Date of deliverable: 31/07/2015 CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. 607642

D3.2 Evaluation of stakeholder needs

Actual submission date: 31/08/2015

Start date of the Project: 1st June 2014. Duration: 24 months

Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab

Version: Final

Project funded by the European Commission Directorate-General Home Affairs in the Prevention of and Fight against Crime Programme		
Restriction Level		
PU	**Public**	
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)**	

Revision history

Version	Object	Date	Author(s)
0.1	Creation	01/06/2015	PJ
0.2	Revision	02/06/2015	PJ
0.3	Revision	31/07/2015	PJ
0.4	Final draft	22/08/2015	PJ
1.0	Final	31/08/2015	RHUL, UNICA

D3.2
Evaluation of stakeholder needs

Responsible
POLÍCIA JUDICIÁRIA

Contributor (s)
Polícia Judiciária
POSTEIT
Cyberdefcon
SBA
MELANI

Contents

LIST OF TABLES

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

Acronym	**Definition**
CAMINO	**C**omprehensive **A**pproach to cyber road**M**ap coord**I**Nation and devel**O**pment
CoE	**C**ouncil of **E**urope
COuRAGE	**C**ybercrime and cyberterr**O**rism (**E**)Uropean **R**esearch **AGE**nda
EAP Project	**Ea**stern **P**artnership – Cooperation against Cybercrime
FIUs	**F**inancial **I**nformation **U**nits
GCC	**G**reek **C**ybercrime **C**enter
GLACY	***G***loba**l** **A**ction on **Cy**bercrime
ISTAT	**I**stituto Nazionale di **Sta**tistica (Italian National Institute of Statistics)

LEA	**L**aw **E**nforcements **A**gency
NECOMA	**N**ippon-**E**uropean **C**yberdefense-**O**riented **M**ultilayer threat **A**nalysis
RASI	**R**elatório **N**acional de **S**egurança **I**nterna
ISP	**I**nternet **S**ervice **P**rovider

EXECUTIVE SUMMARY

We are living an era characterized by worldwide exchanges and connections: globalization. It affects, and is in turn also affected by, technological innovations, geopolitics and economics. The changes it has introduced are wide reaching. One of these changes is for instance society's new take on the meaning of "distance". It is now easier than ever to obtain information about evenements happening on the other side of the globe, even in a remote isolated corner (LIPOVETSKY & JUVIN, 2010). It has similarly become easier to commit crime usuing computers based from one continent but with victims located in another one.

Computer has become an essencial element of economic, cultural and social activity. Our society has become entirely dependent on the continuous availability, accuracy and confidentiality of Information and Communication Technology (ICT). Technology has thus enabled old crimes to be committed through new and subtler *modus operandi* (UK GOVERNMENT, 2011).

This report summarises a number of national initiatives to identify the stakeholders and their needs when responding to cyber crime. The report reflects on the data gathering activities to date of CyberRoad in this area together with national reports published on the topic and analyses this data to identify where cybercrime response frameworks should be further strengthened.

INTRODUCTION

As established in CyberRoad's Description of Work, "**The aim of this task is to identify, for each group of relevant stakeholders, the key interests and concerns, and what each stakeholder wants and needs**."

The CyberRoad consortium includes several types of stakeholders, ranging from law enforcement agencies and military forces, to financial institutions, to research bodies and small entreprises. They can provide significant direct expertise and know-how on what they perceive as the main policy to implement to tackle cyber crime.

As a methodology, we started by making a short analysis of a few of the most relevant and similar projects that the Commission financed over the past ten years. The aim was to analyse if and how the projects addressed the stakeholder's needs over the past few years.

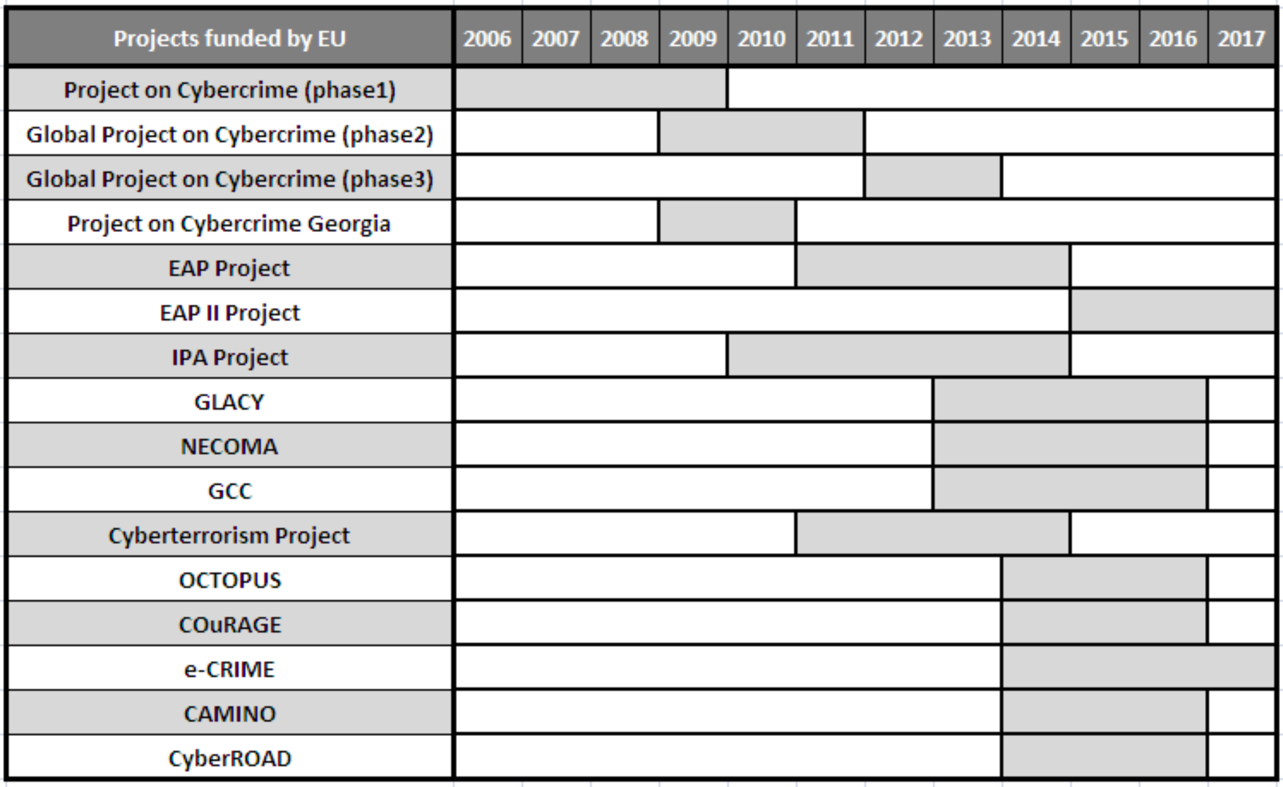
Then, we continued by taking into consideration the results of surveys carried out under Workpackages 5 and 6 of CyberRoad. They also provided significant and up-to-date information from stakeholders who answered the various questions pertaining to their needs. Those stakeholders were reached through the wide network of the partners in the CyberRoad Project and contributed to get a better understanding of the issue.

Making use of the information collected as mentioned before allowed the drawing of conclusions that may be of help to influence future action from the Commission.

I - SHORT ANALYSIS OF SOME EUROPEAN CYBERCRIME PROJECTS

Further to the Cybercrime Convention adopted in Budapest, November 23, 2001, the European Union funded several research and development projects under the FP7 and H2020 programmes. These were aimed at promoting and supporting the implementation of the Convention, both in Europe and worldwide. The projects focused on:

- Capturing the understanding of cybercrime and cyberterrorism;
- Improving education and research in the newly growing area of cybercrime;
- Assessing the impact of cybercrime;
- Delivering specific results in terms of legislation;
- Enabling and strengthening criminal justice authorities;
- Engaging in international cooperation on cybercrime and electronic evidence;
- Developing and demonstrating new cyberdefense mechanisms;
- Developing metrics for deployment and evaluation.



Projects funded by EU	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Project on Cybercrime (phase1)	▨	▨	▨	▨								
Global Project on Cybercrime (phase2)				▨	▨	▨						
Global Project on Cybercrime (phase3)							▨	▨				
Project on Cybercrime Georgia				▨	▨							
EAP Project						▨	▨	▨	▨			
EAP II Project										▨	▨	▨
IPA Project					▨	▨	▨	▨	▨			
GLACY								▨	▨	▨	▨	
NECOMA								▨	▨	▨	▨	
GCC								▨	▨	▨	▨	
Cyberterrorism Project						▨	▨	▨	▨			
OCTOPUS									▨	▨	▨	
COuRAGE									▨	▨	▨	
e-CRIME									▨	▨	▨	▨
CAMINO									▨	▨	▨	
CyberROAD									▨	▨	▨	

Table 1 – European funded Projects on cybercrime

1. **Project on Cybercrime** (phase 1)

The Project on Cybercrime, phase 1, was launched in September 2006 and terminated in February 2009. The aim of the project was to promote a broad implementation of the Convention on Cybercrime (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189) and to deliver specific results in terms of legislation, criminal justice capacities and international cooperation.

The project relied on the cooperation with a multitude of other stakeholders, be it national authorities, international organisations, private sector and non-governmental initiatives. Phase 1 was followed by the Global Project on Cybercrime (Phase 2)[1].

According to the available information on the website of the project[2], the main achievements are claimed as follows:

- The first phase of the Project on Cybercrime helped to establish the Convention of Budapest as the primary reference standard for cybercrime legislation globally. The recognition of the Convention by a wide range of international and regional organisations illustrates the standard it has become. The ever stronger cooperation with the private sector and other initiatives does so as well;
- The Project helped to create a momentum of cooperation against cybercrime at all levels;
- It familiarised hundreds of law enforcement and criminal justice officers around the world with the investigative tools provided by the Convention. In this connection, modules for the training of judges were prepared by the project stakeholders;
- It provided specific legislative advice and helped to shape cybercrime legislation in a wide range of European and non-European countries, like in Africa, Asia, the Caribbean and Latin America;
- It promoted an effective international cooperation basis and it created the 24/7 points of contact and stronger cooperation with the G8 High-tech Crime Subgroup and Interpol.

[1] http://goo.gl/0KYOId

[2] http://goo.gl/0KYOId

During the phase 1 of this project, the needs identified included[3]:

- The need for public-private cooperation, in particular the cooperation between law enforcement agencies and internet service providers;
- The need to protect personal data and privacy while enhancing the security of cyberspace;
- The need for a further strengthening of measures to protect children from exploitation and abuse on the internet.

2. **Global Project on Cybercrime** (phase 2)

Global Project on Cybercrime, phase 2, was launched at the Octopus Interface conference in March 2009 and ended in December 2011.

The aim was to promote a broad implementation of the Convention on Cybercrime (ETS 185) and its Protocol on Xenophobia and Racism (ETS 189) and related international standards.

Contributions from the governments of Estonia, Japan, Monaco and Romania, as well as Microsoft, McAfee and Visa Europe complemented the European funding[4].

