. In order to combat new forms of cyber and organised crime fostered by decentralised digital currencies, there needs to be:

- an in-depth understanding and econometric analysis of business models arising from digital currencies,
- an analysis of possible gaps in EU legislation that enable unregulated use of digital currencies,
- an analysis of the profiles and behavioural patterns of legitimate and illicit digital currency users,
- Further analysis of the technical aspects should lead to the creation of tools to improve tracing of illicit transactions,
- Mitigation of new malware threats such as mining malware.



17.6 RESEARCH ACTIONS GANTT

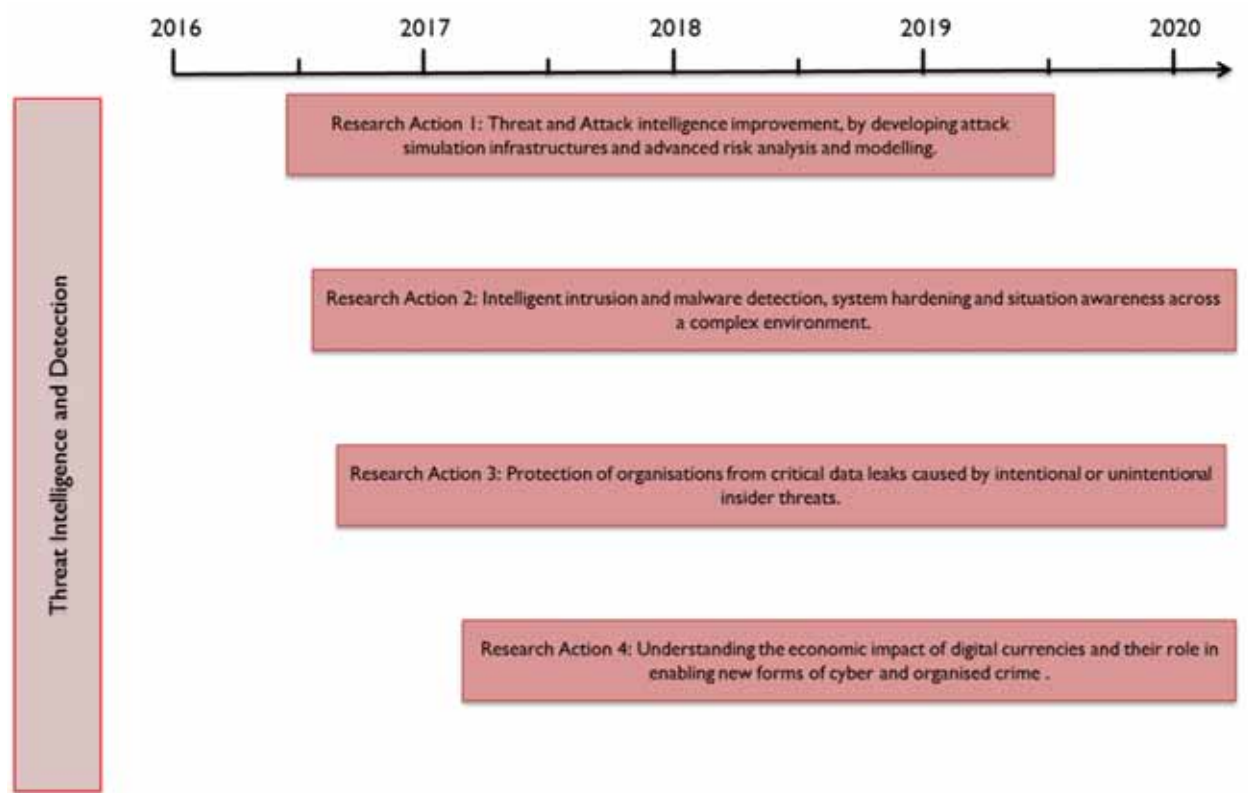


Figure 27 - Threat Intelligence and Attack Detection RAs GANTT



18 TRUST CHAINS AND IDENTITY

CC RG-6 and CT RG-3	Automated ways to identify existing trust chains, improvement of threat management models
CC RG-18 and CT RG-15	New methodologies and architectures for establishing trust between components of a network
CC RG-42 and CT RG-42	Byzantine fault tolerant cyber-physical systems
CC RG-43 and CT RG-43	Secure component certifications
CT RG-77	Code integrity monitoring
CT RT-64	Analysis of the threats that can be generated in financial markets driven by crypto currencies

