CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

D6.1 – Cyber Terrorism Stakeholder Needs and Threats Evaluation

Date of deliverable: 31/05/2015
Actual submission date: 22/06/2015

Start date of the Project: 1st June 2014 Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 1.1

Project funded by the European Commission Directorate-General Home Affairs in the Prevention of and Fight against Crime Programme		
Restriction Level		
PU	Public	no
PP	Restricted to other programme participants (including the Commission services)	no
RE	Restricted to a group specified by the consortium (including the Commission services)	no
CO	Confidential, only for members of the consortium (including the Commission)	✓

Revision history

Version	Object	Date	Author(s)
0.1	Creation	05/03/2015	PJ, INOV
1.0	Revision 1	15/03/2015	PJ, INOV
1.1	Revision 2	25/05/2015	PJ
1.2	Revision 3	30/05/2015	PJ
2.0	Final	22/06/2015	PJ

D6.1

CYBERTERRORISM
Stakeholder Needs and Threats

Responsible
PJ - POLÍCIA JUDICIÁRIA

Contributor(s)
INOV
UNICA
INDRA
SM
FORTH-ICS
NASK
HMoD
MCAFEE

1 Table of Contents

2 LIST OF FIGURES

3 LIST OF TABLES

4 ACRONYMS AND ABBREVIATIONS

Acronym	Definition
ACM	Association for Computing Machinery
CDD	Cyber Defence Directorate
CIT	Clean IT
COTS	Commercial Off The Shelf
CT	Counter-terrorism
CTW	Check the Web
EDA	European Defence Agency
EJI-CT	European Joint Initiative on Internet and Counter Terrorism
ENLETS	European Network of Law Enforcement Technology Services
EU IRU	European Union Internet Referral Unit
EUMS	European Union Member States
FBI	Federal Bureau of Investigation
FTF	Foreign Terrorist Fighters
HMOD/NSA	Hellenic Ministry of Defence/National Security Authority
ICT	Information and Communication Technologies
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
I2P	Invisible Internet Project
IRC	Internet Relay Chat
IRU	Internet Referral Unit
ISIL-ISIS-IS	Islamic State of Iraq & Levant- Islamic State of Iraq & Sham- Islamic State
ISP	Internet Service Provider
JHA	Justice and Home Affairs
LEA	Law Enforcement Agency
OSINT	Open Source Intelligence
PJ	Polícia Judiciária
IPCT	Information Processing and Communication Technology
UN	United Nations
TOR	The Onion Router
UNCT	Unidade Nacional Contra-Terrorismo (National Counter-Terrorism Unit)
UNODC	United Nations Office on Drugs and Crime

Cyberattacks perpetrated by terrorists	Such as defacement of sites, like governmental ones, TV station chains or any other infrastructures and social media – causing great impact with the potential to disturb the organization of the societies.
Cyberterrorism	The concept of cyberterrorism is quite controversial among experts and analysts on the field. Two possible definitions are: • The politically ideologically motivated use of cybermeans and information technology to cause severe disruption of the States' Security, widespread fear and threat among the population. In that sense, the concept of cyberterrorism as a general category comprises: cyberterrorist attacks, cyberattacks perpetrated by terrorists and the use of internet by terrorists for different purposes. • Digital attack of a ideological nature by practice of an illicit act, with the intent to cause disruption, damage or affecting confidentiality, integrity, availability and non-repudiation of electronic information.
Cyberterrorist attack	Use of electronic means/ ICT to perpetrate attacks – threatening or eliminating human lives, causing huge damage, challenging and jeopardizing the State security based on democracy and the rule of law – having a political, ideological, ethnical and/or religious nature and motivation.
Terror	"*Something that intimidates, an object of fear*," from Old French terreur (14c.), from Latin terrorem (nominative terror) "*great fear, dread, alarm, panic; object of fear, cause of alarm; terrible news*," from terrere "*fill with fear, frighten*," (Online Etymology Dictionary, 2015).
Terrorism	The use of violence and threats to intimidate or coerce, especially for political purposes (Dictionary.com, 2015).
Terrorist offences	Intentional acts which, given their nature or context, may seriously damage a country or an international organization where committed with the aim of: seriously intimidating a population, or unduly compelling a Government or international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization

	(European Union, 2002)
Use of internet by terrorists	The use of internet for terrorist purposes, such a diffusion of propaganda, indoctrination and recruitment, radicalization, plotting, training, publication of communiqués. logistics, planning, etc.

6 EXECUTIVE SUMMARY

The aim of Work Package 6 is to contribute for a better understanding of cyberterrorism, in its multiple *modus operandi*, trying to provide a more concrete overview of the various facets and expressions.

It will focus on the evaluation of stakeholders' threats and needs in this criminal field. It will give inputs for the Deliverables 6.2 and 6.3, with a view to identify best practices that may increase resilience and protection against cyber threats related to terrorism. By knowing the threats and identifying the needs to face the threats, it will be possible to identify best practices.

This document will try to contribute to a definition of cyberterrorism, which might be commonly accepted as a basis for further insights on the subject.

Three new concepts will be considered and will be taken into account in this document: "Cyberterrorist attack", "Cyberattacks perpetrated by terrorists" and the "Use of internet by terrorists". These concepts will be further explained in point 8.3 -. It is really important to make a distinction among each of them, in order to be more concise and enabling to address each of these three new perspectives.

The initial question that we wanted to address is to know to what extent Europe and the European Union Member States (EU MS) are aware of the threats posed by terrorism, how they are prepared to neutralize and/or to fight against it. The standard of awareness is vital for the preparedness to face such threats.

A reference will be made to internet as the platform that has been allowing for the change in crime paradigm. Alike other forms of crime, the use of internet turn terrorism into cyberterrorism.

The traditional forms of crime have been "upgraded", when using cyber means to perpetrate it. For instance:

Burglary → Hacking;

Deceptive callers → Phishing;

Extortion → Internet extortion;

Fraud → Internet Fraud;

Identity Theft (identity documents) → Identity Theft (digital identity);

Child pornography → Child pornography (online).

In the same way,

Terrorism → cyberterrorism - when it is perpetrated using cyber means (electronic means based on internet).

After identifying the threats, there will also be a focus on the needs, trying to find the gaps between both.

Keywords: *internet, cyberterrorism, needs, threats.*

7 METHODOLOGY

In order to meet the goals of this deliverable, the methodology considered to be more appropriate consisted of the documentary analysis and the bibliographic research throughout books, articles, newspapers articles, reports from related European funded projects and documents issued by relevant European and International organizations. Most of the information and documents analysed are public and open source based.

Whenever possible and adequate, the external open source information was complemented with internal information emerging from the activities and work performed by Polícia Judiciária (PJ), which is a Law Enforcement Agency (LEA) and an end-user of CyberROAD.

Terrorism and internet are addressed, with a view to prepare the context for the analysis of cyberterrorism.

Some studies were analysed and brought to this document, as they focused on cyberterrorism, aiming at contributing to multilateral responses to this issue. An overview of threats and consequent needs is made in three main fields, in terms of vulnerability to cyberterrorism: internet and mobile devices, social networks and critical infrastructures.

A questionnaire was prepared in order to collect information on stakeholders' threats and needs. This questionnaire was personally introduced and explained to stakeholders considered as relevant by the partners. Taking advantage of the fact that this work package is led by a LEA, most of the entities were LEA in several EU MS: Austria, Belgium, Bulgaria, Cyprus, Croatia, Denmark, Slovakia, Spain, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, United Kingdom, Czech Republic, Romania and Sweden.

Among the entities that were approached to answer the questionnaire, beyond LEA, there were SME, critical infrastructures and universities. Europol and Interpol were also contacted, but for any reason, they did not answer the questionnaire.

The aim of the questionnaire was to obtain updated perspectives on the issue of cyberterrorism. The results will be presented in point 10.3.4.

The analysis of the information obtained allowed for the comparison between the knowledge contained in the available literature analysed and the "real world" in this moment, expressed in the answers to the questionnaire. Those answers helped to draw conclusions and recommendations concerning threats and also to take into account the identified needs.

Those conclusions and recommendations may be relevant for the future action of the EU.

8.1 TERRORISM

Terrorism has its linguistic roots in Latin etymon TERROR, "*fear*", "*terror*" from, "*terrere*", "*scare*", "*cause fear*" (Dictionary.com, 2015). The acts of terror have been present since the origins of civilization. However, it is not possible to accurately identify the date for the appearance of the first terrorist actions in history**.** A few examples are**:** between the first and second centuries B.C., e.g. "*Resistance to the Romans by the Zealots, who tried to protect the Jewish tradition and its most radical sector, hit men who murdered both Roman authorities as Jews who collaborated with the occupation*."; in the Middle Ages, the Inquisition was hunting people accused of witchcraft (the witches, mostly women), people considered dangerous who were chased and persecuted, beaten and beheaded in public; more recently, the attacks on 11 September 2001 in the USA, committed by *Al-Qaeda*; and currently the genocide being carried out by the *ISIL-ISIS-IS* against the population of the ancient states of Syria and Iraq (Sham or Levant).

Terrorism definition is controversial, its borders are diffuse and the concept has been extensively discussed. It is known as a social phenomenon, "*constitutes one of the most aggressive forms of organised crime, by the means used and purposes which aims to achieve*" (Braz, 2009,) and it is "*distinguished by acting based on political motivations, ideological and religious, not having as ultimate goal to obtain financial compensation*" (Ventura, 2003,); it reaches indiscriminately a large number of innocent victims - men, women and children. It is intended to cause fear, panic and a feeling of insecurity in people or the State, enhanced by publicity and media coverage. In this regard it is worth to recall that a terrorist act is only valid if it is disclosed. As early as 1985, the then British Prime Minister Margaret Thatcher pointed the finger at the media *"that democracies must find a way to starve terrorists and hijackers of the oxygen of publicity on which they depend" (*Cottle, 2006)

Indeed, terrorism is powerless if not publicized. It depends on the dramatic impact to capture the attention of public opinion and, consequently, achieve its main objective: to spread fear[1] (Faria, 2007).

Quoting the old chinese saying: kill 10 and you will call the attention of tens of thousands. In other (equivalent) words rather then the effects and concrete consequences of the terrorist attacks, the major outcome and impact, results in the sense of threat and the feeling on insecurity or unsafety among the community and its population. That is exactly what terrorists are looking for.

For organised crime, financial advantages and income are the major end goals to be achieved. For terrorists, financial assets and profits are basically or merely means to reach political-ideological objectives.