The main goals were on the following levels:

- Legislation and policies
- International cooperation
- Law enforcement – service provider cooperation
- Financial investigations
- Training of judges and prosecutors
- Data protection and privacy
- Protection of children

The main results obtained are listed as follows, according to Final Project Report Presentation[5]:

[3] ibidem

[4] http://goo.gl/tsGMXC

[5] http://goo.gl/lpRzXj

- International Cooperation: Capacities of 24/7 points of contact, high tech crime units and of authorities for mutual legal assistance strengthened was achieved to a large extent;
- Law enforcement - service provider cooperation: the investigation of cybercrime improved on the basis of the guidelines adopted in April 2008. The need for cooperation between law enforcement agencies and service providers is now widely acknowledged;
- Financial investigations: enhanced knowledge among high tech crime units and Financial Investigation Units to follow money flows on the internet and stronger cooperation between financial intelligence and investigation units, high-tech crime units and the private sector was fully achieved;
- Training of judges and prosecutors: The institutionalized training for judges and prosecutors in cybercrime and electronic evidence was fully achieved;
- Data protection and privacy: Data protection and privacy regulations in connection with cybercrime investigations improved in line with the ones from the Council of Europe and other relevant international standards;
- Exploitation of children and trafficking in human beings: Enhanced knowledge of standards against the sexual exploitation and abuse of children and trafficking in human beings on the internet was achieved to a large extent.

The needs identified during phase 2 of this project included:

- Judicial training components should be incorporated into future projects on cybercrime;
- The effectiveness of mechanisms for mutual legal assistance remains a major challenge in international cooperation;
- Support to the conclusion of specific agreements between law enforcement and service providers cooperation would have required more resources than were available;
- The structure of the Council of Europe Secretariat, that now combines cybercrime and data protection within one division, should be conducive;
- Encourage countries to adopt legislation to protect children against online sexual abuse and to facilitate international law enforcement cooperation against such crimes.

3. **Global Project on Cybercrime** (phase 3)

Phase 3 of Global Project on Cybercrime was launched in January 2012 and completed in December 2013.

The aim was to promote a broad implementation of the Budapest Convention on Cybercrime and related standards and tools[6];

- Experience exchange: best practices related to measures against cybercrime documented and shared;
- Assistance: countries assisted in the implementation of the Budapest Convention and related standards and best practices;
- Assessment of cybercrime legislation available.

The Final Report is not available[7]. Therefore, it was not yet possible to draw any conclusions about the needs to be taken into account.

4. Project on Cybercrime in Georgia

This project was designed to contribute to the security and confidence in information and communication technologies in Georgia by helping the authorities to develop a consistent policy on cybercrime through the implementation of the Convention on Cybercrime. The project properly addresses some major needs of Georgia in the fight against cybercrime: legislation, training (law enforcement and judicial training institutions) and cooperation between law enforcement agencies and internet service providers. It was launched in June 2009 and completed in May 2010.[8]

According the Evaluation Final Report[9], the main results of the project can be listed as follows:

- The project has reached substantial impact in a very short time, when compared to other technical assistance projects - according to the indicators of the workplan, all results have been fully achieved;
- Georgian legal system has many similarities with with the Council of Europe and the European Union standards on cybercrime and protection of personal data;
- Comprehensive and professional training material including training curricula for judges, prosecutors and investigators were created;
- The cybercrime unit (including the 24/7 contact point) was formally established;

[6] http://goo.gl/dTpo0Y

[7] http://goo.gl/A218DI

[8]http://goo.gl/ophvdv

[9] http://goo.gl/EVqaRo

- Law enforcement agencies and internet service providers formally signed a Memorandum of Understanding (“Principles of Cooperation”).

The needs identified during this project included:

- The materials for training curricula for judges, prosecutors and investigators should be less general and more in-depth, adapted more specifically to the Georgian legal system;
- A possible need on the part of law enforcement agencies and internet service providers for training on the procedures of cooperation should also be taken into account;
- The cybercrime unit should be supported by a strategy on the available means to systematically fight cybercrime, with appropriate advanced hardware and software training courses to take advantage of such tools;
- Advice and support on the procurement of the necessary hardware and software tools for cybercrime investigation.

5. **EAP Project** (Eastern Partnership – Cooperation against Cybercrime)

EAP was launched in March 2011 and completed in December 2014. The aim was “to strengthen the capacities of criminal justice authorities of Eastern Partnership countries (Armenia, Azerbaijan, Moldova, Ukraine and Georgia) to cooperate effectively against cybercrime in line with European and international instruments and practices.” [10];

According to the project summary[11], the needs identified and addressed are:

- Policies and awareness of decision-makers: The project is supposed to raise awareness among decision-makers and help them to define strategic priorities regarding cybercrime and electronic evidence;
- Harmonised and effective legislation based on the Budapest Convention on Cybercrime: The project is supposed to assess legislation in place, help draft proposals for amendments to legislation and assess the effectiveness of legislation, among other things based on criminal justice statistics and case law;
- Judicial and law enforcement training on cybercrime and electronic evidence;
- Internet service provider cooperation in the investigation of cybercrime: international cooperation, including judicial and police cooperation and strengthening of 24/7 points of contact;

[10] http://goo.gl/9I5jdj

[11] http://goo.gl/TFQ8Bz

- Financial investigations: the need for measures to prevent and control money laundering and to search, seize and confiscate crime proceeds on the Internet.

6. **EAP II Project** (Eastern Partnership – Cooperation against Cybercrime)

EAP II Project is the follow up of the EAP Project. It was launched in May 2015, has a duration of 30 months and is expected to be completed in October 2017.
The aim is to enable efficient regional and international co-operation on cybercrime and electronic evidence[12].

The main goals are[13]:

- The authorities responsible for mutual legal assistance in the six EAP countries will have better skills and tools (manual and online resources) for international co-operation on cybercrime and electronic evidence;
- The role of 24/7 points of contact will have been strengthened in the six EaP countries;
- Recommendations for amendments to procedures and rules on mutual legal assistance on cybercrime and electronic evidence are available for the six EaP countries.

The main constraints identified included:

- Complex and time-consuming procedures for mutual legal assistance;
- Absence of mechanisms for expedited mutual legal assistance in the sense of Article 31 of the Budapest Convention;
- Limited role of 24/7 points of contact - delays in replies and often no replies from foreign countries to requests for police and judicial cooperation;
- Limited cooperation with multi-national service providers;
- Limited trust in cooperation with and between the six EaP countries.

According to the Assessment report, the needs identified[14] included:

- Cybercrime policies and strategies;
- Complete and effective legal basis for criminal justice action;

[12] http://goo.gl/xMGrux

[13] http://goo.gl/vuOF5W

[14] http://goo.gl/vromIH

- Specialised cybercrime units;
- Law enforcement training;
- Judicial training;
- Financial investigations and prevention and control of fraud and money laundering on the Internet;
- Cooperation between law enforcement and Internet service providers;
- More efficient regional and international cooperation.

7. **IPA Project** - Regional Cooperation against Cybercrime in South-Eastern Europe

The IPA Project was launched in November 2010, for a duration of 30 months and was completed in April 2013.
The aim was to strengthen the capacities of criminal justice authorities of Western Balkans (Albania, Bosnia and Herzegovina, Croatia, the Former Yugoslav Republic of Macedonia, Montenegro, Serbia and Kosovo) and Turkey to cooperate effectively against cybercrime[15].

According to the Assessment Report[16], the main results achieved included:

- Legislation on cybercrime and electronic evidence is now stronger and more in line with the Budapest Convention, the rule of law and human rights principles;
- Specialisation and the number of specialised units in police and prosecution services have increased;
- Law enforcement training has become a stronger priority;
- Judicial training has been or is on the way to being mainstreamed into judicial training curricula;
- The ground has been prepared to ensure that in the future criminal money on the Internet can be seized and confiscated;
- A culture of cooperation between public and private sector is emerging;
- Countries and areas now do engage in regional and international cooperation against cybercrime and the securing of electronic evidence;
- A number of practical tools are available, ranging from good practice studies on specialised cybercrime units, to a blueprint for law enforcement training strategies, judicial training materials or the electronic evidence guide.

The needs that were identified included:

[15] http://goo.gl/sxTHgg

[16] http://goo.gl/nM1jp8

- Cybercrime policies and strategies;
- Complete and effective legal basis for criminal justice action;
- Specialised cybercrime units;
- Law enforcement training;
- Judicial training;
- Financial investigations and prevention and control of fraud and money laundering on the Internet;
- Cooperation between law enforcement and Internet service providers;
- More efficient regional and international cooperation;

From the topics above, some examples of needs could be presented as follows:

- ✓ Accurate statistics showing the nature and range of investigations, prosecutions together with disposals … to design comprehensive cybercrime national strategies and training strategies;
- ✓ Equip cybercrime units with a standard operating platform, adequate hardware and a basic suite of analytical tools;
- ✓ Development of new techniques and operational policies increasing criminal use of Internet;
- ✓ Increase the number of individuals engaged in specialist cybercrime units
- ✓ Reduce tacit education and training knowledge into operational manuals and standard operating procedures;
- ✓ Operational manual and standard operating procedures continuously reviewed as criminal tactics and technology change;
- ✓ Development of forensic and special investigation tools;
- ✓ Creation of a centre of excellence to assist and create new relationships with others in industry and academia that specialise in these matters;
- ✓ Reduce bureaucracy obtaining international assistance dealing with cybercrime;
- ✓ Standardised multi-language request templates; possibility for direct contacts available under different agreements; specific regime for subscriber information (IP identification); more pro-active role of 24/7 points of contact;
- ✓ Prosecutors and police commanders should draft protocols or operating policies which include, policies on communication, referral, extent of analytical/intelligence investigations and delegated levels of authority;
- ✓ Enhance the direct contact of law enforcement agencies and judicial authorities with US-based internet service providers to obtain information.

8. **GLACY** - Global Action on Cybercrime

GLACY was launched in November 2013; it has the duration of 36 months and will be completed in October 2016.

The aim is to prevent and fight against organised crime, enabling criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention[17];

Results are expected in the following areas:

- Engagement of decision-makers
- Harmonisation of legislation
- Judicial training
- Law enforcement capacities
- International cooperation
- Information sharing
- Assessment of progress

9. **NECOMA -** Nippon-European Cyberdefense

NECOMA stands for Oriented Multilayer threat Analysis. The European Commission and the Japanese Ministry of Internal Affairs and Communications fund this project, which started in 2013 and will end in 2016.

The aim is to develop and demonstrate new cyberdefense mechanisms that leverage the metrics for deployment and evaluation[18].

NECOMA is an ongoing project. It has already some publications which can be accessed under http://www.necoma-project.eu/publications/, but it was not possible to extract any conclusions on the needs that could contribute to the broader picture of this project.

10. **GCC:** Greek Cybercrime Center

The Cyber Crime Center of Excellence for Training, Research and Education in Greece[19] is a national project of Greece, funded by the European Commission. It is part of an emerging

[17] http://goo.gl/02W5p3

[18] NEUCOMA

coordinated European effort, which has the capacity to significantly improve education and research in the newly growing area of cybercrime. It started in 2013 and will end in 2016. There are so no conclusions which can be helpful for this current CyberRoad task 3.2.