18.1 ABSTRACT

Trust is a fundamental component in various aspects of individuals' life (e.g., as users of online services, of the healthcare system, and as employees), as well as in organizations (companies, financial institutions, etc.), institutions (e.g., governments), financial markets, and so on. Interactions between the different actors involved in all such contexts are indeed based on underlying trust chains. Trust chains are also implied between components of hardware and/or software systems, and in particular in complex cyber-physical and Internet-of-things systems, whose complexity, autonomy and scope is constantly increasing, even in critical infrastructures (e.g., transportation systems).

Trust chains are undergoing significant changes due to the widespread use of information technology. In particular, less invasive and adaptive devices (the "disappearing computing" phenomenon) are leading to the emergence not only of novel, but also unnoticed trust chains.

Under this viewpoint, the essence of cybercrime is the abuse of unprotected trust chains. For instance, cyber criminals can abuse the trust chains between individuals to steal personal, sensitive data (e.g., by a phishing attack); similarly, cyber terrorists can exploit vulnerabilities in the trust chains between hardware and/or software components to disrupt cyber-physical systems that control critical infrastructures; they can also abuse the novel trust chains underlying financial markets to disrupt them. More specifically, any attack can be seen as abusing a trust boundary that surrounds a given asset. The identification of trust boundaries is indeed one of the main steps in threat modeling; they are also one of the elements of the threat definition language developed by Microsoft, and widely used by many organizations, including the Open Web Application Security Project (OWASP).

18.2 RESEARCH ACTION #1 TRUST CHAINS BETWEEN INDIVIDUALS.

DISTANCE TO THE MARKET: 5 (TRL)

COST OF THE TOPIC: 3 STREPs

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 36 months

ACTORS: universities, research institutions

Information technologies are profoundly changing the relationships between individuals, and between individuals and organizations, or institutions. One of the effects is the change in the underlying trust chains, and the emergence of novel and even unnoticed ones, due to the disappearing computing and immersed human paradigms. This exposes trust chains to several kinds of abuses.

For instance, the access to personal information in social networking sites is regulated by a network of trust implied by relationships; however, issues like the lack of strong authentication mechanisms or the



willingness to increase one's own popularity can lead to exposing personal information to unknown people, which can lead to a poisoning of the network of trust.

As another example, in the working life of individuals new habits like bring-your-own-device (BYOD), working at home, usage of cloud services, etc., cause the disappearance of the traditional enterprise trust zone, exposing corporate information systems to several new threats coming from different sources (e.g., employees are more easily targeted by modern social engineering attacks).

Analogous issues emerge from rapidly changing environments like healthcare systems.

In general, the digital "ecosystems" supporting the digital experience continuity are nowadays specialized for different contexts: for example, the smartcars ecosystem or the home automation ecosystem. The spreading of a blended style of living across a wide range of citizens, and the seamless experience offered by the digital ecosystems, also enable seamless deception techniques. This implies that services today must have a high degree of Contextual Intelligent Quotient (CQ), i.e., the ability to constantly analyse the surrounding reality from different, uncorrelated points of view and to adjust the decision making process in a matter of days/weeks.

To address these issues, it is therefore important to:

- identifying the underlying trust chains in a given context
- make users, or a whole ecosystem, aware when some of the underlying trust chains are being abused
- understand how users can be part of the protection system without altering their usage experience or transferring responsibilities to them.