Those political-ideological end goals or objectives to be reached could be, for example, the institution of the worldwide Islamic caliphate – as islamists towards *Al-Qaeda* and the *ISIS-ISIL-IS*

[1] *Vassily Yastrebov, mental health specialist, believes that one of the most important consequences of terrorism, desired by the terrorists, is the state of panic the population. For him, "the specific characteristics of the different forms of terrorism is a prolonged state of anxiety and fear among the population, which remains in expectation of tragedy; this uncertainty that causes serious psychological disturbances*."

are intending and fighting for – the self-determination of a certain population and/or geographical area without autonomous sovereignity – take the Basque Country (ETA) the so-called Eealem (LTTE) Kurdistan (PKK) or the Corsican Island (FLNC) as a few examples; or even disrupting States' democracy acting under the rule law by the imposition of anarchism, far-left (marxist-leninist) or far-right (national-socialism) ideologies and eventually associated dictatorships in a given country.

Contemporarily, following the murder of King Alexander of Yugoslavia, who was assassinated along with the French Foreign Minister, Louis Barthou, in Marseille in October 1934, the League of Nations brought terrorism to the international agenda, discussing a convention to prevent the phenomenon and punish its interpreters. Three years later, a diploma was published but it never turned into force.

Since the sixties of the latter century, there has been an increasing concern about terrorism, as we may conclude by the number of resolutions signed by UN Security Council, namely:

- **International Convention in order to stop Terrorism Financing, adopted in New York in December 9th, 1999** – has been adopted by the UN General Assembly on the 9th December 1999;

- **International Convention for the Suppression of Terrorist Bombings, adopted in New York in the December 15th 1997** - Adopted by the UN General Assembly on the 15 December 1997 and opened for signature on the 12th January 1998;

- **International Convention against the Taking of Hostages**, adopted in New York, on the December 17th 1979;

- **Convention on the Prevention and Punishment of Crimes against People who enjoy an International Protection, including the Diplomatic Agents**. Adopted in New York in December 14th, 1973;

More recently, especially since the 9/11 September 2001, in the USA, the UN Security Council, signed several resolutions[2] to fight against terrorism, namely:

- **Security Council Resolution 1368** (on the 12th September 2001), where we can read:

  "The Security Council,

  Reaffirming the principles and purposes of the Charter of the United Nations,

  Determined to combat by all means threats to international peace and security caused by terrorist acts,

  Recognizing the inherent right of individual or collective self-defence in accordance with the Charter,

  1. *Unequivocally* condemns in the strongest terms the horrifying terrorist attacks which took place on 11 September 2001 in New York, Washington, D.C. and Pennsylvania and

[2] http://www.un.org/en/sc/documents/resolutions/

> regards such acts, like any act of international terrorism, as a threat to international peace and security;
>
> 2. *expresses* its deepest sympathy and condolences to the victims and their families and to the people and Government of the United States of America;
>
> 3. *Calls* on all States to work together urgently to bring to justice the perpetrators, organizers and sponsors of these terrorist attacks and stresses that those responsible for aiding, supporting or harboring the perpetrators, organizers and sponsors of these acts will be held accountable;
>
> 4. *Calls also* on the international community to redouble their efforts to prevent and suppress terrorist acts including by increased cooperation and full implementation of the relevant international anti-terrorist conventions and Security Council resolutions, in particular resolution 1269 (1999) of 19 October 1999;
>
> 5. *Expresses* its readiness to take all necessary steps to respond to the terrorist attacks of 11 September 2001, and to combat all forms of terrorism, in accordance with its responsibilities under the Charter of the United Nations;
>
> 6. *Decides* to remain seized of the matter." *(Security Council - Resolution 1368 (2001)*

- **Common Position 2001/931 / CFSP** - The Extraordinary European Council meeting of 21st September 2001 has defined terrorism as one of the biggest global challenges and had identified the fight against terrorism as one of the priority goals of the European Union (EU);

- The **Framework Decision 2002/475/JHA** of the Council of the 13 June 2002, is the basic instrument of the EU law on the fight against terrorism.

8.2 INTERNET

"The era we are living in is marked by a strong and irresistible chain of unification around the world" (Lipovetsky & Juvin, 2010). The globalization of the world, human relations, economy, technological innovations, ideas and thoughts became possible thanks to communication model clusters, which throughout computers and networked devices, allow the sharing of information in real time.

The internet, initially ARPANET (*Advanced Research Project Agency Network*), emerged in the sixties at the height of the Cold War, starting from military research of the US Department of Defense. Only 10 years later, universities were allowed to enter the network via the telephone network, and in the early nineties' with 7 million users we already could consider the internet as an international platform. In this decade there was an increase in technologies for internet access, in terms of contents available, and an exponential growth of users. According to internet World Stats, by June 30, 2014, the number of internet users was established in 3,035,749,340[3] and the access to this cyberroad has been materialized as a fundamental right of users[4].

[3] According to Internet World Stats in http://www.internetworldstats.com/stats.htm

[4] According to BBC News http://news.bbc.co.uk/2/hi/technology/8548190.stm

Internet has become a land for all and nobody, a place where you can find the best and the worst of mankind. Internet has democratized knowledge leading us everytime to everywhere, to a vast world of information accessible to almost everyone, making it easier the communication among people and organizations who are physically far away.

Industrialized and emerging countries use internet in all sectors of State´s activities, from the political level to social and economical ones, especially in the modern infrastructure systems, which come from the 19th century. There has been an increase of the value Internet has in the economy and security of the countries, particularly in the most developed ones.

Internet has not only benefits; it is also a very powerful instrument for the perpetration of serious crimes. It is the privileged instrument for the change of crime paradigm. Cyberterrorism is just an example.

8.3 CYBERTERRORISM

According to the earliest and still most used definition originating from US Army sources in the nineties cyberterrorism is "*The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives*".

Further from this perspective, **c**yberterrorism is limited to actions by individuals, independent groups, or organizations. If such actions are state sponsored, it is by definition an act of cyberwar. A now commonly held macro view is that digital attacks to cyber based businesses, ideologically based, are cyberterrorism (*e.g.* recent Sony attacks). This is opposite to economic based ones, which one would classify as cybercrime. The impact is quite different.

The additional protocol to the Budapest Convention, the Convention on Cybercrime, establishes the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Although the Convention does not directly state that this is a protocol for cyberterrorism, relevant authorities refer to it as the source of reference on the issue of cyberterrorism and which, furthermore, has been ratified by numerous countries. Therefore, we could conclude that the definition of cyberterrorism can fall under the same definitions as cybercrime but with an extended scope. This means that international cooperation may be critical to counter cyberterrorism attack**s**.

According to the experience collected and gained by PJ on the ground of criminal investigation and in dealing with cybercrime, terrorism and cyberterrorism, we could perhaps conclude that cyberterrorism is a specific chapter of cybercrime – the overall or general category – while one would notice or detect significant differences in terms of impact of cyberterrorism, based on its pursued political-ideological motivations as explained in detail in the previous items. On the other complementary perspective, the fact that cyberterrorism means some sort of digital attack of a ideological nature by practice of an illicit act, with the intent to cause disruption, damage or affecting confidentiality, integrity, availability and non-repudiation of electronic information.

“*The fight against terrorism in all its forms is now the major European and international priority*” (Reeb, 2010). Until the advent of September 11, 2001, the competent authorities basically faced terrorist action outbreaks of religious outlook, but we see now that it was just the starting point to cyberterrorists, who intensified their actions resulting in huge losses. “*Since then, new standard was stated and a new trend materialized which achieved expression in global terrorism”* (Ventura, 2010,).

“The emergence of the cyberterrorism domain means that a new group of potential attackers on computer and telecommunication technologies may be added to the list of traditional criminals threatening Information and Communication Technology (ICT) Infrastructure” (Janczewski, 2007).

Internet has thus become an alternative space of action for criminals and criminal organizations, it is an area without physical borders, landless and transnational, allowing to cause harm to geographically distant States.

“Contrary to the definitions of terrorism (including the psychological aspects of the terrorist’s behaviour, the criminological features of terrorist action and its constituent elements, commonly referred to by various doctrine, the current definition of ‘cyberterrorism’ is still more controversial than that of terrorism, and it is usually focused on the attacks to physical structures of modern information, processing and communication networks” (Bravo, 2010).

Despite the fact that cyberterrorism definition can potentially lead to misunderstanding in criminal field mostly all the authors link the two concepts - terrorism and cyberterrorism - to a certain political purpose regarding the use of violence or the threat of its use where no one is excluded,“*neither women, nor children*”; for most of the thinkers, the issue at hand here has not been accepting that terrorist acts might be taking place within networks and IPCT, but considering that cyberterrorism only exists when the attack is related to behaviours with particular motivations and intensities with some impact in society. Others would underline in particular the circumstance that cyberterrorism has been defined as a type of terrorism perpetrated through attacks to IPCT infrastructures, which equals it to a massive destruction weapon, due to the notorious social consequences that might result or derive from there. According to this point of view, cyberterrorism will always translate into an attack aimed at compromising security (in a wide sense), which has simplicity and surprise as features, and which is (mainly) targeted at civilians and/or militaries. The issue is of peculiar relevance, not only because the topic is a current one and the public is sensitive and aware of it, but also because there are other “attacks” likely to occur within the IPCT which shall not be considered as cyberterrorism (Bravo, 2010).

A cyberterrorist attack involves the loss of human lives – or a significant threat and risk for those human lives - or it causes huge economic damages, when hiting critical infrastructures, disturbing and jeopardizing the regular functioning of a State (thus attempting to the State security) disregarding the activity of the cyberspace itself. (cf. https://www.academia.edu/943512/From_the_Spectrum_of_conflict_within_information_networks_Towards_a_conceptual_reconstruction_of_terrorism_in_cyberspace).

Neither the definition nor the context of the term cyberterrorism have reached so far a broad consensus within the (international) instances dealing with this topic.

The use of internet by terrorists is known from intelligence services and/or LEA for a long time. From the point of view of the fight against terrorism, the activities performed by terrorists using internet holds four main objectives: Communication, propaganda, recruitment and training (Mariani, 2015).

In the line of the previous statement and taking into account internal considerations, doctrine and concepts in use by PJ's National Counter-Terrorism Unit (PJ-UNCT) where criminal investigators identify and explain some basic definitions and contexts of terrorism, the present document adopts those definitions for the purpose of this deliverable, as follows:

- **Cyberterrorist attacks** , the possibility to use electronic means/information technologies to perpetrate attacks, whose dimension threatens human lives, may cause huge damage, challenging and jeopardizing the State security based on democracy and the rule of law. Such attacks have a political-ideological, ethnical and/or religious nature and motivation;
- **Cyberattacks perpetrated by terrorists**, such as defacement of sites, disturbing the regular functionality of services as TV Channels and other infrastructures. These attacks may have a great impact on society holding the potential to disturb the organization of the societies;
- **Use of Internet by terrorists**, the use of internet / information technologies for terrorist purposes, like propaganda, financing, communication, recruitment, plotting, indoctrination, radicalization, logistics, planning, training, material dissemination, etc.