11. **Cyberterrorism Project –** by Swansea University (UK)

The Cyberterrorism Project was funded by the British Academy. It consisted of a multidisciplinary research approach started in 2011 and completed in 2014.
The aim of this project was to capture current understandings on cyber terrorism within the research community. The main focus was to collect knowledge on what cyberterrorism is, the threat that it poses and the appropriate forms of response to it. That knowledge was possible through a questionnaire which was distributed to over 600 researchers, authors and other experts, working in 24 countries across six continents.[20];

Some main conclusions

Most of the Cyberterrorism Project Survey respondents considered cyber terrorism a significant threat, identifying the main focus of the threat as being the governments/states, critical infrastructures, computer networks, civilians/individuals, organizations from public or private sector, corporations, the economic structures and the society in general.

Regarding the question of the most effective countermeasures against cyber terrorism, most of the respondents consider that a greater international cooperation is necessary, and refuse to exaggerate the threat. They answered the same way to cybercrime and to the prevention of radicalization.

To the question of the differences regarding the more traditional forms of counter terrorism, the most common answers were:

- Same strategies with different methods;
- Greater technical expertise required;
- Greater role of private sector;
- Greater role of individual citizens.

[19] http://www.cybercc.gr/

[20] http://goo.gl/SsDMQ9

12. **CYBERCRIME@OCTOPUS**

This Project has the duration of 36 months. It started on January 1, 2014, and will end on December 31, 2016.

The aim is to support the implementation of the Budapest Convention on Cybercrime and related instruments[21].

13. **COuRAGE** - Cybercrime and cyberterrorism European Research Agenda

This Project has the duration of 24 months. It started on January 1, 2014 and will end on the April 30, 2016.

The aim is to deliver a measured, comprehensive, relevant research agenda for Cybercrime and Cyber Terrorism (CC/CT)[22]. This is one of the three projects financed by the European Commission under the same topic (CAMINO and CyberRoad).

14. **CAMINO** - **C**omprehensive **A**pproach to cyber road**M**ap coord**I**Nation and development

This project has the duration of 24 months, from April 2014 until April 2016.

The aim is to develop a comprehensive cybercrime and cyberterrorism research agenda and to iniate long term activities providing a stable platform of security research experts and organizations.[23]

15. **CyberROAD** - CYBERcrime and CYBERterrorism reseach ROADmap

This Project has the duration of 24 months, from the 1st June 2014 until the 31st May 2016.

The aim is to identify current and future issues in the fight against Cybercrime and cyber terrorism in order to draw a roadmap for cyber security research[24].

[21] http://goo.gl/kJKCPS

[22] COURAGE

[23] http://www.fp7-camino.eu/

[24] CyberROAD

16. **E-CRIME**

This Project will examine the economic impacts of cybercrime. It has the duration of 36 months, from April 2014 until March 2017.

The aim is to reconstruct the spread and development of cybercrime in non-information and communications technology (non-ICT) sectors from the perspective of its economic impact on the key fabrics (i.e. economic and social) and different levels of European society, while also identifying and developing concrete measures to manage and deter cybercrime.[25]

Some considerations on the projects above

After a short overview of the projects above, developed during the period between 2006 and 2015, we conclude that most of them, such as Project on Cybercrime (all phases), Project on Georgia, EAP and EAP II Project, IPA Project, GCC, GLACY and OCTOPUS had similar aims: to promote and implement the Cybercrime Convention in the legislative and judicial domains.

This is a critical step forward in the prevention and fight against cybercrime. However, given that some time elapsed since the progressive adjustment of Europe to the Cybercrime Convention, and given the natural evolution of cybercrime with its new emerging problems and challenges, it make sense that a few issues have to be further explored.

This outlook moved forward with more specialized projects focused on cyberdefense (e.g. NECOMA), on examining economic impacts of cybercrime (e.g. the e-Crime Project), and on the threats that cybercrime and cyberterrorism pose to society as a whole (e.g. the Cyberterrorism Project, Courage, Camino and CyberROAD). These projects, which are currently ongoing will allow for a better understanding of the stakeholder needs.

The following table resumes the different needs of stakeholders that were identified in each project, which are divided into three domains: public sector (goverments, law enforcement agencies, and criminal justice officers), private sector and individuals (citizens). They are also divided into four dimensions: social, economic, political, and legal.

[25] E-CRIME

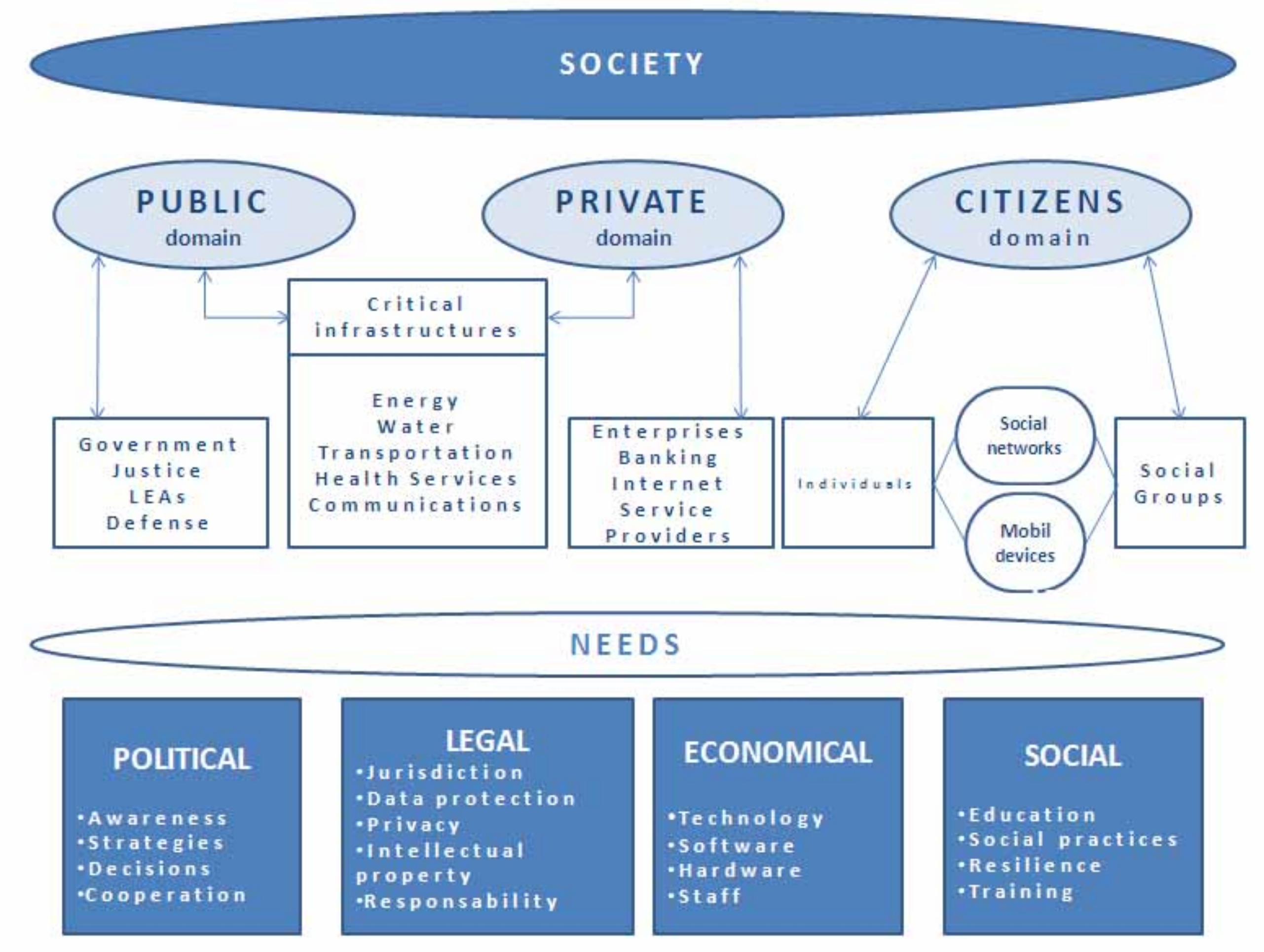


Table 2 – Stakeholder's Needs Evaluation

II - Highlighting Stakeholder Needs from Independent Initiatives in the EU

Throughout the EU, independent initiatives in the form of projects and surveys provide valuable insights and perspectives on the impact of cybercrime. Groups, associations and organisations with an interest in, and knowledge of, cybercrime prevention can tap into resources and reach specific stakeholders that may, otherwise, be unavailable. Here, an overview is given of a sample collaborative project from the ICSPA 'International Cyber Security Protection Alliance'[26] which is supported by EC3 at Europol, ENISA, the City of London Police and a number of industry players such as Atos, McAfee, CGI Canada, Trend Micro, Cassidian and Visa.

Additionally, at a micro level an overview of stakeholders' needs in the retail industry is provided from an assessment of The British Retail Consortium (BRC) together with stakeholders' views from the perspective of the Federation of Small Businesses (UK).

Project 2020 - ICSPA International Cyber Security Protection Alliance (ICSPA, 2012)

The aim of this ongoing project, which began in 2012, is to provide an assessment of future challenges and opportunities, as a means of preparation for governments, businesses and citizens. An early output is the report 'Project 2020 Scenarios for the Future of Cybercrime' **(ICSPA, 2012)**

The methodology provides a number of scenarios from the perspective of an ordinary Internet user, a manufacturer, a communications service provider and a government. An analysis of the threat landscape in 2012 comes from evidences provided by ICSPA members across a range of Internet security companies via collaboration with Trend Micro[27].

Emerging technologies in the form of scientific abstracts and open source material were reviewed by experts in the appropriate fields together with Europol specialists to identify a number of key uncertainties for the future. These were combined with the outcomes from two workshops held for multi-stakeholders and the latest social, economic and geopolitical research and examined in the context of a network of interdependencies.

[26] https://www.icspa.org/

[27] http://www.trendmicro.co.uk/

The result was "the identification of criminal opportunities, vulnerabilities and unanswered questions concerning such aspects as legislation, governance and interoperability." These are summarized by Project 2020 as "Implications for Cybersecurity Stakeholders" as below:

- Who owns the data in networked systems and for how long?
- Who will distinguish between data misuse and legitimate use, and will we achieve consistency?
- What data will the authorities be able to access and use for the purposes of preventing and disrupting criminal activity?
- Who covers (and recovers) the losses, both financial and in terms of data recovery?
- Who secures the joins between services, applications and networks?
- And how can objects that use different technologies operate safely in the same environment?
- Do we want local or global governance and security solutions?
- Will we be able to transit to new governance and business models without causing global shocks, schisms and significant financial damage?

Conclusions

The 'Implications for Stakeholders' identified in 'Project 2020' raise a number of questions that are important for stakeholders across the 3 key domains that are relevant to this deliverable: the public sector, the private sector and individuals (citizens). Further research into each of these areas is required In order to satisfy the needs of all stakeholders over the coming years.

A Stakeholder's View (Macro) – Survey Results from the British Retail Consortium

The British Retail Consortium (BRC), a leading trade association representing the retail industry, conducts an annual survey of retail businesses in British. "The BRC Retail Crime Survey 2014" (The British Retail Consortium, 2014) details incidences of crime affecting retail businesses. In 2013-2014 the number of cyber-enabled attacks increased with retailers reporting that they posed a significant threat to their business.