18.3 RESEARCH ACTION #2 TRUST CHAINS IN CYBER-PHYSICAL SYSTEMS, IOT, AND SUPPLY CHAINS.

DISTANCE TO THE MARKET: 4 (TRL)

COST OF THE TOPIC: 4 STREPs, 1 IPs

AVAILABILITY OF COMPETENCE IN EUROPE: 4

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: universities, research institutions, industry, critical infrastructure organizations, standardization bodies

Cyber-physical systems and the Internet-of-things (IoT) are becoming an essential component in fields like building automation and in critical infrastructures like transportation systems. They involve complex hardware and software architectures, with the interaction of a number of different devices, sensors and software modules, with different protocols, standards and interfaces. Such systems are exposed to risks like remote manipulation, e.g., to get unauthorized access to a smart building, to disrupt cyber components, and to impact on the operational capabilities and performance of cyber/physical assets.

A specific issue related to the digital infrastructure is the reliance on trusted hardware and software components in the supply chain, to avoid the usage of compromised components (e.g., with a back door). Current efforts in the field of trusted software components are based on the Component-Based Software Engineering methodology, and the Trusted Platform Module implementation of trusted hardware components proposed by the Trusted Computing Group. However, several issues exist. For instance, "market places" that sell and share trusted software components can be infiltrated by cyber criminals, to modify or to replace components with vulnerable ones; the same standardization processes for secure software components might be undermined, as well as certification authorities of trusted hardware and software components that are likely to be established in the near future; cyber terrorists may even create components that individually pass formal verification tests, but behave maliciously in combination and using a specific set of input parameters.

To address the above issues, research is needed in the following areas:

- solutions for establishing trust between the different components of a network, focusing on the interfaces to external modules and systems
- risk analysis and modelling for cyber-physical systems, aimed at enabling Byzantine fault tolerance

- developing standards and protocols for secure component certifications
- improvement of techniques for monitoring code integrity based on checksums

18.4 RESEARCH ACTION #3 TRUST CHAINS IN FINANCIAL MARKETS.

DISTANCE TO THE MARKET: 3 (TRL)

COST OF THE TOPIC: 3 STREPs

AVAILABILITY OF COMPETENCE IN EUROPE: 3

TIME SPAN FOR ADDRESSING THE ACTION: 36 months

ACTORS: universities, research institutions, governments, financial institutions

Financial services are a specific sector affected by the changes in traditional trust chains, and by the emergence of novel ones, as a consequence of disintermediation and decentralization. Financial transactions are managed by increasingly long sequences of peer financial intermediaries, which are not guaranteed to adopt the same quality standards. The trust chains between them become therefore less clear. There are some ongoing efforts in this area, like the development of Payment Card Industry (PCI) standards by the PCI Security Standards Council. They are however not yet satisfactory; for instance, they do not involve bank clerks and their software.

The introduction of crypto currencies like Bitcoin is a prominent example of the replacement of traditional networks of trust (in this case, societal structures like governments) with a distributed network that can act as a third-party trust mechanism. More importantly, the block-chain technology, originally developed as the Bitcoin backbone, is likely to have a relevant role in the development of a number of novel applications involving financial transactions, as well as transactions of different kinds, replacing the networks of trust currently involving centralised institutions and bureaucracies. In essence, the block-chain is a shared, trusted, public, distributed database of transactions based on the peer-to-peer technology, that can be inspected by every user, but cannot be controlled by any single user.

The above changes in the trust chains expose financial markets to several risks, up to their disruption. A thorough analysis of the possible threats is necessary, in order to develop suitable, technical and policy solutions (e.g., encryption among the former, and regulatory frameworks for operators and exchangers among the latter), as well as to increase awareness among financial markets operators.