These three concepts follow the common understanding shared by officials pertaining to the international counter-terrorism (CT) community as stated by Mariani (2015).

According to the report issued by the European funded *Clean-IT* Project, "*Reducing terrorist use of the Internet*" (National Coordinator for Counterterrorism and Security, 2013), which is the result of a "*structured public-private dialogue between government representatives, academics, Internet industry, Internet users and non-governmental organizations in the European Union, two concepts were addressed within the European framework and contribute to the European terminology acquis – "Terrorist offences" and "Terrorist use of the Internet*"**:**

- **Terrorist offences** - the EU has defined terrorist offences as *"intentional acts which, given their nature or context, may seriously damage a country or an international organization where committed with the aim of: seriously intimidating a population, or unduly compelling a Government or international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization*" (EU Framework Decision, 2002/475/JHA of 13 June 2002 on combating terrorism). The EU has further identified the following offences as being linked to terrorist activities: '*public provocation to commit a terrorist offence, recruitment for terrorism, and training for terrorism'* which can also be committed in the online environment (Framework Decision 2008/919/JHA, 28 November 2008, amending the 2002 Framework Decision).
- **Terrorist use of the Internet** - the use of the internet for terrorist purposes, including for public provocation (radicalisation, incitement, propaganda or glorification), recruitment, training (learning), planning and organizing terrorist activities which are also terrorist offences on their own according to the current legislation.

Cyberspace is used by terrorists as a target, as a weapon and/or as a resource as well. As a target, terrorist activities are aimed at the internet itself and its infrastructure; as a weapon, attacks are perpetrated against physical targets via the internet; as a resource, it provides extremists and terrorists with a wide range of possibilities and applications to pursue their cause. *"The main uses are gathering and dissemination of propaganda, radicalization and recruitment, planning, communication and coordination and fundraising"* (United Nations Office on Drugs and Crime, UNODC 2012).

Further to the above mentioned uses of internet, it is also used as an instrument to control the public perception, the so-called "spin control". This consists of a purposeful strategy of flooding cyberspace with targeted information, which aims at assessing and manipulating public opinion. Actually, this seems to be one of the main features of *ISIL-ISIS-IS*, which often resorts to narratives of propaganda and manipulation of public opinion in social networks and search engines.

Cyberterrorism is more anonymous than traditional terrorist methods – "*in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross; no customs agents to outsmart"* (Weimann, 2005); it can be conducted remotely; it requires less physical training, less psychological and economical investment, less risk of mortality and travel than conventional forms of terrorism; it is easier for terrorist organizations to spread its "terrorist culture", which includes its history, postulates and objectives to be achieved with its cause; it makes it easier to recruit and retain followers; the variety and number of targets are enormous; it has the potential to affect directly a larger number of "*people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want"* (Weimann, 2005).

In this context, when countries face the threats posed by terrorists, who can "*access to sensitive information and to the operation of crucial service having broken into government and private computer systems, cripple or at least disable the military, financial, and service sectors of advanced economies*" (Weimann, 2005), there is a general perception that the organizations, infrastructures, and people are vulnerable. *In effect, the cyberterrorist will make certain that the population of a nation will not be able to eat, to drink, to move, or to live. In addition, the people charged with the protection of their nation will not have warning, and will not be able to shut down the terrorist, since that cyberterrorist is most likely on the other side of the world* (Collin, 1997).

Considering the enormous potential of cyberterrorism to cause huge damage, the fight against terrorism in all its forms is a great European priority, as well as worldwide, and although international cooperation in fighting terrorism has been intensified for many years, there is still a long way to follow specifically in this new trend on the fight against cyberterrorism.

9 LEGAL FRAMEWORK

From the point of view of a LEA, the legal framework is one of the basis needed for the CT action. Therefore, we looked at the legal framework in Portugal, which has recently adopted complementary legislation on the fight against terrorism, somewhat including cyberterrorism. In order to get a broader picture, we overlooked at the member countries of the Council of Europe. We can easily conclude that cyberterrorism represents a huge concern for the great majority of those countries.

9.1 PORTUGAL

- National Strategy on the Security of Cyberspace – RCM nº 36/2015, 12 June.
- National Strategy on the Fight against Terrorism – RCM nº 7-A/2015, 20 February.
- Law on the fight against money laundering and the financing of terrorism - Law nº25/2008, 5th June.
- Law No. 52/2003, 22nd August - Anti-Terrorism Act.
- Adoption of the Framework Decision 2002/475 / JHA of the Council on 13th June 2002 on action to combat terrorism, have linked the EU MS to adapt their national law in the manner specified therein by the 31 December 2002 (this gave birth, under the mechanism of transposition, to the Portuguese Law 52/2003, the Anti-Terrorist Act.

9.2 COUNCIL OF EUROPE

The Council of Europe publishes in its Internet Portal, (http://www.coe.int), under the topic Human Rights and Rule of Law, Action against Terrorism, a table with the legal framework of the Council of Europe member and observer states, and its legislative and institutional counter-terrorism capacity.

We had a look at the legal framework of each country, trying to find out how European States, namely the members of the Council of Europe, are worried about cyberterrorism phenomena and the legal instruments which are available to deal with it. As we can see below, most of the countries have already integrated the "cyber" context in their legal instruments for CT.

CODEXTER database (June 2015)

Countries	Cyberterrorism – the use of Internet for terrorist purposes (1)	Counter-terrorism capacity (2)
Andorra		
Albania		📄
Armenia	📄	📄
Austria	📄	📄

Belgium	📄	📄
Bosnia and Herzegovina	📄	📄
Bulgaria		📄
Croatia	📄	📄
Cyprus	📄	📄
Czech Republic	📄	📄
Denmark	📄	📄
Estonia	📄	
Finland	📄	📄
France	📄	📄
Georgia	📄	📄
Germany	📄	📄
Greece		📄
Hungary	📄	📄
Iceland		📄
Ireland		📄
Italy		📄
Latvia	📄	📄
Lithuania	📄	📄
Liechtenstein		📄
Luxembourg	📄	📄
Malta		📄
Monaco		
Montenegro		📄
Republic of Moldova	📄	📄
Netherlands	📄	📄
Norway	📄	📄
Poland		📄
Portugal	📄	📄
Romania	📄	📄
Russian Federation	📄	📄
San Marino		
Serbia / Serbie		📄
Slovakia	📄	📄
Slovenia		📄
Spain	📄	📄
Sweden	📄	📄
Switzerland	📄	📄
“the former Yugoslav Republic of Macedonia” (FYROM)	📄	📄
Turkey	📄	📄
Ukraine		📄
United Kingdom	📄	📄
European Union		📄
Mexico	📄	

United States of America		
Canada		📄

Table 1 – CODEXTER Database

(1) http://www.coe.int/t/dlapil/codexter/country_profiles.asp, assessed on 11-06-2015
(2) http://www.coe.int/t/dlapil/codexter/cyberterrorism_db.asp, assessed on 11-06-2015

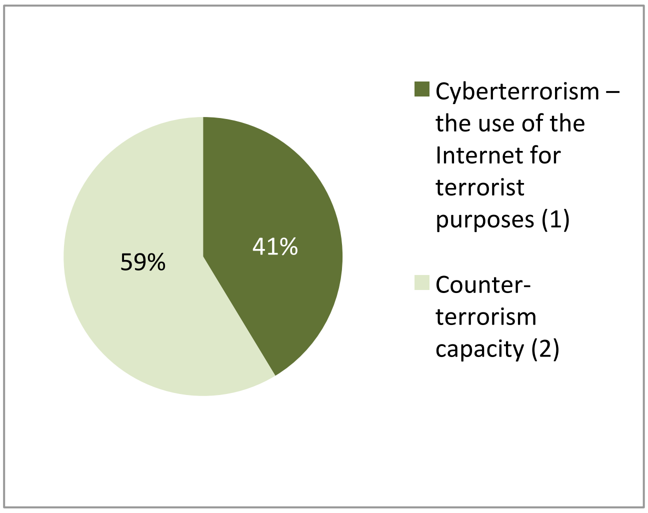


Figure 1 - CODEXTER database

9.3 *European context: Portugal and Greece in European fora on terrorism*

The EU has intensified the efforts to better understand the eco-system of cyberterrorism. There have been and there are several initiatives with this aim, either by financing projects on this issue or by reinforcing the mechanisms of cooperation among EU MS. Two end users of CyberRoad are LEA from Portugal and Greece, whose experience in participating in European initiatives may bring some knowledge and added-value on the European efforts to face the cyberterrorist threats.

9.3.1 Portugal – PJ Institutional participation in EU projects on Cyberterrorism

The globalization of the society based on the ICT has created changes in the criminals' *modus operandi*, and terrorists are not definitely an exception. Therefore, the concept of cyberterrorism has necessarily to be addressed by governmental institutions, amongst which the criminal investigative police agencies, such as PJ.

The possibility of using internet as a target or, most commonly, as means to perform a terrorist attack, or even as a vehicle to disseminate propaganda and violent *jihadist* content, has been in the last few years one of the major concerns placed in the CT agenda of the European and national institutions. Due to the rise of the international threat related to the *jihadist* Syrian-Iraqi insurgency and to the *ISIL-ISIS-IS* (whose notoriety worldwide owns much to the thoroughly dissemination of propaganda by the social networks), the EU felt the need to include the Internet and its misuse in the fight against terrorism and in particular foreign terrorist fighters (FTF).

Within this context, the Dutch Authorities promoted early in 2011 a European project, named "*Clean IT – CIT*", whose motto was "*Reducing the impact of the Terrorist Use of the Internet*". CIT counted with the participation of various EU MS amongst which was Portugal represented by PJ-UNCT.

CIT's project main action consisted on collecting best practices towards the reduction of internet use by terrorists. For attaining such goal, the project gathered in its working group, for the first time, governamental/official institutions and/or policy makers, competent for acting in case of detection of terrorist use of the internet, as well as private entities, – a reliable example of a potential public-private partnership in a critical domain - whose intervention was mainly to provide access to ICT technologies (mainly Internet Service Providers – ISP). The final result of this working group was a public document with the collection of best practices entitled "*Reducing the terrorist use of Internet*", formally presented by the EU CT Coordinator, Mr. Gilles de Kerchove (European Commission, 2013).