Major outcomes from the survey:

- Businesses are increasingly the victims of crime committed online, such as cyber-enabled fraud. In 2013-14, fraud increased by 12 per cent and accounted for 37 per cent of the total cost of crime. The majority of fraud is committed online.
- An estimated 59% of fraud is committed by organised groups and can often operate across several geographic areas.
- Credit and debit card fraud accounted for 81 per cent of fraud by volume.

- Theft of data and hacking were considered to pose the most critical threats. (See Figure 1)

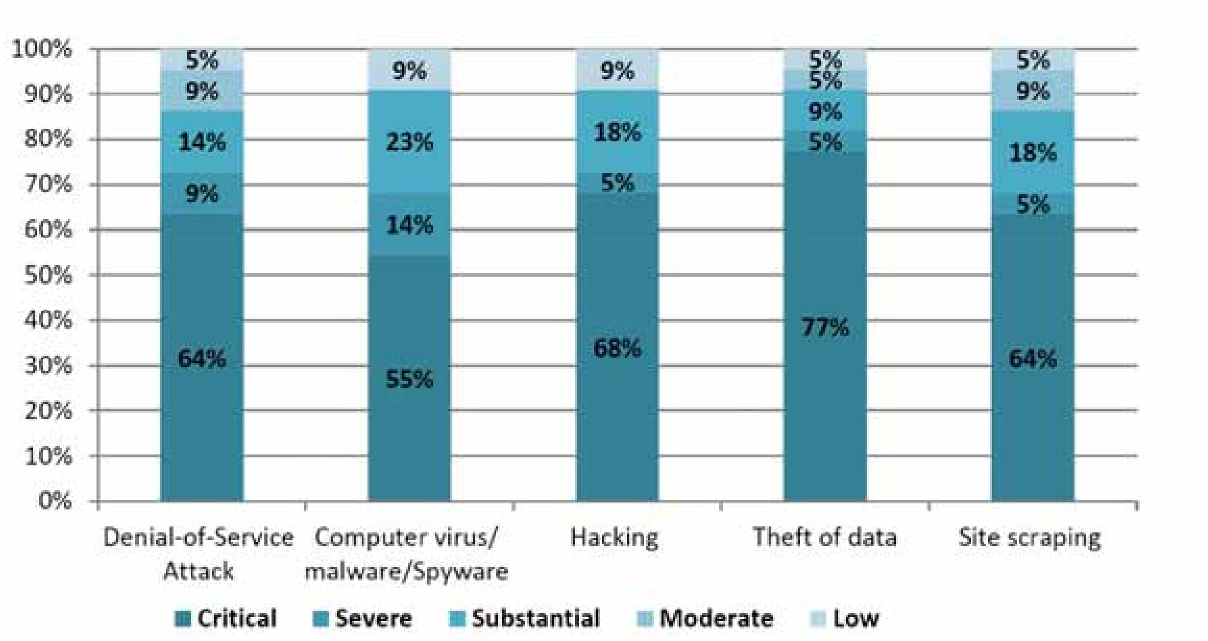


Figure 1: Threat Posed by Cyber Attacks, by Proportion of Respondents (The British Retail Consortium, 2014)

Impacts on Stakeholders

Respondents to the BRC survey reported a number of impacts as a result of the frauds that were committed. Loss of staff time and distraction from business purpose together with reputational damage to the brand were cited as having the most significant impacts. Another highly ranked consequence, which the report highlights as an overlooked area, is that of damage to employee morale.

Challenges that need to be met

Retailers cite a number of failings in the way that cyber-enabled crimes are reported and a lack of subsequent prosecutions. These issues are summed up as follows:

- The capacity of law enforcement to respond effectively to cyber-enabled crime. Only a tiny proportion of fraud cases result in any action being taken.
- An apparent inability of law enforcement to respond to offending that crosses police force borders.
- A lack of intelligence sharing from the National Crime Agency about emerging cyber threats.
- No confidence in the police response. This was cited as a major reason for failing to report incidents of fraud (cyber-enabled or otherwise.)

Conclusions

The challenges cited by British retailers are found, as well, throughout EU countries which points to significant gaps in meeting stakeholders needs. For example, WP5 D5.1 “Cybercrime **–** Evaluation of Stakeholders Needs and Threats, an overview of Crime Statistics, Section 4.2.4 - A Comparison Statistics” contains a quote from the United Nations on Drugs and Crime (UNODC) report (UNODC, 2013), Annex 2 entitled, ‘Measuring Cybercrime’ (UNODC, 2013), *“...for cybercrime events, the difference between victimization and police-recorded crime can be many orders of magnitude”* (pp.259 – 266).

The CyberROAD “D5.1 Survey #1 Cybercrime” highlights, as well, the problem of low incident reporting to the police with 36.6% of respondents saying that they had not reported being a victim of cybercrime to the police. 27.6% did report an incident but the police took no further action, while only 7.2% of respondents stated that the police had achieved a successful prosecution.

Reporting incidents and achieving successful prosecutions by the police remain a significant challenge for stakeholders throughout the EU.

A Stakeholder’s (Micro) – from the Federation of Small Businesses (UK)

The Federation of Small Businesses (FSB) report ‘Cyber security and fraud: The impact on small businesses’ (FSB, 2013) details 2,667 responses focusing on the specific interests of small and micro businesses.

The report recognizes that online crime, and fraud in general, whether real or perceived, presents a number of distinct problems for small businesses and, as a consequence, the costs involved can be a barrier to growth in the e-commerce market.

When asked the question: “How much money has your business lost as a result of fraud and/or online crime over the past 12 months?” 41% reported being a victim with an average of £3,926 (EUR 5,502) lost. The most prevalent cybercrimes experienced were ‘virus infections’ (20%), ‘hacking or electronic intrusions’ (8%) or ‘system security breach/loss of availability’ (5%). 73% of respondents were concerned that they may be unaware that their computer systems had been compromised.

Preventing cyber-enabled fraud was reported as being a significant cost to the business.

Bring Your Own Devices (BYOD) brings additional risks to small businesses through possible malware infection to company data and systems, loss of data and unauthorized access. Managing this risk with extra security measures including encryption, mobile security solutions and Network Access Control (NAC) adds to small business overheads.

Small businesses expressed concerns about compliance being weighted towards larger organisations. Although recognizing that standards are designed to improve data security through the adoption of good business practice, paying for an assessor or completing lengthy self-assessment forms adds additional pressures for SMEs.

Challenges that need to be met

Small businesses in the UK expressed the need for customized and realistic practices to enable SMEs to meet the growing challenges from cyber-enabled fraud. Improvements are required in:

- Customized security guidance for small and micro businesses
- Improving law enforcement responses to online crime
- Improved cooperation from banks and payment providers in the cyber security area
- More information sharing within the private sector
- More efficient reporting methods for all crime including online crime and fraud
- Simplified and streamlined standards and benchmarks aimed at SMEs

Conclusions

The needs of SME stakeholders may differ from the larger corporate entities creating additional financial pressures, which has the potential to limit growth in this market. A one-size-fits-all policy to corporate online security may not be appropriate with SMEs requiring simplified and streamlined guidance. Without these improvements SME's will remain vulnerable to cyber-enabled crimes and increasingly become the target for opportunistic crimes as a weak point of entry for the cybercriminal.

The views expressed by SME's in the UK align with responses to questions posed on the subject of the importance of information sharing on cyber issues in "WP5 Survey #3 Social, Economic and Political issues". (See Figure 2).

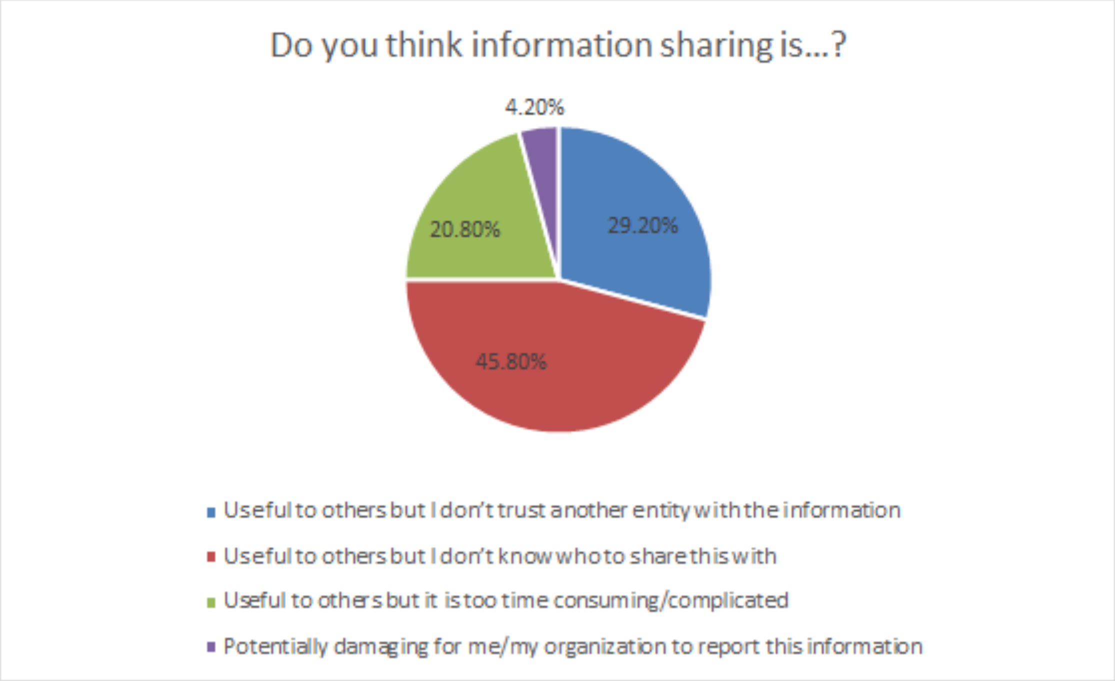


Figure 2: Responses from WP5 Survey #3

The advantages of information sharing are understood by end-users whether they are consumers, business owners or employees but knowing how to enact this appears to be a different matter. Currently, there is no system that fulfills the needs as expressed by the SMEs in the FSB survey.

Their views are supported by findings from the CyberROAD Cybercrime surveys. Issues of trust, lack of knowledge on where or how to report problems and cost are major challenges currently being faced. Accommodating these demands will determine the success of the eco-systems of the future.

The WP5 & WP6 Surveys/Questionaire are further analysed in Section IV.

III - SOME INPUTS FROM ITALY, AUSTRIA AND PORTUGAL

ITALY – ANALYSIS OF NATIONAL REPORTS ON CYBERCRIME

Foreword – State of Cybersecurity in Italy

This chapter gives an updated overview of the cybercrime in Italy. So far, the national law enforcement agencies don’t disclose any report on cybercrime. Nevertheless, some relevant national bodies and private organizations collect and publish significant data. As a result of our analysis, the findings of significant reports published in 2015 are summarized in this chapter.

State of the Italian Digital Services: The Digital Economy and Society Index (Source: European Commission – EC)

Background

Each year the European Commission publishes the Digital Economy and Society Index (DESI). It is one of the analytical tools used to measure how countries are progressing towards the targets set in the Digital Agenda for Europe. To get more in details, it is “*a composite index that summarizes some 30 relevant indicators on Europe’s digital performance and tracks the evolution of EU Member States, across five main dimensions: Connectivity, Human Capital, Use of Internet, Integration of Digital Technology, Digital Public Services*”.