18.5 RESEARCH ACTIONS GANTT

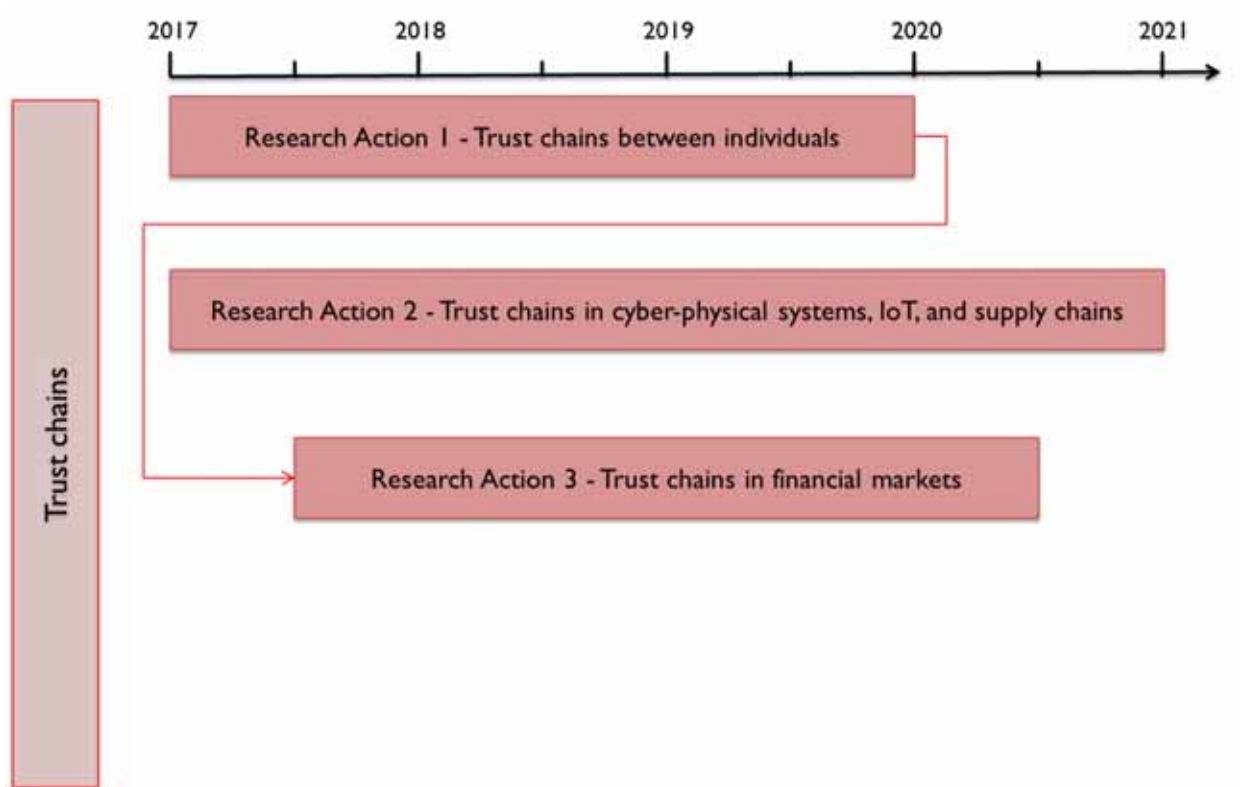


Figure 28 - Trust Chains and Identity RAs GANTT



19 VULNERABILITY ASSESSMENT

CC RG-40	Component and System level penetration testing procedures during development and integration of complex systems
CC RG-44	Assess vulnerabilities and risks of integrating ICT components in physical/embedded systems or field devices
CC RG-49	Attack simulations
CC RG-50	Component level penetration testing
CT RG-51	Component level penetration testing
CC RG-87 and CT RG-84	Assessment tools for specific vulnerabilities of data exchange nodes

19.1 ABSTRACT

The level and diversity of cyber threats that citizens, companies, public authorities and society in general is currently facing is unprecedented and all forecasts indicate that it will tend to get worse, due to multiple factors.

Of particular concern is the fact that mobile platforms for personal and professional usage, like smartphones and tablets are increasingly present in today's society. Companies are slowly adopting BYOD (bring-your-own-device) policies, integrating user's devices into their infrastructure and using new professional applications in their daily activities. Although major platforms like Android and iOS try to establish some security in their architecture, the proliferation of malware in the official application distribution channels, as well as speculation about pre-installed malware at factory level, has demonstrated that current security levels are insufficient and current vulnerability assessment methods are inappropriate for the current level of threats.