During 2013, also under the leadership of Dutch Authorities, a new project – a follow-up of the CIT – was started. This project originated a consortium named "*European Joint Initiative on Internet and Counter-Terrorism- EJI-ECT*", composed exclusively by governmental entities, policy makers and investigative police agencies, in which Portugal participated as an invited observer, also through PJ-UNCT.

The following year was marked by two working meetings gathering members and observers of the EJI-ICT. The main scope of this working group focused on the urgency in obtaining a best and broader cooperation from the private industry, namely from the industry with responsibility in ICT, ISP, social networks, video broadcasting platforms, etc. The common point consisted on reinforcing the EU with a common strategy and approach towards such private companies – most of them well-known multinationals with head offices sieged outside the European borders. It was stressed that the cooperation from the industry was crucial and even vital to countering and preventing terrorism and namely the FTF phenomena. Another common approach was considered with the cooperation of Europol, especially through the already existing and dedicated Europol products – such as the Focal Point *Check the Web* (CTW), an analytical working file dedicated to collect, store and analyse terrorist content, spread through the internet. This last proposal was addressed in the final document as an outcome of the meeting held this year by EJI-ICT (it took place on the 25th and 26th February 2015) but this time with a draft roadmap leading to its implementation.

The work resulting from these two projects, in which Portugal participated, was, so to say , the backstage of the decision taken by the Justice and Home Affairs (JHA) Council which took place on the 12 March 2015 previewing the creation of a EU Internet Referral Unit (EU IRU) to be established at Europol. The mandate of JHA Council of 12 March 2015 towards the implementation of an EU IRU was firstly prepared in previous JHA councils held at the beginning of 2015, in the aftermath of the two terrorist attacks held in European soil ("Charlie Hebdo" attack, in Paris, France, on 07 Jan 2015, and the Copenhagen, Denmark, terrorist attacks on the 14 and 15 February 2015).

On 12 March 2015, JHA concluded that one of the four priority areas of the "*Fight against terrorism*" consisted of the need of "*building upon Europol's CTW, Europol should develop an EU IRU by 1 July*

2015" (Europol, 2015). The core tasks of the EU-IRU, which will be assumed by Europol, will consist of:

- Coordinating and sharing the identification tasks (flagging) of terrorist and violent extremist online content with relevant partners;
- Carry out and support referrals quickly, efficiently and effectively, in close cooperation with the industry;
- Support competent authorities, by providing strategic and operational analysis;
- Act as a European Centre of Excellence for the above tasks.

The project towards the creation of the EU IRU is an ongoing task that has to be developed in close cooperation between the EU MS and Europol.

United Kingdom has already established its *Research, Information and Communications Unit (RICU)* within UK's Office for Security and Counter-Terrorism, which produces and deals with strategic information on terrorism. One of its tasks is to produce web contents that may overlap radicalism contents in web. This means a new narrative, aiming at developing actions and contents that may contribute to dismantle the arguments used by extremists.

Europol plays a critical role in sharing information and intelligence. Europol has a central role in the definition of a European strategy that should be followed by EU MS. Beyond that, Europol should provide for the development of mandatory actions, resulting from that strategy. This could be a way of changing the *status quo* of LEA, namely those who are slower in the adoption of organizational changes that can turn the organization more efficient in the fight against cyberterrorism.

As we can read in the document available online "*Terrorist use of Internet and social media has increased dramatically over recent years. Jihadist groups in particular have shown a sophisticated understanding of how social networks operate and have launched well organised social media campaigns to recruit followers, promote or glorify acts of terrorism and violent extremism. Recent studies have shown that within four months, more than 46.000 Twitter accounts were used by supporters of the Islamic State (ISIS) and as many as 90.000 tweets and other social media responses are produced every day. Some EU Member States (MS) have taken measures to reduce the abuse of the Internet by terrorists for propaganda purposes. They have created specialist police units to monitor the cyber environment, identify content suspected of having a violent extremist or terrorist nature and work closely with the industry to remove it on the basis that it breaches individual companies' user policies.*" (Europol, EU Internet Referral Unit at Europol - 7266/15, 2015).

9.3.2 GREECE – MINISTRY OF DEFENSE / CYBER DEFENSE DIRECTORATE WITHIN NATO AND EUROPEAN DEFENSE AGENCY.

In Greece, countering cyberterrorism is a part of the CT Unit, which belongs to the Ministry of Citizen Protection. It is a law enforcement unit with traditional tasks and operations in the field of terrorism and a recently created section dedicated to cyberterrorism. However, the Hellenic Ministry of Defence is also the National Security Authority. Therefore, since terrorism and cyberterrorism are constant threats to the national security, there is an indirect involvement on CT issues.

HMOD/NSA and CT Unit are cooperating at the strategic/political level through information exchange on threat intelligence. Similarly HMOD/Cyber Defence Directorate which is the military authority for cyber defence, is collaborating with the cyberterrorism section at the operational and technical level, according to operations requirements and level of confidentiality.

Cyber Defence Directorate (CDD) has an extensive background and expertise for more than 10 years. It participates in NATO's and EU's relevant technical projects and exercises, improving the technical skills and collaboration with other authorities at public, private and academic sector.

Since 2009, CDD is participating in largest NATO Cyber Defence exercise Cyber Coalition, which aims to enhance collaboration between member nations and partners, in order to achieve an efficient response and defence from cyber threats including terrorist attacks. The main effort is to manage the cyber crisis after a large scale attack, improve information exchange at every level (strategic, operational and tactical) and develop better technical capabilities for cyber defence.

This year, Greece became also a full member (sponsor nation) at NATO's Cooperative Cyber Defence Center of Excelence in Estonia, which is a dedicated research and capabilities development center providing training, knowledge and expertise to the MS with the same goal; improve cyber defence capabilities. Additionally, there is a legal section with several projects and reports published, addressing cyber legislation issues at national and international level, including cyber terrorism topics.

At the European level, CCD participates in European Defence Agency's Project Team for Cyber Defence, which is responsible for addressing cyber defence aspects, especially after the selection of cyber defence as one of the top 10 priorities for the EU. Several projects have been supervised and reviewed by the EDA's project team, aiming at improving cyber defence capabilities for MS. Recently it was decided that defence, civil, academia and private sector should cooperate further and deeper in order to combine efforts towards the fight of cyber threats. One of the EDA projects that delivered important knowledge benefitial for cyber terrorism activities is the study "*Cyber Threat Intelligence*" (Roehrig, 2013), where extensive analysis on threat actors, sources of information, assessment methodologies and processing are being described in detail.

9.3.3 Some contributions to enhance knowledge on Cyberterrorism

9.3.3.1 The Use of the Internet for Terrorist Purposes, Report from the United Nations, 2012, (PUBLIC)

The United Nations Office on Drugs and Crime (UNODC) plays a key role in providing assistance to Member States, in furtherance of its mandate to strengthen the capacity of national criminal justice systems to implement the provisions of the international legal instruments against terrorism, and does so in compliance with the principles of rule of law and international human rights standards (United Nations, 2012).

This document provides an overview of the means by which the Internet is often utilized to promote and support acts of terrorism, in particular with respect to the purposes of propaganda, training and financing, planning and executing such acts. The opportunities offered by the internet to prevent, detect and deter acts of terrorism.

9.3.3.2 *Study on Methodologies or Adapted Technological Tools to efficiently detect violent radical content on the Internet, from the European Commission, 2012, CONFIDENTIAL UE (paper).*

This study was commissioned by the European Commission in order to make it easier for law enforcement authorities to counter the use of the internet by terrorists. The study focuses on applications currently being used in the EU for detecting online violent radical content.

According to the final report of this study, which compiled an overview of technologies and tools applied by LEA of the EU MS and of the gaps and requirements identified, the main conclusions and recommendations were:

- LEA of EU MS have a relatively low level of expertise in applying technologies and tools and need effective tools to detect online violent radical content;

- LEA of EU MS generally has limited access to appropriate resources on Islamist extremism and terrorism trends and developments. A centralized database on Islamist and terrorism should be developed in order to facilitate and enhance the level of open source intelligence for LEA of EU MS.

9.3.3.3 *Cyberterrorism: A Survey of researchers, The Cyberterrorism Project by Swansea University (UK), March 2013, (PUBLIC).*

This report provides an overview of findings from a project designed to capture current understandings of cyber terrorism coming within the research community. The project ran between June and November 2012, and employed a questionnaire which was distributed to over 600 researchers, authors and other experts, working in 24 countries across six continents. The Cyberterrorism Project was established at Swansea University, UK, in 2011, by academics working in the School of Law, College of Engineering, and Department of Political and Cultural Studies. The project has the following objectives:

(1) To further understanding amongst the scientific community by engaging in original research on the concept, threat and possible responses to cyber terrorism;
(2) To facilitate global networking activities around this research theme;
(3) To engage with policymakers, opinion formers, citizens and other stakeholders at all stages of the research process, from data collection to dissemination;
(4) To do the above within a multidisciplinary and pluralist context that draws on expertise from physical and social sciences.

"Security practice does not require definition of threat. It is performative - it constructs its own threats and its reasons for being. Cyberterrorism, or 'terrorism', performs an oppositional construct that doesn't require specific definition." (Swansea University, 2013, p.20).

This was one of the additional comments provided by one of the respondents. However, the definition and conceptual clarity as well as greater understanding of the cyber terrorist threat was the most common answer concerning the most pressing issues in the field of cyber terrorism. Most of the respondents consider cyber terrorism a significant threat, identifying as the threat´s referent (focus´ threat): Government/State, Critical infrastructure/computer networks, civilians/individuals, organizations/ private sector/corporations/economy, society (everyone).

9.3.3.4 *Cyber Security Countermeasures to Combat Cyber Terrorism, Strategic Intelligence Management, National Security Imperatives and information and Communications Technologies (Ahkgar & Yates, 2013)*

This book is a collection of works from leading practitioners and academics concerned in the field of national security intelligence management. It introduces both academic researchers and law enforcement professionals to contemporary issues of national security and information management and analysis. It explores the technological and social aspects of managing information for contemporary national security imperatives.

The first part of the article focuses on the difference between cybercrime and cyberterrorism. Most contemporary definitions of cyberterrorism focus on the following three aspects:

- Motivation of the perpetrator(s),
- Targeted cyber system and
- Impact on a certain identified population.