The DESI report we analyzed focusing on the Italian country profile was published in February 2015 and includes rankings of the best/worst digital performers, therefore putting in evidence the digital gaps that must be filled by the country.

Report findings

- Digital experience varies a lot from country to country – as performance varies from digital top-players such as Denmark with a 0.68 score to lower-performance countries such as Romania with a 0.31 score.

Italy has an overall score of 0.37 and ranks only 25th out of the 28 EU Member States.

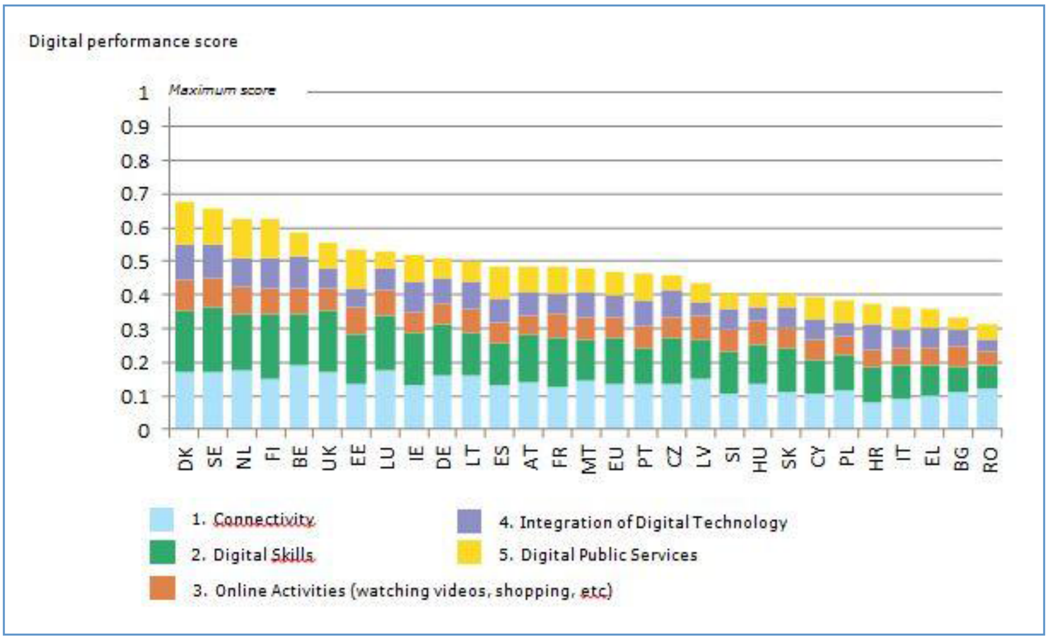


Figure 3 - Digital performance score

- Most of European citizens use the Internet on a regular basis: 75% in 2014, ranging from 93% in Luxembourg to 48% in Romania. In Italy, there is a low level of digital skills: the percentage of regular Internet users is 59% and 31% of Italian citizens have never used the Internet. This may be due to the high percentage of aged people (21.7% of population is aged 65 years and more)[28], even if 1.5 million of them "surf" the web daily[29].

  The level of trust in Italy is also quite low (42% of Internet users are online bankers and just 35% of them shop online).

- Europeans are enthusiast consumers of online audiovisual contents: 49% of European "surfers" have played or downloaded games, movies, images or music. 39% of households play on-demand videos. Italy performs badly on Connectivity (high-band Internet arrives to only 36% of the households and only 3.8% of broadband subscriptions reach 30 Mbps).

- Small and medium sized businesses (SMEs) face barriers with e-commerce: only 15% of SMEs carry out online sales - and fewer than half of them sell across borders. Italian

[28] ISTAT - Italian National Institute of Statistics http://www.istat.it/en - http://www.tuttitalia.it/statistiche/indici-demografici-struttura-popolazione/

[29] CENSIS - Social study and research institute - http://www.censis.it//25?shadow_testo_con_relazioni=139

businesses are still mainly non-digital and could increase e-Commerce (only 5.1% of Italian SMEs carry out online sales).

- Digital public services are used every day in some countries but almost non-existent in others: 33% of European citizens have used online forms to send information to public authorities (69% in Denmark - 6% in Romania). Italy scores close to the EU average; nevertheless, there's no mass-usage of e-Government services, partly because of public services on the web not being sufficiently developed and partly because of the lack of digital skills.

- Italy is classified among the low-performance countries[30], performing below average.

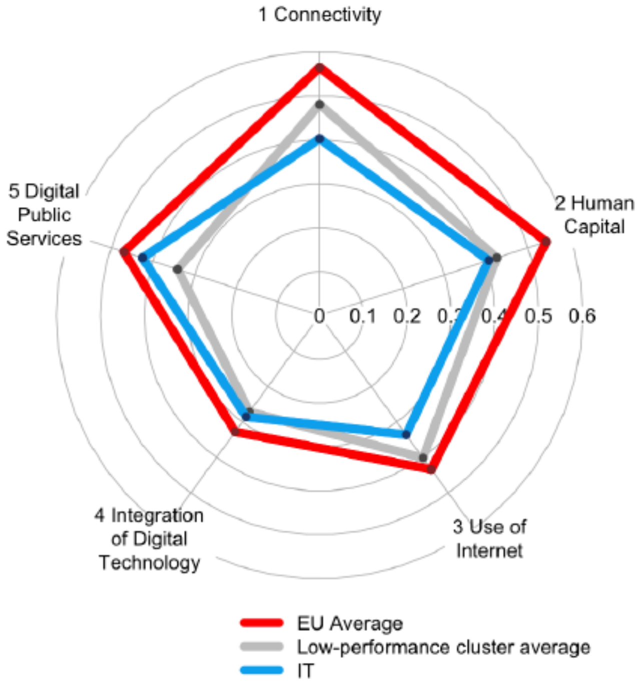
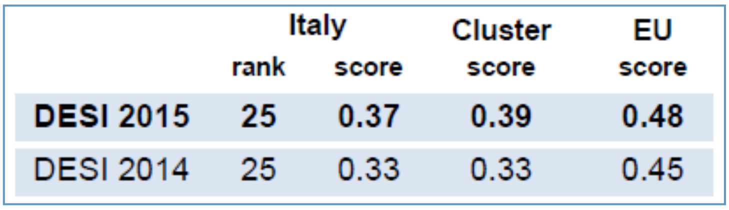


Figure 4 - DESI 2015 - Italy radar



	Italy		Cluster	EU
	rank	score	score	score
DESI 2015	**25**	**0.37**	**0.39**	**0.48**
DESI 2014	25	0.33	0.33	0.45

Table 3 - Italy DESI ranks and scores comparison

[30] DESI 2015 low-performance countries: Bulgaria, Cyprus, Czech Republic, Greece, Croatia, Hungary, Italy, Poland, Romania, Slovenia and Slovakia.

Conclusions

The European Digital Single Market offers the possibility to unlock plenty of opportunities for European citizens and companies. Online shopping and training, internet payments and the usage of public services over the net and across the national borders are a goal that can't be missed.

Some European countries are ready to catch this opportunity; yet some others – Italy is one of them – need to invest firmly on Digital Services in order to satisfy citizens' needs: people want to access online content quickly, easily and safely. Businesses have to innovate and grow in this direction; governments need to work in order to boost trust in online financial and governmental services. We need to adapt to citizens' needs and to work for a fully-fledged Digital Single Market.

Annual Report on the National Information Security Policy

(Source: Italian Security Intelligence Department - DIS)

Background

The overall political responsibility for intelligence in Italy is vested in the President of the Council of Ministers. He exercises his functions through the DIS – Dipartimento Informazioni per la Sicurezza (Security Intelligence Department), an organization that ensures a fully unified approach to intelligence collection, analysis and operations. The DIS coordinates all intelligence activities, including national cybersecurity.

By law (n. 124/2007), each year the Government shall send the Parliament a written report on its security intelligence policy and results achieved for the previous year. The report includes activities related to the protection of critical infrastructures, as well as cyber defense and security. It describes the most significant cyber threat-related phenomenon and outlines the future challenges the intelligence will face in relation to the evolution of the criminals' modus operandi and to the wide range of purposes and actors that represent a wide and diversified catalogue of potential new risks for the national security.

Report findings

During 2014, the DIS gave high priority to activities countering cyber threats, focusing mainly on:

- structured, persistent and pervasive threats to national critical infrastructures;
- digital espionage activities on public and private entities, operating in sectors strategic to national security, on owners of sensitive or valuable know-how in the field of research and technology;

- single attacks or attack campaigns, undertaken by hacktivists, targeting institutional entities;
- internet usage in issuing propaganda, giving misinformation, doing counter-intelligence, proselytism, planning criminal or terrorist acts;

The strict monitoring of such aspects brought to a better comprehension of these structural criticalities:

- increased number of planned and executed illicit activities by means of digital resources that are considered rapid, effective and secure;
- difficulty of tracing back the attack sources by means of tamper-proof digital evidences, especially when anonymization techniques are used;
- easy access to products and innovative tools, designed to increase the offensive capabilities, even of those with few economic resources available.

Summary of other relevant findings for 2014

Hybrid wars

2014 has seen a massive usage of sophisticated cyber weapons and information warfare techniques in real war scenarios (as in the Ukrainian or Syrian conflicts);

Actors, techniques and goals

Threats are getting more and more polymorphic and actors' profiles are getting even more "opaque" than before; a wide range of actors - each with different goals - operates as singles or as structured organizations; they're state-sponsored, members of criminal organizations or both and it's getting more and more difficult to classify such a heterogeneous set of actors, as no clear line has been drawn between the categories;

Digital espionage

During the year, a number of state-sponsored digital espionage activities have been conducted against national targets operating in the high-tech sector. Sensitive information related to technologies, processes, programs and future products has been exfiltrated; some of this information has been used to achieve a competitive advantage in financial operations and in taking stakes in companies.

Industrial and commercial digital espionage has also been conducted directly by companies and corporations. SMEs confirm to be an easy target, due to the lack of investments and of adequate security policies.

From a technical point of view, these attacks have been more sophisticated than in the past, extremely pervasive, persistent and adaptive, especially when attempting to bypass the defensive measures put in place by target organizations.

Hacktivism

The hacktivists operating on the national panorama have shown high-quality operating standards and in particular increased technical abilities and made attack techniques more sophisticated.

Real-world demonstrations are getting more and more synchronized with digital ones and Anonymous confirms its role as a reference point for the anarchists all over the world.

Attack campaigns are planned, discussed and coordinated by means of forums and chat. Hacktivists groups use cryptography more often to protect communications anonymity. Virtual Private Networks (VPNs) and the TOR network are still the most used anonymization tools. There are guidelines and recommendations on how to avoid geo-localization by LEAs.

Conclusions

Networks of strategic significance

The greatest critical issues emerged during 2014 related to the national networks and telecommunication infrastructures are mainly linked to technical factors and to the lack of an updated map of the national data flow. Due to economic agreements established between the major international carriers, data flows can cross the borders of countries that pay scant attention to privacy issues and that easily allow communication hijacking practices. In case the "building blocks" of the Italian telco infrastructures do not adopt adequate levels of protection, this will constitute a serious threat to the confidentiality and integrity of communications.