Threats to cyber-physical systems, e.g. to disrupt cyber components, impacting operational capabilities and performance of cyber/physical assets, as well as cyber-attacks applied to entire company systems are now common place, and in many cases they seem to be "state-sponsored" to some extent. Malware attacks against industrial systems, as well as specifically targeted malware (using software and hardware components) are now a real threat to the multitude of critical infrastructure operators that support the core functions of modern society.

To address and mitigate the above mentioned threats, it is essential to be able to clearly assess the level of cyber vulnerability existing in each component, model, system, procedure and entity (company, etc.), which are interconnected and can produce cascading effects beyond the obvious. Only in this way it can be possible to fully understand, in a continuous way, what needs to be corrected and the level of resources that will eventually be needed. To achieve this objective, a new type of vulnerability assessment tools and procedures is needed, that can go beyond currently used penetration testing and equivalent procedures.

19.2 RESEARCH ACTION #1 VULNERABILITY ASSESSMENT TOOLS AND PROCEDURES.

DISTANCE TO THE MARKET: TRL 5-7

COST OF THE TOPIC: 2 STREPs + 1 IP

AVAILABILITY OF COMPETENCE IN EUROPE: 5

TIME SPAN FOR ADDRESSING THE ACTION: 48 months

ACTORS: national cybersecurity centres, law enforcement agencies, IT security industry, high-tech SMEs, research/academia, critical infrastructure operators, public authorities, electronics and semiconductor industry



Penetration testing as a technique to validate system security has been around for several decades, but only in the last 15 years it has grown into a full blown industry. The technique involves active analysis of target systems for potential software vulnerabilities, operational weaknesses, including people and the processes the system is part of. It is done so, by simulating an attack to the system employing automated tools or manual actions, or both, in order to violate some security properties of the system or process.

Different methodologies have been defined providing completeness and effectiveness of the performed tests and a wide range of certifications for security testers (CPT, CPTE, CompTIA, CSTA, GPEN, OSCP, CEH, CEPT, etc.) has been developed giving customers some assurance about the contracted services.

Independently from the chosen method, penetration testing depends on a good characterization of the target infrastructure. One of the first steps after identifying the target (differently represented in each methodology) is to understand the security assumptions, the threats and identify the goals of the test. This can typically be achieved by building some kind of attack tree that will guide the tests to be conducted. Tools are used to assist in fields such as: vulnerability assessment, fuzzing, brute forcing, SQL injection, exploitation frameworks, protocol analysis, reverse engineering, etc.

Other tools try to minimize the security analyst's work by performing dynamic application security testing simulating an attacker. Nevertheless, fully automated broad spectrum security testing is always of limited utility and manual tuning is required for trustable results.

What is now envisioned is a new level of vulnerability assessment tools and procedures, that can go beyond currently used penetration testing and equivalent procedures. These should include, among other innovative features: advanced risk analysis and modelling, security testing at all points of data exchange and component level penetration testing.

The minimum expected outcome from the proposed action should include, but not be limited to, the following deliverables:

- Component and system level penetration testing procedures used during development and integration of complex systems.
- Assess vulnerabilities and risks of integrating ICT components in physical/embedded systems or field devices.
- Attack simulations.
- Component level penetration testing.
- Assessment tools for specific vulnerabilities of data exchange nodes.