The key issue in cyberterrorism is the motivation to carry out an activity in cyberspace resulting in violence/harm or damage to individuals and/or their property. If considered in these terms, it becomes clear that a number of existing activities in cyberspace, which result in harm to individuals and/or their property, might be constituted as cyberterrorism simply on the basis of establishing the motivation for the activity. This leads us into a current debate as to whether cyber terrorism actually exists or is simply another expression of existing malicious and criminal activity in cyberspace.

A number of commentators have sought to make the argument that there is neither evidence nor rationale to argue that cyberterrorism exists independent of existing cyber activities (ACM, Conway, 2011). However, we would support the view put forward by a number of other authors in a way that there is sufficient evidence, highlighted in particular by events such as Stuxnet and others described later in this chapter, to justify a consideration of cyberterrorism as a separate entity within this space (Greengard, 2010).

The main difference between cybercrime and cyberterrorism lies in the objective and motivation of the attack. Cybercriminals are predominantly out to make money, while cyberterrorists may have a range of motives, notably of political ideological, religious or ethnic nature and will often seek to have a destructive impact, particularly on critical infrastructure. Cyberterrorists also want to have maximum impact with the greatest stealth. Greengard (2010) identified a range of cyber attack methods that can be deployed by cyberterrorists, including "*vandalism, spreading propaganda, gathering classified data, using distributed denial-of-service attacks to shut down systems, destroying equipment, attacking critical infrastructures, and planting malicious software*."

9.3.3.5 Terrorists´use of the Internet, A Symposium (Final report), The Cyberterrorism Project by Swansea University (UK), June 2014, (PUBLIC).

This report contains findings from the Cyberterrorism Project Symposium on terrorists' use of the Internet. The event was hosted by Swansea University, UK, on 5-6 June 2014. 43 delegates attended the symposium, including researchers from a number of UK universities, as well as institutions from Republic of Ireland, France, the Netherlands, Norway, Turkey, Canada and Australia. Other attendees included representatives from the Home Office, South Wales Police and the Scottish Organized Crime and Counterterrorism Police Unit.

This symposium brought together a range of experts from different disciplines (across the physical and social sciences) and different jurisdictions (from across Europe, Canada and Australia) in order to explore different forms of online terrorist activity, evaluate legislative and policy responses to terrorists 'online activities in terms of their impact on democracy, liberty and the rule of law and explore the opportunities that the Internet provides for intelligence and LEA, not only for surveillance and intelligence purposes but also to the construction and promotion of counter narratives and other strategic communications.

Terrorist organizations have already expressed an interest in developing offensive cyber capabilities. The potential for malware to be used strategically as a weapon was illustrated by Stuxnet. Whilst a very high level of sophistication and resources were needed to develop Stuxnet, malware for sabotage may be expected to become more prevalent and mainstream in the next five to ten years as the required knowledge and skills to prepare such an attack become more widespread.

Whilst terrorists launching a cyber attack potentially poses a future threat, they already use the Internet for a range of other activities. These include: planning, communication, propaganda, indoctrination, radicalization, recruitment, training and fundraising.

Numerous areas were identified where understanding is currently lacking and further research is required. These included: gaining a better understanding of the terrorists themselves, the materials they place online and their cyber capabilities; gaining a better understanding of the consumers of extremist online content; developing a more dynamic understanding of the relationship between the Internet and the offline world; analyzing the effectiveness of CT laws and policies, including accountability mechanisms, and how to assess effectiveness; gaining a deeper understanding of how CT policies are produced and how cooperation can be engendered between the private and public sectors and within the international community.

Many online terrorist activities transcend national boundaries. Terrorist publicity, propaganda and radicalization campaigns all have a global reach. Terrorist financing is also increasingly transnational in nature. As a result, CT also needs to be transnational. International law has a significant role to play, and international cooperation is essential. At the same time, however, it is important to recognize that many terrorist groups have a specific geographical focus, as the tweets during the Westgate attack illustrated.

10 Stakeholders' threats and needs

10.1 Threats

The decisive technological developments in the reconfiguration of the current paradigm of globalization, coupled with the revolution in information, technology and telecommunications, providing a significant change in the organization of countries, from economics, culture to social and behavioral practices, largely positive changes, but yet, if we put together internet to that equation (computer + telecommunications), we have a result that leaves many questions, in particular regarding security issue. The technological devices that had more impact on people and organizations, changing the usual communicational channel, have been mobile devices, namely, computers, phones and more recently tablets.

10.1.1 Internet and Mobile devices

"*We are not in the age of Information. We are not in the age of the Internet. We are in the Age of Connection. Being connected is at the heart of our democracy and our economy. The more and better those connections, the stronger are our government, businesses, science, culture, and education.*" (Weinberger, 2008). According to this author, connection is the substance of daily lifestyle of society today, closely tied to new technologies, particularly those which facilitate the contact and communication between people and organizations wherever they are. Those are the case of portable computers, tablets and mobile phones, which through the Internet make that connection possible. "*According to a survey by INOV-INESC, the use of mobile phones to access the internet and social networks among young people has doubled in the last three years. The tablet is among the most used devices at home.*" (Godinho, 2014). *The cellphone becomes a "televerything", a device that is both phone, camera, television, cinema, news information receiver, emails diffuser and SMS, WAP, sites updater (moblogs) GPS locator, music player (MP3 and other formats), electronic wallet ... now we can talk, watch TV, pay bills, interact with others through SMS, take pictures, listen to music, pay for parking, buy tickets to the cinema, walk into a party and to organize political and / or hedonistic demonstrations (the case of smart and flash mobs)* (Lemos, 2015). "*Today, the explosion of mobile devices, mainly smart phones, together with Web 2.0 applications and the pervasiveness of public access or hacked-into wireless networks together with broadband access have resulted in a significant expansion of the threat" (*Winters, 2013).

The most relevant vulnerabilities in this sector of technology, since it allows users and criminals, who are in "mobility mode", to communicate, to access and to transfer data through cybespace, are software and human practices.

"Besides compromising the security and privacy of our digital interactions, software vulnerabilities can put at risk other parts of our daily activities, or even our lives" (SysSec, 2013). The most usual forms of software vulnerabilities are:

- Mobile malware, worms and viruses: infecting the software with the purpose to steal sensitive information, thus threatening privacy;

- Unsecured or unlicensed applications: "*Unlicensed apps can cost a company a lot of money in legal costs. There are even websites that offer rewards to employees who turn in their employers for running unlicensed software*" (Olsen, 2010);
- Network access: *Unauthorized network access means either an external intruder accessed a computer on your network or an employee accessed data that he or she should not have* (Olsen, 2010);
- Eavesdropping a hacking technique through the breach of confidentiality - unauthorized messages reading and/or listening.

Concerning human practices, if we consider that these mobile devices have physical characteristics of small size and are portable, this means they can be easily lost and stolen allowing intruders to access remotely to a server, for instance, logging and stealing whatever they want. *We've all seen the news reports about laptops being lost or stolen -- along with names, Social Security numbers and financial data. Several sources claim that 12,000 laptops are lost at major airports each week: Simple math extends that to more than 600,000 laptops per year. One report says that, of that number, only 30% the machines are recovered by the owner, and half of the owners say their laptops contain sensitive customer data or business information. And now that PDAs and smartphones can store more data, the problem will only get worse* (Olsen, 2010).

10.1.2 SOCIAL NETWORKS

"*The right to freedom of opinion and expression is as much a fundamental right on its own accord as it is an "enabler" of other rights, including economic, social and cultural rights, such as the right to education and the right to take part in cultural life and to enjoy the benefits of scientific progress and its applications, as well as civil and political rights, such as the rights to freedom of association and assembly. Thus, by acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the Internet also facilitates the realization of a range of other human rights*." (Rue, 2011). The Human Rights Council Resolution 7/36 underscore the right to access Internet has two dimensions: access to online contents, without any restrictions except in a few limited cases permitted under international human rights law; and the availability of the necessary infrastructure and information communication technologies, such as cables, modems, computers and software, to access the internet in the first place (Rue, 2011).

According to this, the right of all individuals to seek, receive and import information and ideas of all kinds through the Internet, namely through social networks, store, make available, in quantity and diversity information and personal data related to their businesses, activities, and their personal lives; even businesses also came with a more active and intensive role and interaction with consumers in the last couple of years; it raises the question: how to identify ordinary citizens, who are making use of their right of free access and expression on Internet from those with illegal objectives, notably those using internet and social networks to cyberterrorist purposes? How to protect these human rights without giving up on individual freedom?

According to Gordon Snow, assistant director of the Cyber Division of US Federal Bureau of Investigation (FBI) social networks facilitate cyberterrorism by allowing it to become less constrained geographically and broaden the audience to their criminal actions; expects an increase of cyberterrorism as the number of connected devices exceeds the number of people worldwide. "*Terrorists are not only sharing ideas, they are asking for information, and to improve methods of communication. Ever safer*." says Ralph Boelter, Deputy Director of the CT Division. And are still radicalizing Americans and creating extremists in America (Kasperkevic, 2012); Scammers are using the recent devastation in Nepal to demand for donations. FBI reminds the public to apply a critical eye and conduct due diligence before giving to anyone soliciting donations on behalf of disaster victims. Requests can originate e-mails, websites, door-to-door collections, phone calls and similar methods (Foxworth, 2015).

As mentioned previously, terrorists are using internet for their activities of propaganda, financing, communication, recruitment, plotting, indoctrination, radicalization, logistics, planning, training, material dissemination, etc; the most commonly used tool of social engineering on the web to perform these tasks are the social networks, such as the Facebook, blogs and social media. According to the US Secretary of Homeland Security, Jeh Johnson, in an interview with ABC television network, the minister said that it is a new situation due to the "(...) *use of social networks and the internet by IS and thus can reach people in the territory" of the United States, as "lone wolves*" (Correio da Manhã, 2015).

10.1.3 CRITICAL INFRASTRUCTURES

Critical Infrastructures (hereafter CI) are comprised of a set of complex systems, in other words, CI is a system of systems targeted to deliver essential services and products for citizens. According to the European Council Directive 2008/114/EC *"Critical infrastructure (CI) means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions* (Lazari, 2014)

This directive establishes sectors and subsectors for the CI at European level:

Sector	Subsector
I Energy	1. Electricity: Infrastructures and facilities for generation and transmission of energy in respect of electricity supply.
	2. Oil: production, refining, treatment, storage and transmission by pipelines
	3. Gas: production, refining, treatment, storage and transmission by pipelines, LNG terminals

II Transport	4. Road transport
	5. Rail transport
	6. Air transport
	7. Inland waterways transport
	8. Ocean and short-sea shipping and ports

Table 2 – Sectors and subsector in CI according to Annex I (EU2008)

Reviewing the papers, reports, etc. on *Threat Landscape in Critical Infrastructure*, one of the most relevant sources is found in ENISA (2013).