Systems vulnerabilities

- The main weaknesses of the national industrial control systems (Supervisory Control and Data Acquisition – SCADA) are represented by the obsolescence of the existing installations: designed to operate autonomously, they have been integrated over the years with newly designed systems, by means of non-segregated open networks. Most of the national SCADA systems are based on very old software platforms and are affected by old and newer vulnerabilities that are very difficult to fix for economic and technical reasons;

- The EXPO 2015, the first national fully cloud-powered event, represents an attractive target due to the high exposure on the international scene.

The progression of threat: projections for 2015

During 2015 an increasing level of threat is expected; the main reasons are:

- the increasing sophistication of the attack techniques;
- an inadequate security level from a technical and organizational point of view;
- an inadequate perception of risk;
- the growth of the “attack-surface” driven by the increasing number of mobile phone applications.

In order to compromise their target organizations, hostile actors will increasingly adopt spear-phishing and social engineering techniques. These attack scenarios suffer the effect of the non-adequate level of investments in ICT Security. Risks related to the supply-chains managed by public or private operators are particularly evident, exposing IT products and components to potential tampering.

Trends and Scenarios

Immanent, polymorphic and increasingly pervasive, cyber threats are hostile actions planned by a vast and heterogeneous range of actors. Digital espionage, hacktivism and the cyber jihad are concrete threats today and in the medium term. They can have a serious impact on the security of citizens and on the political, military, economic, scientific and industrial interests of the country.

As stated before, the major risks are represented by the increasing sophistication of the attack techniques, whose impact will be obviously higher; the less adequate will be the adopted level of protection. Therefore, the predictable growth of the quantity and quality of the attacks shall be faced consolidating the national cyber architecture, by strengthening the interinstitutional synergies, the public-private partnerships (PPPs) and the essential international multilateral and bilateral cooperation.

A Study by PwC Crime Survey (Source: PricewaterhouseCoopers – PwC)

Background

PwC is a private company that offers professional services to enterprises and individuals in several areas as strategic advisory, corporate finance, due diligence, legal and tax advisory. In its “Global Crime Survey 2014”, PwC makes a wide investigation about the financial and economic fraud phenomenon, ranging from corruption to cybercrime. The results, gathered with more than 5,000 interviews in 95 countries, include also 101 Italian enterprises.

Report findings

Cyber frauds at a glance

Italy has has experienced *a strong increase in economic/financial frauds* that have grown from 17% to 23% in only two years. According to the global scenario, 37% of enterprises have been hit by fraud at least once during 2014, while Italy is placed below global average, along with other countries:Turkey, Peru, Hong Kong/Macao, Japan, Portugal, Denmark, and Saudi Arabia.

The most widespread fraud category remains the misappropriations (65%), followed by the “pure” cybercrime and accounting frauds (22%). The enterprises that experiment the greatest number of frauds are in the manufacturing (67%), energy and utilities (43%), logistics (40%) and financial services (28%) sectors.

One enterprise out of two has declared that cyber frauds have been early intercepted thanks to suspicious transactions monitoring systems and to fraud/risk management activities (20% of the cases), while 15% have been intercepted thanks to external tip-offs.

A systematic monitoring of the risks of frauds, resulted in an increased awareness on the phenomenon, improved the overall effectiveness of the controls put in place and raised the probability of early interception.

In 26% of cases, money losses range from 1 to 75 millions of euros. The higher impact frauds are perpetuated by internal employees (85%). Beside the economic losses, the enterprises are aware also of the side-damages which are difficult to estimate, like: employee motivation (22%), enterprise reputation (17%) and sanctions from law-enforcement authorities (13%).

Fraudster Identikit

The identikit of the typical “*insider*”: a man ranging from 41 to 50 years, with 10 years of working experience in the company, with a senior management role and with high educational qualifications. At a global level instead, the fraudster is typically a middle manager aged from 31 to 40, with a level of education ranging from high school to graduation.

The main reasons that bring the insiders to perform their malicious activities are: the opportunity to act without being discovered and their ability to bypass the internal security systems (72%).

The external fraudster is typically a customer (67%), while in the 2011 report edition 60% of them were individuals without any relation with the enterprise (i.e. former employees, competitors, criminal organizations).

Corruption

27% of surveyed companies operating in markets with a high risk of corruption claim to have lost a business opportunity in favour of a competitor who may have paid a bribe, while 40% believe that they probably missed an opportunity, because of a bribe paid by a competitor.

Only 13% of respondents reported cases of corruption - a slight increase compared to 2011 (10%) - while globally the reported cases are more than double (27 %).

However, Italian companies are aware that corruption could lead to the risk of business disruption (39% of cases), to reputation damage (34% of cases) and to financial losses (18% of cases).

“Pure” Cybercrime

Cybercrime is the second threat to businesses (22%) after embezzlement, and it is widely confirmed that it’s not just a “technological issue” but also a strategic matter as cybercrime threatens the business processes of every company that makes use of technology and the Internet.

Cybercrime strikes across most types of industries: financial services, insurance, energy, communications, entertainment and media.

In the 2011 report edition, financial services resulted as the most affected ones: frauds related to e-banking, credit/debit cards cloning, or cyber-laundering were really common.

In 2014, the most frightening impacts of cybercrime were: damage to reputation (65%), risks related to the violation of regulations (64%), direct financial losses resulting from computer frauds (60%), any interruption in services (59%), loss of users’ personal data (58%), theft of confidential information and data (55%).

Conclusions

According to the PwC’s survey, the situation looks extremely clear to an external observer: while “traditional” and consolidated cyber frauds seem to be under control and an increased general awareness level has been reached, new trends in cybercrime still seem incorrectlyaddressed, revealing gaps that must be quickly filled.

Summary and General Conclusions

The tricky situation that has been depicted in this chapter, points out that cybercrime in Italy is still a plague quite far from being eradicated. Appropriate measures should be adopted by national bodies in order to regularly monitor trends and evolutions of cybercrime. Specific strategies must be developed to protect SCADA network in National Critical Infrastructures; continuous training for security specialists and awareness campaigns for citizens must be somehow included in the National Cybersecurity Strategy; finally, it is necessary to keep a specific focus on data protection issues and on compliance to National and European regulations.

AUSTRIA - SOME ONGOING AND FINISHED PROJECTS

CISA - Situational Awareness Centers for Critical Infrastructures

Critical infrastructures offer a prime target for terrorists, since a small amount of direct damage can lead to vast amounts of secondary inflicted damage. This is especially interesting in case of IT critical infrastructures that could be attacked via the net, but also regarding classical critical infrastructures that were introduced to the Internet and thus became vulnerable to cyber attacks. Thus it is of vital importance for the national stakeholders responsible for the welfare of the country to be able to have an up-to-date overview on the backbone infrastructure, as well as critical infrastructures with respect to cyber attacks.

A situational awareness center collects all data on important infrastructure in real-time and enables governmental stakeholders to detect and analyze attacks. This is especially critical in order to detect cyber attacks targeting selected regions, as well as selected industries or specific infrastructures, e.g. the ACONET backbone.

The target of this project lies in merging the results of previous projects on national and international levels in order to generate a working prototype of such a center. The evaluation will be done incorporating most of Austria’s major stakeholders in an effort to construct results that are less on the theoretical side but actually useable in everyday business.

Bitcrime-Prosecution and Prevention of organized white-collar crime with virtual currencies

According to a recent report of the European Central Bank, virtual currencies “could represent a challenge for public authorities, given the legal uncertainty surrounding these schemes, as they can be used by criminals, fraudsters and money launderers to perform their illegal activities.” The BITCRIME stakeholders – the Austrian Ministries of the Interior and of Finance – and their German counterparts in this bi-lateral cooperation, share these concerns.

The goal of this project proposal is to research innovative solutions for the identification, prevention and reduction of organized financial crime, such as money laundering, with particular regard for virtual currencies (or more exactly decentralised virtual cryptographic currencies).

In its social, economic and legal aspects, the project will deliver a detailed survey including the collection and evaluation of information about the social and political landscape as well as trend prognoses created jointly with stakeholders. One part of the survey will describe the current situation regarding financial crime and its patterns, and will analyse existing financial institutions, products and supply chains, particularly in the context of virtual currencies. A second part will analyse existing virtual currencies, the role they play, and the problems they create. Information gathered from both Germany and Austria will be shared throughout the project and yield enhanced insights and analyses. The results will be made available in the form of four written reports, two available at the end of the first project year, and two available at the end of the second project year.

In the technical part of the project, we plan to test two hypotheses. First, in the context of the social, economic and legal survey, we will catalogue the characteristics of transaction patterns in organised financial crimes (money laundering, extortion, drug trade, etc.). We hypothesize that (a) similar patterns will apply to financial crimes carried out with virtual currency, and (b) we can automatically detect these patterns by analysing the transaction chains of those virtual currencies.

Our second hypothesis is that the application of a heretofore unique combination information sources (transaction, social media and Darknet analyses) to the problem of de-anonymization can contribute to a higher degree of efficiency in identifying actors in virtual currency transactions.

The resulting identifications should provide law enforcement agencies with information necessary to further an investigation, for example by providing evidence necessary for subpoenas, warrants, or wiretaps. The confirmation of our hypotheses will be demonstrated through software that will be installed, tested and evaluated by the project stakeholders.

Currently, the project has been started and the first results with respect to side parameters, requirements and analysis of the overall technical ecosystem have been generated. Especially regarding requirements, the main concern lies in the different targets of cryptocurrencies (namely anonymous transactions) versus law enforcement, where as much transparency as possible is needed.

SpeedFor – Speed Forensics

Digital forensics has received increasing attention in recent years as more and more crimes are conducted exclusively or with the involvement of computers. Especially in case of crimes that are solely conducted in the virtual world, e.g. certain prohibited forms of pornography, no offline "crime scene" exists, all evidence has thus to be seized in computer systems.

Tools and methods of digital forensics are used by private investigators as well as law enforcement analysts all over the world. One of the increasing challenges in digital forensics is the vast amount of data that needs to be analyzed. Commodity hard drives with up to four terabytes and more storage capacity are commodity hardware nowadays, and can be readily obtained by anyone.

However, the forensic processes in place today do not scale well to multi-terabyte workloads. Creating an image of a multi-terabyte hard drive for analysis takes 10-15 hours alone, and the time needed for further processing can exceed this many times over.

This is due to the fact that during investigations the complete data area on hard drives needs to be analyzed in detail instead of only allocated files, to search for deleted files or partially overwritten artefacts. As such, complex additional analysis steps like file fragment identification or advanced file system metadata analysis are often neglected, and their use on a regular basis does not take place due to time- and/or money constraints. This often leaves the analyst with the bare minimum of information extraction techniques like naive string search with word lists and superficial file system artefact analysis, while ignoring a multitude of additional information sources.

This project aims at fundamentally increasing the performance of current state-of-the-art forensic methods and decrease the manual work necessary for a forensic analyst in the course of a crime investigation by: by
1) developing new methods to increase the use of parallelized data processing within the specific environment of digital forensics;

2) identifying the best method(s) on how to exclude a possibly vast number of files and file system artefacts that are not specific to a case, and

3) streamlining and improve methods proposed in the literature that have not been included into existing processing steps for additional insights for various reasons.