19.3 RESEARCH ACTIONS GANTT

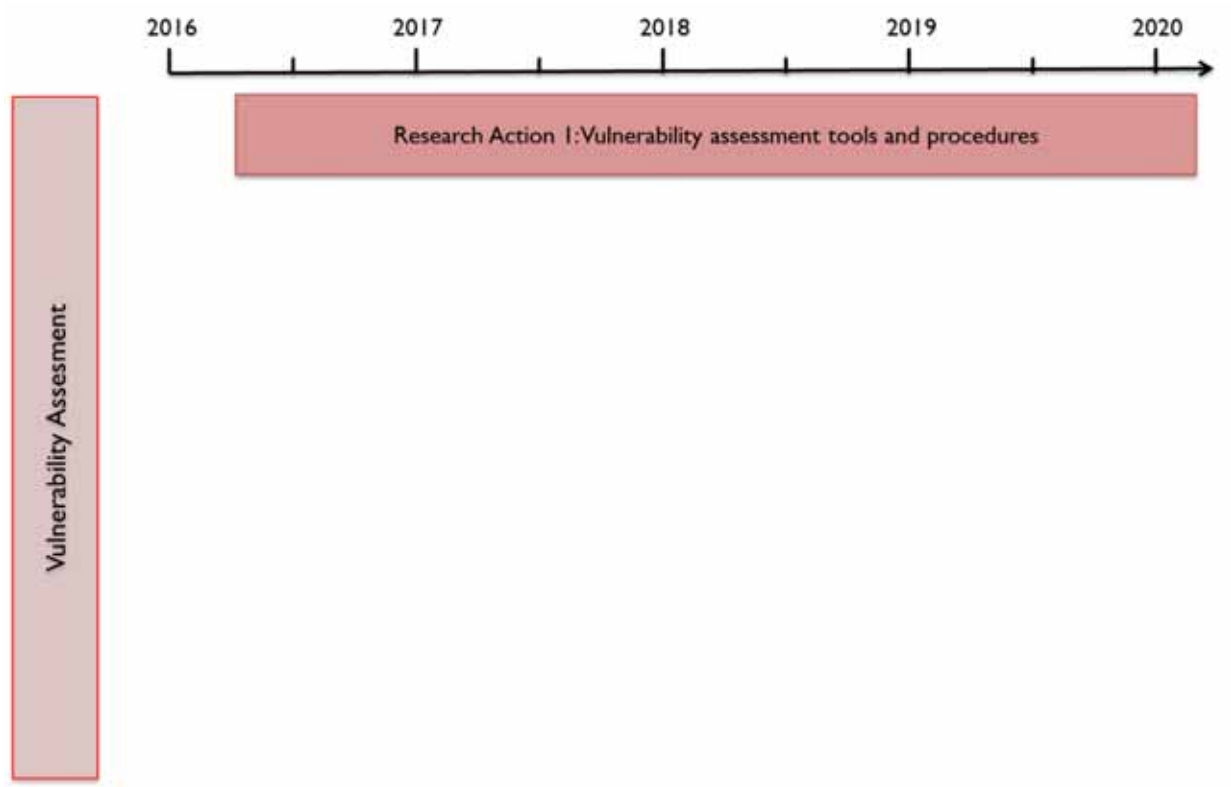


Figure 29 - Vulnerability Assessment RAs GANTT

ANNEX I - TEMPLATE FOR THE DESCRIPTION OF THE RESEARCH TOPICS AND ACTIONS

ABSTRACT	 <p>Funded by the European Commission Seventh Framework Programme</p>
	 <p>Cyber ROAD Development of the Cybercrime and Cyber-terrorism Research Roadmap Grant Agreement N. 607642</p>
	<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit</p> <p>Author(s): John Doe, Jane Doe</p> <p>GAP #1 - Lorem ipsum dolor sit amet, consectetur adipiscing elit GAP #2 - Lorem ipsum dolor sit amet, consectetur adipiscing elit GAP #3 - Lorem ipsum dolor sit amet, consectetur adipiscing elit</p>
	<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla.</p>
	 <p>D2.3 Final Roadmap Funded by the European Commission under the Seventh Framework Programme</p>
	Page 1 of 3

RESEARCH
ACTION # 2.A

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt?

- *Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt?*

DISTANCE TO THE MARKET: 0
COST OF THE TOPIC: 0 STREPs + 0 IP
AVAILABILITY OF COMPETENCE IN EUROPE: 0
TIME SPAN FOR ADDRESSING THE ACTION: 0 months
ACTORS: Lorem ipsum dolor sit amet

(Write description here)

RESEARCH
ACTION # 2.B

Lorem ipsum dolor sit amet, consectetur adipiscing elit?