Although the scope of the report is for Smart Grids, the threat classification is totally applicable for CI in general. Below, the threats will be explained in detail to outline the threats landscape in CI protection:

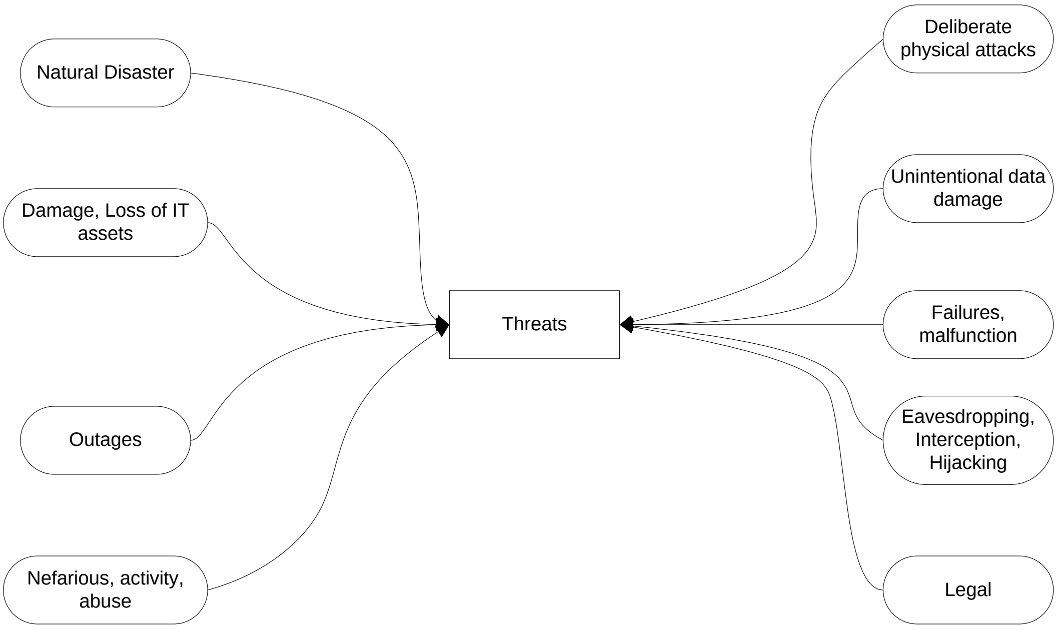
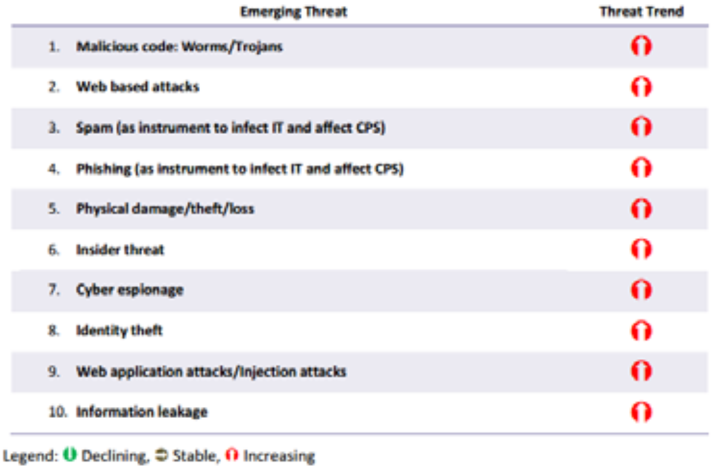

Natural Disaster
Damage, Loss of IT assets
Outages
Nefarious, activity, abuse
Threats
Deliberate physical attacks
Unintentional data damage
Failures, malfunction
Eavesdropping, Interception, Hijacking
Legal

Figure 2 - Threat Landscape for Smart Grids according to (ENISA, 2013)

- Threat Group: Loss/Damage
  - Threat: Loss of devices, media and documents
  - Threat: Information Leakage
- Threat Group: Eavesdropping, Interception, Hijacking
  - Threat: Interfering radiation
  - Threat: Man in the middle, session hijacking
  - Threat: Interception of information
  - Threat: Network reconnaissance and information gathering
  - Threat: Replay of messages
- Threat Group: Failures/Malfunction
  - Threat: Failure of devices and systems
  - Threat: Failure or disruption of communication links (communication networks)
- Threat Group: Nefarious Activity/Abuse
  - Threat: Unsolicited e-mail
  - Threat: Denial of Service attacks
  - Threat: Manipulation of hard- and software
  - Threat: Malicious code /Activity
  - Threat: Unauthorized access to information system / network
  - Threat: Manipulation of information
  - Threat: Misuse of information/Information Systems
- Threat Group: Physical attack
  - Threat: Fraud

The previous list of threats are not prioritized. However, ENISA (2014) delivered one technical report with the top ten emerging threats in Cyber Physical Systems with their associated trends:



Emerging Threat	Threat Trend
1. Malicious code: Worms/Trojans	↑
2. Web based attacks	↑
3. Spam (as instrument to infect IT and affect CPS)	↑
4. Phishing (as instrument to infect IT and affect CPS)	↑
5. Physical damage/theft/loss	↑
6. Insider threat	↑
7. Cyber espionage	↑
8. Identity theft	↑
9. Web application attacks/Injection attacks	↑
10. Information leakage	↑

Legend: ↓ Declining, ⇄ Stable, ↑ Increasing

Table 3 – Emerging threats and their trends in the area of cyber physical systems (ENISA, 2014)

10.2 *NEEDS*

10.2.1 INTERNET AND MOBILE DEVICES

According to the literature, the most critical sources of vulnerabilities are software and human practices.

It is difficult to separate internet and mobile devices from social networks when we analyse the needs of the stakeholders. Therefore we have decided to address both items globally, as they require a compreehensive approaches. The measures required dealing with the threats coming from internet, mobile devices and social networks are globally the same.

It would be necessary to allow for the easy access to OSINT (open sources) over cyber intelligence methods and mechanisms, creating an effective and actionable intelligence for LEA, not only under the criminal investigation approach but also under a criminal prevention approach/perspective. Most of *modus operandi*, nowadays applied in cyber terrorism, context and/or in terrorism-related content over **i**nternet, come from native **c**ybercrime behaviours and can be supported by **c**ybercrime actors with very high hacking skills. Therefore and considering this scenario**,** LEA must be technically well equipped, namely with a cyber intelligence solution (cyberterrorism oriented), able to prevent and investigate crime over the internet, with very specific features as follows:

- Multi-language;
- Ontology (Terrorism-oriented);
- Real-Time and auto-translation (*e.g.* Arabic varieties, Russian, Hebrew, Chinese, etc**)**, also terrorism recruitment channels oriented;
- Crawl, collect (*e.g.* thinking of scenarios that are needed to preserve digital contents before taking down the online terrorist-content web source), index, correlate, analy**s**e, report and predict next criminal acts, in open sources and social media networks which must be agnostic to http/https protocols and applications, meaning that it must also be able to run it against IRC channels, **ga**mming chats, etc], all these operations must run in an anonymous way (access)**.**
- The same requirements above, but also being able to run those tasks in a Darknet, like TOR and I2P networks;
- Avatar and emulation features, available for the solution operators - analysts and investigators;
- Geolocation (geotag) features, especially on most common social networks;
- Notification and alert features, based on specific terms, like keywords or hashtags formats criteria;
- Must have mobility features and operative system independent, meaning that it could be accessed by operators - analysts and investigators - from a mobile device like smartphones or tablets, over secure access (VPN);

- Virtual currencies (example: Bitcoin), intelligence features, based on stats, transactions and blocks;

- Static Image (Picture - like graphic files, stored on internet] search based on different criteria (e.g. filename, hash value, etc), identification (*e.g.* face recognition), analysis and comparison features;

- Dinamic Image (Video - like movie files, stored on internet) search based on different criterias (*e.g.* filename, hash value, etc), identification (*e.g.* face recognition), analysis and comparison features;

- Audio (like sound files, stored on internet) search based on different criteria~~s~~ (*e.g.* filename, hash value, etc), identification (*e.g.* voice recognition), analysis and comparison features.

A cyberterrorism oriented **c**yber intelligence solution must be complemented with a local (field) **w**ireless actionable intelligence solution (device), able to collect information near the target and submit it in real time and from any place (location) to a unified platform (command and control center), working at the backoffice.

It must have the flexibility to complement with an internal development (R&D), interacting with most common API~~s~~, released by the social network providers.

10.2.2 SOCIAL NETWORKS

From the point of view of the stakeholders that have the mission to prevent and fight against cyber offences, one of the measures to be taken could be the mandatory provision of LEA with free (unpaid) access to information stored in social network databases. This could be achieved through specific free API that would be given by the owner of the social network (Google, Facebook, Instagram,..).

Please see point 10.2.1 above, which applies to social networks as well.

10.2.3 CRITICAL INFRASTRUCTURES

Every citizen relies on public utilities such as energy, natural gas and water supplies and distribution to carry out daily activities. Electric blackouts, disruption of oil, gas or water supply, interruption of transportation (trains, metro, and traffic control) can cause consistent problems to governments and citizens. Unfortunately, these utilities are extremely vulnerable to cyber-attacks, hence they are within easy reach of cyber attackers and cyber terrorists. Clearly, there is a direct connection between utilities vulnerabilities to cyber-attacks and the society vulnerability to cyberterrorism. Cyber-terrorist, indeed, may target one of these vital infrastructures to hit governments or citizens. Concerns about an attack against national utilities are high. According to Kaspersky (2012) "*each country needs to make a very serious audit of the critical infrastructure within its borders*". In addition, he pointed at the power network as the most critical of all (nothing can work without power) followed by telecommunications, financial services and transportation[5].

Nowadays, utility companies need to reduce the cost of running their core operations. This objective is achieved primarily by increasing industrial process automation, thus minimizing the human impact on those costs. The widespread use of automation systems and the establishment of new interconnections that were simply not there in the past, have exposed implications concerning the availability of the assets. This in turn impacts the security and safety of the processes. Software and component vendors have introduced an additional worsening factor for security. They have begun to include in their products COTS (Commercial Off The Shelf) in order to improve interoperability among utility networks and lower their development costs. As a result, critical systems now run on common software platforms (such as Windows) for which vulnerabilities are regularly discovered. Attackers can leverage those vulnerabilities to gain access to critical systems and alter critical operations.