Specifically, at the beginning of the project we evaluated new methods based on sector hashing in combination with fuzzy hashing to allow local file fragment (re-) identification of deleted and partially overwritten files. Currently we are creatingmethods based on the use of hash trees with adaptive hashing granularity during image creation to incorporate multiple sources of readily available file and sub-file hash values during analysis. Finally, based on the results derived from our work, we will design a privacy-aware protocol for private set intersection on a large scale to allow the use of cloud computing during digital forensic investigations. Data on hard drives contains per se sensitive information, and protecting this information is a vital requirement which needs to be guaranteed.

Past Projects:

1. SCUDO-A structured approach towards defence simulation trainings against cyber attacks

IT systems are nowadays heavily integrated into critical infrastructures and attached to vital parts of operative core components. Many organizations have contingency plans in case of attacks on their critical systems, especially targeting direct attacks against the company infrastructure. Post-mortem reviews of the contingency plans indicate that the plans are often outdated or even completely unknown to key players. The situation is even worse when the contingency plan of an organization relies on establishing communication with parties outside the administrative boundaries of the organization under attack, which is a major problem in cases of CyberTerrorism, where an attacker tries to inflict as much damage as possible by launching clever attacks against all vital parts of an infrastructure ecosystem, covering a multitude of different companies. The lack of updates in the partners’ structure results in loss of vital information, outdated assumptions, and inability to establish appropriate paths of communication and information exchange in case of an attack.

Regular training on different kinds of attack situations offers the possibility to detect and overcome these weaknesses. While the execution of table-top exercises is quite popular in several industries, still there are a lot of gaps in order to generate a standardized way of developing and executing suitable exercises for the participants. This especially includes topics such as the efficient setup of trainings, metrics for measuring readiness and progress, as well as the availability of tools for preparing and developing the exercises, including an appropriate environment for their execution and analysis. Especially important for this project was the focus on malicious attackers with an agenda in mind, not attacks done by mindless script-kiddies, thus also building up the need to involve major governmental stakeholders. Based on the trainings, we thus arrived at two major backgrounds regarding the attackers:

- Attackers that use a security issue in the target's system in order to either carry out criminal activities using the infrastructure, or blackmailing the owner into giving money.
- Attackers that try to damage an industry, attacking competing companies in the same area, as well as suppliers and customers of said industry/companies.

The main target of the SCUDO project lays in the generation of a training kit that allows for the straightforward tailoring of predefined basic scenarios into suitable and diverse training scenarios by non-experts in the field of simulation trainings or table-top exercises. It therefore included:

- A set of practical basic scenarios plus a repertoire of easy to deploy inline events.
- Guidelines for the adaption of the scenarios.
- Guidelines for efficient execution and operation of the training.
- Templates for the documentation of readiness and progress.

A special focus was put on the generation of exercises that involved several related institutions (e.g. supplier-customer) or competing companies, since conflicting contingency plans were identified as a major obstacle. Based on the feedback gathered from industrial and governmental stakeholders, three fundamental incident classes were defined. The first class (IC1) is concerned with a local disruption of vital IT services business operations (e.g. DNS), while IC2 deals with attacks against the availability and integrity of data transfer and (secured) IT-based communications. Finally, IC3 covers the worldwide disruption of integral IT services that are vital for business continuity, e.g. zero day exploits in the backbone router infrastructure. Based on these three significantly different incident classes, the options to be explored by the trainee response team are different in nature and focus, especially regarding issues such as possible information duties towards governmental actors or the general public, down to liabilities and other legal and regulatory issues.

The results of the project were evaluated in practical exercises attended by major players in Austria with emphasis on important providers for critical infrastructures and the respective governmental partners and ministries in an iterative workflow that fed back information and especially stakeholder needs to the project. The exercises indicated that the training simulated scenarios helped to drastically increase the readiness level of all players, leading to better reaction by their response teams, as well as to updating the contingency plans.

DIANA/DIANGO – Digital automated extraction of trends from open source information

Violent groups increasingly use the internet for organizational purposes, i.e. the Internet is increasingly used as means of communication and organization of groups that can be attributed with a terroristic or criminal background. Since the amount of available information in the internet is continually increasing, manual surveillance is not possible anymore. This causes undetected evidences that would have led to the initiation of countermeasures and seizure of the agitating persons when detected in time. By automatic extraction and analysis of global information- and communication services evidences with high potential for danger can be identified and handed over to experts for further analysis.

This allows that public organizations and institutions are informed in time. In the course of this project, new techniques regarding the following areas were developed in order to cater for the needs of LEAs in a context of detection of terroristic and criminal trends and implemented in the form of a usable and linked tool set:

Extraction of Information from the information sources: In this step the required sources are collected by crawler components. The previous state of art lacked the flexibility concerning sudden changes of the input format and handling of invalid file formats. The same applied to the harmonization of different formatting and metadata standards.

Semantic enrichment of messages: In this processing step the collected messages get semantically enriched, for example by the determination of known entities like specific persons or places. Specially problematic and relevant for research is in this context the language – comprehensive detection of known entities, the disambiguation of detected entities (e.g. persons) and the extraction of relations between these entities.

Classification of messages: This step further enriches the collected messages based on external knowledge databases, e.g. developed classification models or rule sets. Challenging was especially the development of a classification process (hierarchical multiclass – multi label classifier) required for a generic solution for this process.

Automated analysis and triggering: During this step the enriched messages get integrated in a graph-based model based on the results of the classification. The graph-based model is then used to detect predefined patterns automatically. The detection of such a pattern leads to the triggering of specific events. Relevant for research was especially the detection of specific patterns in a graph as well as handling time-based changes in the underlying structure.

Further analysis by experts: In this processing step the automatically pre- analyzed messages are forwarded to experts for further manual analysis. Apart from the actual result of the analysis itself the feedback of the automated result, which is used for correction and further improvement of the system, is relevant. Therefore an optimal processing of the massive data for visual and collaborative analyses is an essential criterion for success.

While the DIANA project concentrates more on the fundamental questions and is already finished, the ongoing DIANGO project adds more research in the area of rectifying the correctness of the information. Both projects are carried out in a consortium containing major Austrian stakeholders in order to guarantee the applicability of the results.

Portugal: the perspective of a LEA

Given the increasing development and use of new technologies, particularly those that provide access to the Internet, both in the context of infrastructures and in the individuals' daily life, Portugal is vulnerable and exposed to cybercrime and cyberterrorism.

Portugal adopted the Convention on Cybercrime (Budapest) in 2009, through the Parliament Resolution No. 88/2009 from 15 September. The new reality issued by the Cybercrime Law has created new needs of interaction between the prevention and investigation authorities and private entities. The current criminal investigation often resorts to measures of evidence collection in digital form assuming the collaboration from private entities (e.g. Internet service providers). Such entities - generally private companies - are the only holders of important information, often decisive for the discovery of the truth. In addition, some of the specific procedural steps contradict some of the procedural tradition by requiring effective collaboration from communications operators with prosecutors and criminal police in a way that was not allowed in previous legislative frameworks (secrecy of telecommunications).

Nowadays it is becoming more difficult to separate cybercrime from other criminal behaviors and consequently to provide statistics on cybercrime in Portugal. According to PJ, the major crimes currently investigated are computer fraud, phishing, child pornography, unlawful access (violation of business networks or e-mail and social networks such as Messenger or Facebook) and computer sabotage. These crimes have registered a proportional increase with the increased use of Internet especially in metropolitan areas which have easier access to knowledge, computers and the Internet.

To combat cybercrime, a Point of contact operates at PJ 24 hours a day and seven days a week. The high complexity of these crimes and the increasing number of criminal cases, as well as the huge volumes of data to analyse have led to delays in the process of resolving criminal cases and to high economic losses. Investigation of such crimes as Internet child pornography, require human and technical resources for extensive analysis, screening, decoding of data, including photos and videos that are encrypted or concealed and the identification and location of both criminals and victims.

Currently, Portugal has no National Report on Cybercrime. However, last year (2014) computer crime was for the first time analyzed and included in RASI[31] (Internal Security Annual Report). Data about cybercrime is provided by Polícia Judiciária to RASI. The analysis of this type of data still doesn't give a clear vision of the problem of cybercrime, because (1) it is collected according to efficiency criteria of criminal investigation and (2) due to the ambiguous definitions in the law.

Cybercrime covers two major areas of police action: cybercrime itself, which is established in the Portuguese Cybercrime Law, and all the crimes perpetrated with the use of electronic means. In its genesis, it still includes other types of crime, such as sexual abuse and various types of scams using the Internet **(Sistema de Segurança Interna, 2014)**.

The figures in the table below have the only purpose to show the evolution of the number of criminal cases that enter in the category of Cybercrime, investigated over the years (2005-20149). Also the number of complaints has been growing regularly.

Cybercrime	YEARS									
	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Nº cases investigated	**466**	**590**	**862**	**1652**	**3021**	**3353**	**3992**	**5143**	**5069**	**5461**
Nº Criminal complaints submitted directly to PJ	**266**	**312**	**418**	**841**	**1315**	**1444**	**1619**	**1771**	**1823**	**2270**

Table 4 - Statistical data gathered by PJ

The table below shows the number of defendants of cybercrime that were brought before the court in 2014, by each type of crime. This information also suggests clearly the main areas that must be addressed to bring solutions to the stakeholders' needs.

[31] RASI

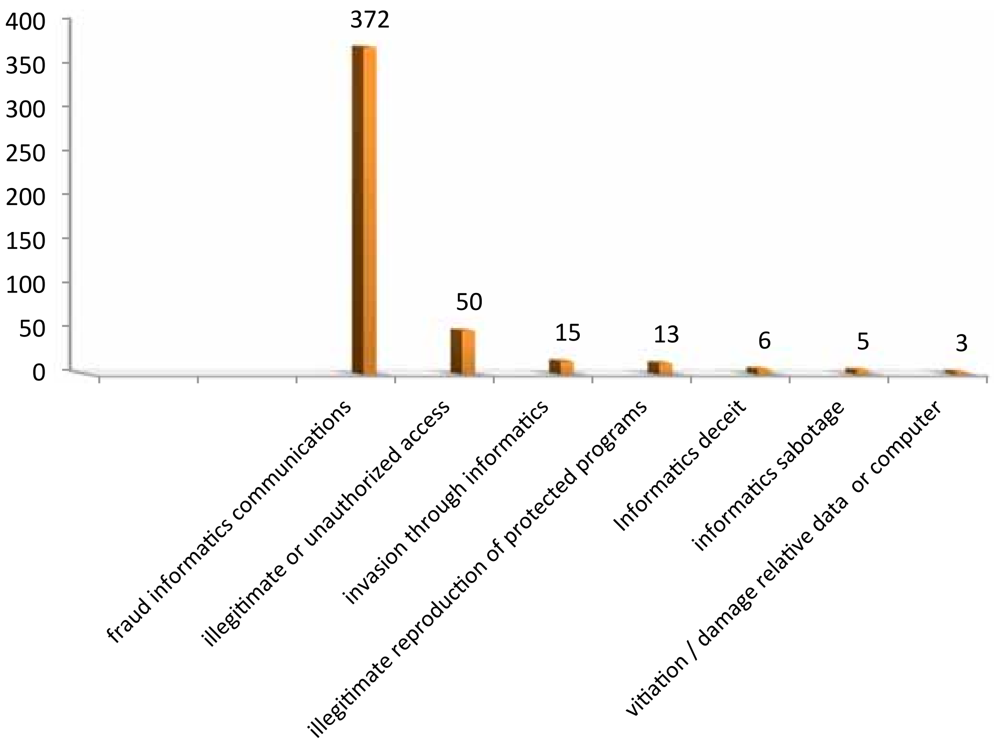


Table 5 - Number of defendants of cybercrime, 2014

Table: violation/damage relative data or computer… (?)