DISTANCE TO THE MARKET: 0
COST OF THE TOPIC: 0 STREPs + 0 IP
AVAILABILITY OF COMPETENCE IN EUROPE: 0
TIME SPAN FOR ADDRESSING THE ACTION: 0 months
ACTORS: Lorem ipsum dolor sit amet

(Write description here)



D2.3 Final Roadmap

Funded by the European Commission under the Seventh Framework Programme

Page 2 of 3



D2.3 Final Roadmap

Funded by the European Commission under the Seventh Framework Programme

Page 85 of 91

Lorem ipsum dolor sit amet, consectetur adipiscing elit?

DISTANCE TO THE MARKET: 0
COST OF THE TOPIC: 0 STREPs + 0 IP
AVAILABILITY OF COMPETENCE IN EUROPE: 0
TIME SPAN FOR ADDRESSING THE ACTION: 0 months
ACTORS: Lorem ipsum dolor sit amet

(Write description here)



D2.3 Final Roadmap

Funded by the European Commission under the Seventh Framework Programme

Page 3 of 3

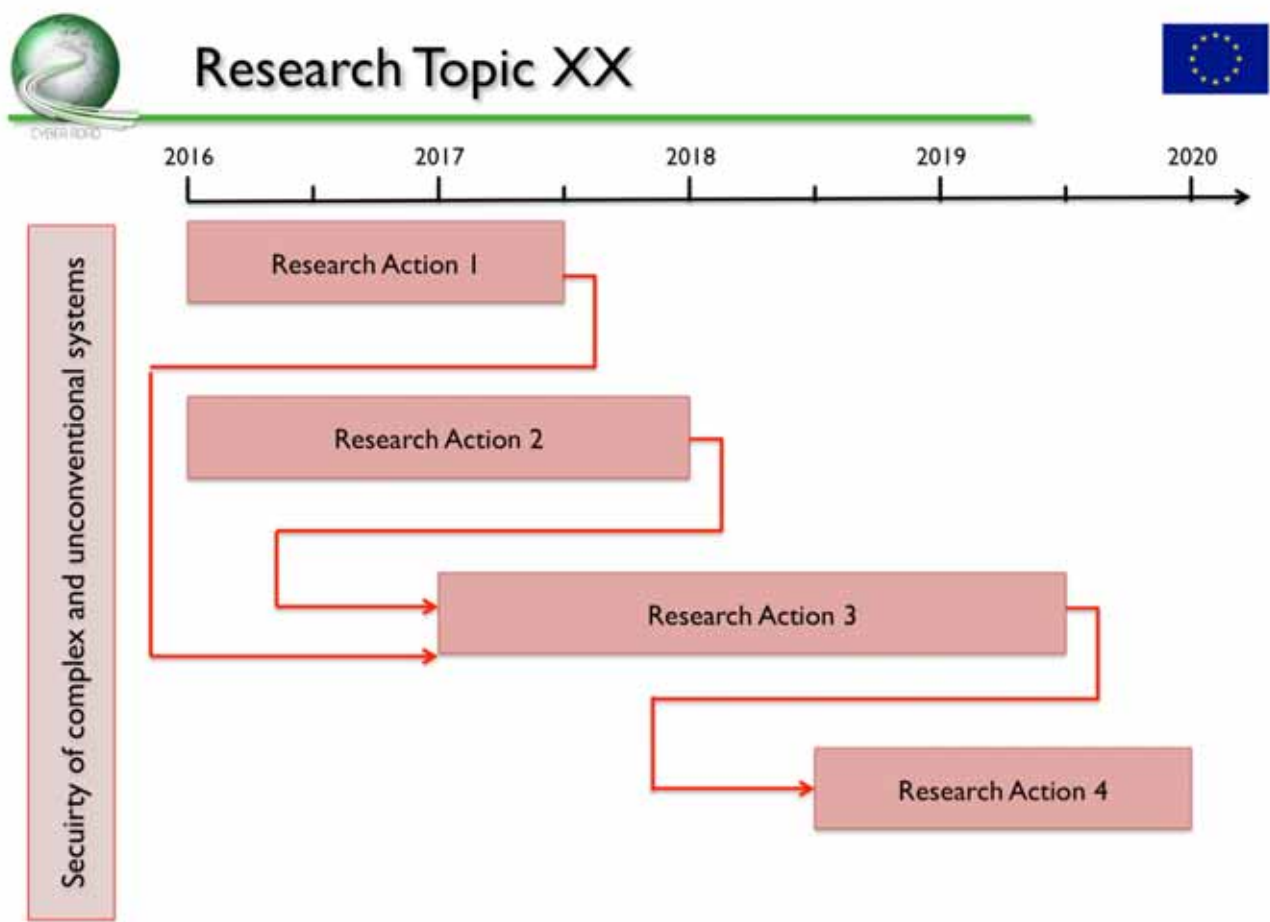


D2.3 Final Roadmap

Funded by the European Commission under the Seventh Framework Programme

Page 86 of 91

ANNEX II - TEMPLATE FOR THE GANTT DIAGRAM ASSOCIATED WITH EVERY RESEARCH TOPIC



ANNEX III - TEMPLATE FOR THE PRIORITIZATION OF THE RESEARCH TOPICS

Template for the prioritization of the Research Topics.

Research topic	Threat	Asset Types	Affect ed asset	Data Breach Risk Consequence	Health & Safety Risk Consequence	Financial Risk consequence	Intangibl e Risk Consequence	Likelyh ood
[Research Topic Name]	Accidental leak <i>The agent is "friendly user" and intends to protect assets, but accidentally or mistakenly takes actions that result in harm.</i>	Access Data						
		Personal Data						
		Commercially Sensitive Data						
		Intellectual Property						
		Procedures and Processes						
	Denial of Service <i>Not only DoS but starvation in general at all the levels (NTW, system, service or storage)</i>	Plant and Equipment						
		Personal data						
		Business/Service						
	Eavesdropping, Interception and Hijacking <i>Secretly listening to the private conversation and intercepting data during their transferring (es. MITM)</i>	Access Data						