Facing the emerging problem of the large diffusion of advanced threats targeting objectives to disrupt critical services such as those provided by utility companies represent an urgent need that has to be addressed. Because of the impact that a disruption of the utility services would have on citizens, they have been classified as CI. Protecting utilities from advanced threats is thus crucial and has been constantly ranked high in Governments security policies across Europe. Among the different advanced threats that could hit CI, advanced cyber threats are continually gaining significant coverage in media and news headlines. After the discovery of Stuxnet in 2010, other cyber threats have been found in critical systems (Duqu, Flame, Shamoon), and the security community quickly turn its attention towards assessing their robustness. Several researchers have shown that the security of those systems has been neglected and that a motivated attacker could easily penetrate and take control[6]. Twenty times more software flaws have been discovered in industrial control systems since Stuxnet[7].

Urgent needs for CI are represented by the provision of innovative solutions for enhancing existing procedures and methods and conceiving tools to prevent cyber-attacks that target utility companies, which rely heavily on industrial networks and automated control systems.

In particular, it should be addressed the prevention of cyber-attacks against hardware and software systems such as DCS, SCADA, PLC, networked electronic sensing, and monitoring and diagnostic systems which are used to support critical services of utility networks. Network monitoring and situational awareness are key to preventing and promptly responding to cyber-attacks. Research shows that attacks are often carried out in stealth mode and only after days of months they actually infringe the damage. In addition, even the most advanced threats need to do "*reconnaissance*": analyse the target to identify possible weaknesses. By being able to detect the "*stealth infiltration*" and thanks to the "*reconnaissance*" it would be possible to empower CI stakeholders to respond adequately to cyber-threats, thereby protecting society from being disrupted. In addition, by

[5] http://www.cnbc.com/id/102367777

[6] http://www.digitalbond.com/tools/basecamp

[7] http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240049917/scadasecurity-in-a-post-stuxnet-world.html

providing an easy-to-adopt system, more CI organizations would deploy it hereby significantly increasing the safety and security of European citizens.

Some years ago, the majority of efforts to protect Cyber Physical Systems were targeted to increase reliability (the protection of the system against random faults) (Bouwmans, 2006). Nonetheless, in recent years some other concerns have become paramount for CI. The review of related literature has come up the needs: Prevention, detection and recovery, resilience and deterrence, as follows:

10.2.3.1 *Prevention*

The major need for prevention the compromise of CI systems is to discover ways in which responsible and vendors of ICS will be encouraged to follow best security guidelines.

The National Institute of Standards and Tecnology (NIST) led one of the most modern guidelines for security best practices in CI (NIST, 2014)-. The NIST Framework for Improving Critical Infrastructure cyber security defines five "functions", among them, the identification and protection. The NIST (2014) framework highlights two pillars in the preventative field:

1) "Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities";
2) "Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services".

The ENISA National Cyber Security Strategies advices to follow a national risk assessment approach. Although this guideline establishes a repetitive approach in a traditional risk assessment strategy for the prevention of cyber attacks instead of a continuous process (ENISA, 2012).

Although many efforts in developing standards focused on prevention have been proposed the International Society of Automation (ISA)stated last year that "*Industrial cybersecurity expert warns that not enough is being done to prevent risk of highly destructive cyberattack on critical infrastructure*" (ISA, 2014).

10.2.3.2 *Detection and recovery*

Because the prevention activity can never discard successful cyber attacks, the detection and recovery processes should always put in place, among others, monitoring, intrusion, detection, and anomaly detection tools.

From academia (Pasqualetti, 2013) proposed mathematical framework for Cyber Physical Systems focused on monitoring and detection, they characterized the monitoring limitation from graph-theoretic perspective and designed centralized and distributed attack detection and identification monitors. Finally, they carried out proof of concepts through some examples.

10.2.3.3 Resilience

One of the paramount needs in CI already identified in (Krotofil, 2013) was the resilience concept. Trivedi *et al.* (Trivedi, 2009) analysed some definitions of the term *Resilience*, (Laprie, 2005)_and (Simoncini, 2008) defined resilience *as the persistence of service delivery that can justifiably be trusted, when facing changes* (Huchison), defined it as "*the combination of trustworthiness (dependability, security, performability) and tolerance (survivability, disruption tolerance, and traffic tolerance)*".

The topic of **r**esilience in CI is a trend and thus last November 2014 was proclaimed the month of Critical Infrastructure Security and Resilience by the President of United States (Obama, 2014).

10.2.3.4 Deterrence

(Taquechel, 2012) advocated for a contextual definition of Deterrence in CI field, they defined as *influencing an adversary's decision making process such that their expected utility from attacking a CI changes after we deter by investing*. Cardenas *et al.* (2009) warned on the importance of deterrence in legislation, law enforcement and international collaboration and highlighted the challenge to identify new deterrence mechanism for the security of Cyber Physical Systems (Cardenas, 2009).

10.3 ASSESSING STAKEHOLDERS' THREATS AND NEEDS: THE QUESTIONNAIRE

There is a vast range of literature about cyberterrorism, about the threats and needs, as well as about best practices on the way to deal with this phenomenon. However, we considered that an updated insight on this issue could represent an added value for deliverable 6.1. The information provided for by the stakeholders that answered to the questionnaire would allow to map with the analysed literature and identify the gaps.

Therefore, a questionnaire was prepared, taking into account primarily the experience of operational staff – criminal investigators working on the prevention and investigation of terrorism, either on the traditional *modus operandi* or cyberterrorism.

As already said in the "Methodology", this questionnaire was personally introduced and explained to the list of stakeholders agreed by the partners. Beyond Universities, SME, ISP and CI, the questionnaire was presented to some 70 LEA in several EU MS: Austria, Belgium, Bulgaria, Cyprus, Croatia, Denmark, Slovakia, Spain, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, United Kingdom, Czech Republic, Romania and Sweden.

10.3.1 THE PURPOSE

The purpose of the CyberROAD questionnaire 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.

Perceived threats may be different from the real ones. Therefore, it is important the attempt to correlate stakeholders' experiences and thoughts about cyberterrorism with the situations reflected in the analysed reports and documents.

10.3.2 TARGET GROUPS

The questionnaire was presented to some 90 entities, chosen among the entities with which PJ has organizational relationship and based on the respective role in this eco-system:

- LEA
- Justice Infrastructures
- Universities
- Health service providers
- Rail infrastructures
- Roadtransport companies
- ISP
- CERT
- SME and Large Enterprises

The CyberRoad WP6 partners were also invited to give their contribution, either by answering the questionnaire or by further disseminating it.

10.3.3 THE QUESTIONNAIRE

The questionnaire was structured around five chapters:

- The concept of cyberterrorism
- The Legal system
- Guidelines
- Best Practices
- Plan of Incident Response

Some of the questions were open ones, enabling the respondents to give some more elaborated information on the proposed topics. The negative side of this may have been some difficulties in answering the questionnaire by some stakeholders. We were aware of this risk, but have decided to face it instead, as we wanted more than multiple choice answers. The results led us to conclude that it was worthy taking the concerned risk.

It is important to stress that the respondent could choose not to identify the organization. So, when the identification is explicit, this does not mean a breach of confidentiality.

A quantitative and qualitative analysis was carried out and the results will be presented in point 10.3.4.

The invitation to answer the questionnaire is attached to this document as ANNEX I: PRESENTATION OF THE QUESTIONNAIRE.

10.3.4 Analysis of results

From the 90 entities involved, 56 questionnaires were partially answered and 34 fully answered. The following is a short overview of the questions and answers received. The details are available in ANNEX III: QUESTIONNAIRE ANSWERS.

10.3.4.1 Organization type

Responses were received from Government, Legal and LEA, Military and Defense, Universities, Energy, Transportation, R&D organizations and others not specified.

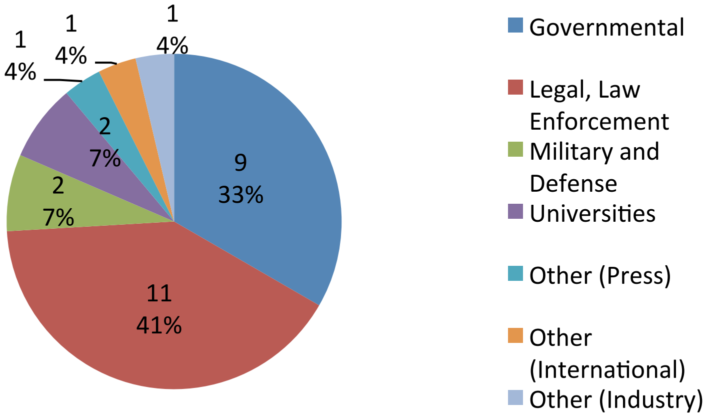


Figure 3 - Organizational Respondents Types

About the concept of cyberterrorism, a tripartite concept was provided, as also explained in point 8.3, pag. 17, and it was asked if they could agree with it or not. If not, the respondent was asked to give or suggest a definition (open question):

Results: 70% (37 answers) agree with the definitions proposed and provided. No alternative definition was suggested.

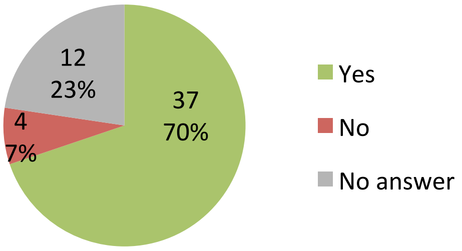


Figure 4 - Cyberterrorism definition

From the **4** respondents who disagree with the definition, only **2** justified their answers and gave inputs for broader definitions.

- The definition of cyberterrorist acts should include a reference to ethnic motivations; the definition of cyberattacks is not adequately developed; Suggesting the following sentence "*…disturbing the regular functionality of public organizations, services and infrastructures…*"
- First definition: I would change the concept of "Cyberterrorist acts" for the concept of "Cyberterrorist Threat".

10.3.4.2 Legal system

In these questions, the respondents were asked to tell how their national legal system pursues the issue of cyberterrorism, as well as the challenges, constraints and/or trade-offs:

> How does your legal system pursue cyberterrorism?

Results: Answers were received from Portugal, Belgium, Spain, Italy, Greece, Hungary and United Kingdom. All these countries have legal basis on cyberterrorism. Only the United Kingdom is in the process of reviewing the existing legislation.

> What are the challenges, constraints or trade-offs (e.g. privacy aspects, legal framework) you consider pursuing the problem of cyberterrorism?