Recent studies have indicated, that economic crime, particulary the crimes perpetrated using cyber means, has been growing fast. However, there is a lack of data from the private sector, namely banks, insurance companies and financial institutions, which have been victim of cybercrime.

In general, these entities prefer not to complain to the authorities and to solve the problem by themselves, absorbing the losses. They fear that public knowledge of these attacks could lead to their disrepute and loss of trust from their customers. Often they consider the consequences of reporting cybercrime to the authorities greater than the criminal occurrence, namely the legal liability due to the protective duty of confidential data. Another common reason is the poor level of awareness or the belief of the ineffectiveness of the criminal inquiry and the feeling of impunity of these crimes. This makes it dificult to measure the reality and to perform quantitative and qualitative assessments about the reality and the consequences on the economy and the political situation.

IV - INPUTS FROM CYBERROAD SURVEYS/QUESTIONNAIRE

THE CYBERROAD SURVEY ON CYBERCRIME (WP5) - EVALUATION OF STAKEHOLDERS' NEEDS AND THREATS

The aim of this Survey was to explore and establish the needs of stakeholders and find out what they see as the potential threats, both now and in the future.

Some conclusions

Most of the respondents (individuals and organizations) assess cybercrime as criminal activity carried out by means of computers or the Internet, as well as any criminal act or hacking of computers and network, acts against the confidentiality, integrity and availability of computer data. There is a moderate (32. 1%) to a very high concern (31.5%) about cybercrime.
At a legal dimension, namely the respondents' action after being victims of cybercrime, 36.6% didn`t report the action to the police; some reported to the police but with no further action (8.1%) and (8.8%) had their report to the police, who followed it through but no prosecution took place.

The questions about ethics meant to reveal the respondents' opinion on what should be the focus of research, in order to fight cybercrime and to make internet a safer place. A better education for users and improved technology for our networks and operating systems is needed.
Cybercrime was considered as rooted mostly in economic interests and technology.

THE CYBERROAD QUESTIONNAIRE ON CYBERTERRORISM (WP6)

The purpose of the CyberROAD questionnaire on cyberterrorism was to obtain an updated view on potential threats identified by the stakeholders as well as the needs, in order to prevent or deal with the threats, both at the present moment and in the near future.

This questionnaire was submitted to stakeholders based on their respective role in this eco-system, namely:

- LEA
- Justice Infrastructures
- Universities
- Health service providers
- Rail infrastructures
- Roadtransport companies

- ISPs
- CERT
- SMEs and Large Enterprises

As to the needs, it was possible to identify the following areas where an action needs to be taken:

- Legal framework and faster creation of legal instruments
- Harmonisation of legal frameworks in Europe
- Competences of police forces
- Timely national and European cooperation
- Awareness (political and social)
- Privacy and trust aspects
- Human resources / IT Resources
- Training for experts IT
- Security policies inside organizations
- Data and privacy issues
- Education for prevention
- Legal framework adapted to new types of digital crimes
- Risk management
- Public-Private Cooperation
- Best practices guides
- Critical infrastructures protection/prevention
- Technology and IT Systems protection
- Ethical domains research
- Political/Social interventions

Analysing the situation at organizations in charge of the prevention and fight, it was possible to identify several aspects that require attention:

- International Cooperation – All entities envolved in the problematic (LEAs, Judicial System, Intelligence entities, European and International entities, …)
- Coordination among security forces
- Harmonisation of legal instruments in Europe
- Clarification of competences of LEAs
- Establishment of specialized units, technologically well equipped and with highly qualified and specialized staff
- Enhancement of law enforcement capabilities
- Capacity to anticipate the innovation capacity of terrorists
- Exchange of information
- Technology and IT systems

- Training
- Cyber intelligence capacity
- Predictive capacities regarding new threats
- Cyber resilience

Concerning general security threats, 23% of respondents said their organizations provide guidelines of best practices, namely tools in the field of security policies, including ISO 27001, behavioural rules and awareness measures, as well computer system hardening, safe browsing and emails handling, but only 18% said their organizations provide a Plan of Incident Response.

Regarding best practices that specifically tackle the threat posed by cyberterrorism, only 9% said to have best practices, which are basically the same as in cybercrime, such as Data loss prevention and security policies, technical aspects including anomaly detection, pattern analysis, malware analysis, blacklists, cloud security, data loss prevention and non-technical aspects including ISO 2007 certification, policies, awareness measures and others. Nevertheless, only 18% of respondents said their organizations have Plan of Incident Response.

Concerning Cooperation, 17% of the respondents of the Cyberterrorism questionnaire said their organizations cooperate with the public and/ or private sector on cybersecurity. However, there is a strong need for a cooperation model that includes the different stakeholders, namely:

- National and International Security forces
- Armed Forces
- LEAs
- Civil Protection
- Private sector
- Academias and Universities
- Think Tanks
- NATO
- European Defence Agency
- …

Regarding the subject above, and on the basis of the same questionnaire, the respondents consider that the key elements for a good Public-Private cooperation model would be:

- Building-up trust
- Sharing of information
- Periodical meetings

- The implementation objective cooperation and not get it just by exercising
- Secure environnements/infrastructures for information exchange
- Well defined rules, outlined by the law, with legislation standards
- Financial improvement on behalf of the Public Sector

V - Final Conclusions

Both the answers to the surveys (WP5) and the questionnaire (WP6), as well as the literature review allow us to suggest that attention should be paid to the various aspects related to cybercrime and cyberterrorism, namely the technological, legal, political, economical social and educational ones.

Taking into consideration the severeness of the threats, it is important to identify the technological innovations that may turn it easier to identify the threats in the digital world and easily neutralize them.

Public policies on education and employment should be translated into a common strategy to increase the level of public awareness and the job opportunities in Europe.

The legal frameworks must be taken into account and they must be adapted to the identified threats and needs. The issues of privacy, digital security and data protection must be addressed also from this perspective.

The cooperation between public and private sectors is a major issue. It is important to bridge them. It is also critical to define a model of public-private partnerships.

The trainings for all the judicial system actors as well as the cooperation with the police needs to be improved.

The level of awareness needs to be improved, both from the perspective of the organizations (public and private) and of the citizens.

(Polícia Judiciária, 2015).

Bibliography

AGNU 2020 - Mídia e Terrorismo. (n.d.). Retrieved 03 03, 2015, from https://minionu15anosagnu2020.wordpress.com/terrorismo-conceitos/

BUIKHUISEN, W., & MEDNICK, S. (1988). *Explaining Criminal Behaviour.* New York: E.J.Brill.

CAMINO. (n.d.). *Cyber security -Cyber terrorism - Cyber crime - ROADMAP*. Retrieved from http://www.fp7-camino.eu/

Comission European. (n.d.). *Comprehensive Approach to cyber roadMap coordINation and develOpment*. Retrieved from http://cordis.europa.eu/project/rcn/185485_en.html

Europe, C. o. (2011, September). *Project on Cybercrime*. Retrieved from Global Project on Cybercrime (Phase 2): http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/2079%20adm%20pro%20summary%20_26%20Sep%202011_.pdf

Europe, Council of. (n.d.). Retrieved from COURAGE - Cybercrime and cyberterrOrism (E)Uropean Research AGEnda: file:///C:/Documents%20and%20Settings/lsampaio/My%20Documents/Downloads/CORDIS_project_185504_en.pdf

Europe, Council of. (2013, June 12). *CyberCrime@IPA*. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/2467_Assess_Rep%20v51_public.pdf

Europe, Council of. (n.d.). *CyberROAD - CYBER crime and CYBER terrorism reseach ROADmap* . Retrieved from http://goo.gl/oglfQx

Europe, Council of. (n.d.). *E-CRIME - the economic impacts of cyber crime.* Retrieved from http://goo.gl/RbGN7t

Europe, Council of. (n.d.). *Octopus - CyberCrime.* Retrieved from http://goo.gl/kJKCPS

Europe, Council of. (n.d.). *Global Project on Cybercrime.* Retrieved from http://goo.gl/tsGMXC

Europe, Council of. (2012, April 9). *Global Project on Cybercrime (Phase 2).* Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_adm_finalreport_V12_9apr12.pdf

Europe, Council of. (2010, May 28).

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/2215_d_Cyb_Georgia_Evaluation_Report_FINAL.pdf. Retrieved from Project on Cybercrime in Georgia: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/2215_d_Cyb_Georgia_Evaluation_Report_FINAL.pdf

Europe, Council of. (n.d.). *IPA Project*. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20project%20balkan/2467_Assess_Rep%20v51_public.pdf

Europe, Council of. (n.d.). *Project Cybercrime EAP*. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Project_EaP/2523%20eap%20cyber%20summary2a_%2009May2014.pdf

Europe, Council of. (n.d.). *Project Cybercrime EAP II*. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@EAP/3271%20CEAP2_summary_v2.pdf

Europe, Council of. (n.d.). *Project on Cybercrime*. Retrieved from http://goo.gl/oKYOId

FSB. (2013). *Cyber security and fraud: The impact on small businesses.*

GARCÍA-PABLOS, A. (1988). *Manual de criminología. Introduccíon Y eoriías de la criminalidad.* Madrid: Espasa-Calpe.

ICSPA. (2012). *Project 2020 Scenarios for the Future of Cybercrime.*

LIPOVETSKY, G., & JUVIN, H. (2010). *L'Occident mondialisé : Controverse sur la culture planétaire.* Paris: Grasset.

Polícia Judiciária. (2015). *Cyberterrorism*. Lisbon: CyberROAD.

PwC's 2014 Global Economic Crime Survey. (n.d.). Retrieved July 24, 2015, from Pricewaterhouse Coopers (2015): http://www.pwc.com/crimesurvey

Relazione sulla politica dell'informazione per la sicurezza 2014. (n.d.). Retrieved July 24, 2015, from Italian Security Intelligence Department - DIS (2015) :

http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2015/02/relazione-2014.pdf

Sistema de Segurança Interna. (2014). *Relatório Anual de Segurança Interna.* Retrieved from http://goo.gl/VSO9Hi

Swansea University. (n.d.). *Cyberterrorism Project.* Retrieved from http://www.cyberterrorism-project.org/

The British Retail Consortium. (2014). *BRC Retail Crime Survey 2014.*

The Digital Economy and Society Index (DESI) 2015. (n.d.). Retrieved July 24, 2015, from European Commission – The Digital Agenda for Europe Initiative: http://ec.europa.eu/digital-agenda/en/desi

UK GOVERNMENT. (2011). *THE COST OF CYBERCRIME.* Retrieved 05 22, 2015, from https://www.gov.uk: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

UNODC. (2013). *UNODC Emerging Crimes - Cybercrime Study 2013.*

UNODC. (2013). *UNODC Emerging Crimes - Cybercrime Study 2013.* Retrieved May 2015, from http://www.unodc.org/unodc/search.html?q=cybercrime

VOGT, w. (1993). *Durkheim´s sociology of law: Morality and cult of the individual.* (Routledge, Ed.) London.