		Personal data						
		Commercially Sensitive Data						
		Intellectual Property						
	Espionage	Commercially Sensitive Data						
		Intellectual Property						
		Procedures and Processes						
	Financial Fraud	Money						
		Reputation						
	Misuse <i>Benign shortcuts and misuse of authorizations, "pushed wrong button". Current employee with harmless intent but unknowingly misuses system or</i>	Reputation						
		Procedure and process						
		Personal data						
		People						



	<i>safeguards</i>							
	Opportunistic data theft <i>Opportunistic individual with simple profit motive.</i>	Access Data						
		Personal data						
		Commercially Sensitive Data						
		Intellectual Property						
		Business/Service						
	Physical theft	Money						
		Materials						
		Plants and Equipment						
	Product/system alteration <i>Incidental alteration of the products, not intentional like Sabotage</i>	Plants and equipment						
		Materials						
		Reputation						
		People						
		Business/service						
	Sabotage <i>Abuse of privileges for sabotage, cyber or physical.</i>	Plants and Equipment						
		Procedures and Processes						
		People						
		Reputation						
	Violence <i>Violent acts toward people</i>	People						
		Reputation						

Scales for the evaluation of the consequences for Data Breach, Health and Safety, Financial, and Intangible Risks.

Data Breach Risk Consequence		Definitions
	10	Large/Severe
	5	Medium
	2	Low/Moderate
		Minor
	1	

Health & Safety Risk Consequence		Definitions
	50	Large/Severe
	10	Medium
	2	Low/Moderate
	1	Minor

Financial Risk consequence		Definitions
	10	Large/Severe
	5	Medium
	2	Low/Moderate
	1	Minor

Intangible Risk Consequence	Definitions
-----------------------------	-------------



10	Large/Severe
5	Medium
2	Low/Moderate
1	Minor

Likelihood	Definitions
10	Highly probable/Likely
5	Medium/Possible
2	Low/Remote
1	Negligible/Unlikely