Results: Answers were received from Portugal, Belgium, Spain, Italy, Greece and United Kingdom. The main issues were:

- Competences of police forces;
- Timely national and European cooperation;
- Poor level of public awareness;
- Lack of specialized staff;
- Lack of specialized units, technologically well equipped and with highly qualified and specialized staff;

- Difficulty to follow the innovation capacity of terrorists;
- Creation of legal instruments is slow;
- Legal framework is not agile enough;
- Privacy aspects;
- Human and IT Resources.

10.3.4.3 Guidelines

To the questions "Does your organization provide a guideline of best practices (program, policies, and procedures) on how to deal with information related to security threats? If yes which one?"

Results: 8 respondents answered that they have Guidelines and Best Practices.

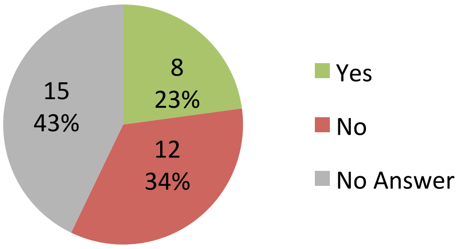


Figure 5 - Guidelines/Best Practices SecurityThreat

8 of these answers were affirmative (yes as a reply) only 7 enumerated theirs organization's procedures which are:

- the availability of tools in the field of security policies, including ISO 27001;
- Behavioral rules and awareness measures;
- Computer system hardening, safe browsing, emails handling.

To the questions "Does your organization provide a guideline of best practices (program, policies, and procedures) on how to specifically approach the threat posed by cyberterrorism? If yes which one?"

Results: 3 respondents answered that they have Guidelines and Best Practices.

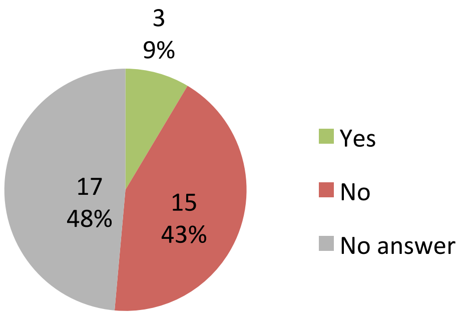


Figure 6 - Guidelines/Best Practices Cyberterrorism

3 of these answers were affirmative but only 2 enumerated their organization's procedures which are:

- Data loss prevention but ending security policies;
- Technical aspects include: anomaly detection, pattern analysis, malware analysis, blacklists, cloud security, data loss prevention; Non-technical aspects include: ISO 2007 certification, policies, awareness measures an others.

10.3.4.4 Best practices

In this topic it was specifically requested to identify the 3 best practices to counter cyberterrorism. Answers were received from Portugal, Spain, Italy and Greece.

Results: The answers focused on:

- (International) Cooperation;
- Coordination among security forces;
- Exchange of information;
- Risk management;
- Enhancement of law enforcement capabilities;
- Situational awareness;
- Software security;
- Training;
- Cyber intelligence;
- Cyber defense.

To the question "Do you consider that there is a need to increase the current sharing of best practices among teams working to counter cyberterrorism?"

Results: the majority answered affirmatively.

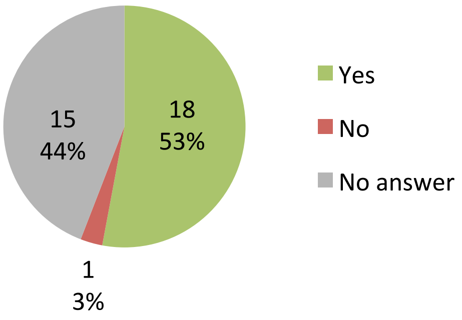


Figure 7 - Need to Increase Sharing Best-Practices

10.3.4.5 Plan Incident Response

To the question: “Does your organization provide a Plan of Incident Response?

Result: Only **18%** (6) of respondents answered positively (yes).

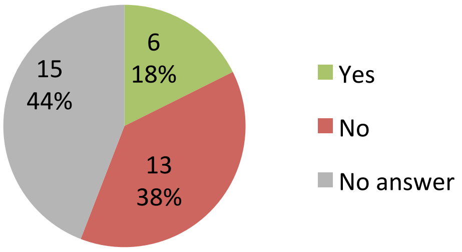


Figure 8 - Plan Incident Response

10.3.4.6 Domains of cybersecurity

To the question: In your opinion, in which domains cybersecurity should be more focused in order to fight cyberterrorism?

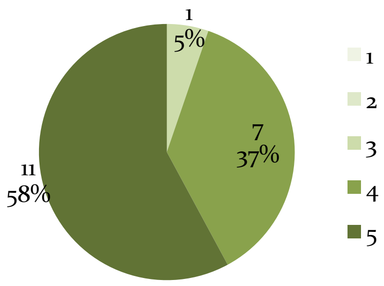
Respondents were requested to rank the following domains which are more relevant (1 for less likely to 5 for the most likely):

- Education/Awareness
- IT & Security Solutions
- Ethical domains research
- Political/Social interventions

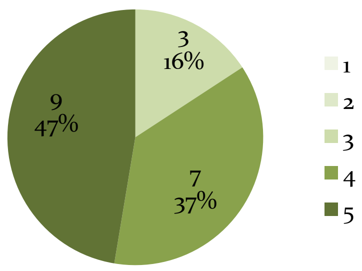
- Critical infrastructures protection/prevention
- System protection of servers/PC
- Forensic activities enhancement
- Theoretical (cryptography, algorithms)

Results: In general terms the domains most valued to fight cyberterrorism were Education/Awareness (58%), Critical infrastructures protection/prevention (67%) and System protection of servers/PCs (74%); and the less valued the Ethical domains research (32%) and Political/Social interventions (26%).

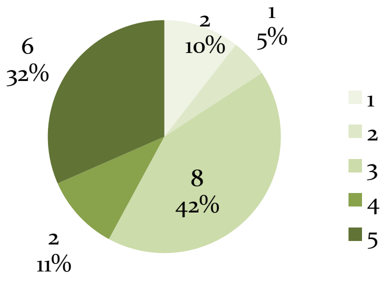
Education/awareness



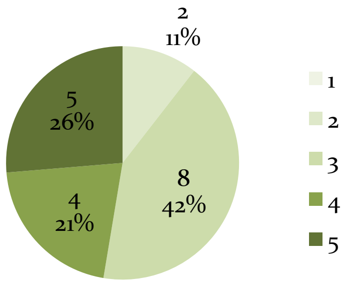
IT&Security Solution



Ethical domains Research



Political/Social Interventions



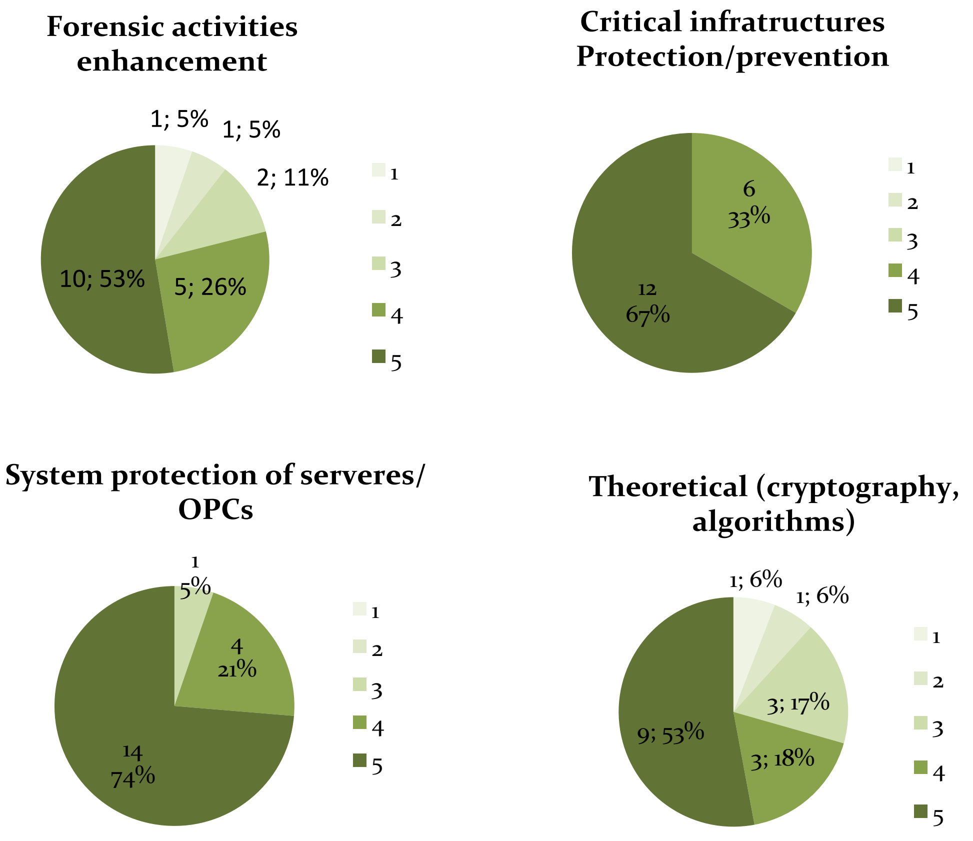


Figure 9 - Cybersecurity Domains

To the question: "What kind of other resources are necessary?" respondents were requested to rank the resources Financial/Hardware/Network/Staff/Training they consider to be necessary to fight cyberterrorism.

Results: the resources selected as more necessary were the Training (16), Staff (13), Hardware (10), Network (10), and the less important the Financial (7).

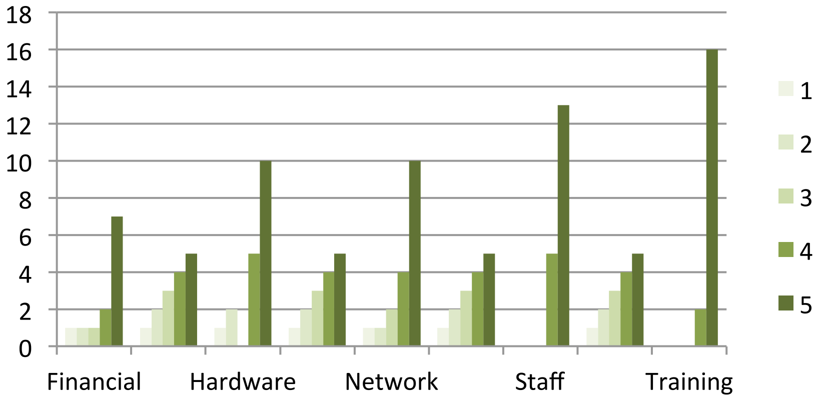


Figure 10 - Resources to fight cyberterrorism

To the question: “What is their cost/effectiveness ratio?” respondents were demanded to grade the conditions that can influence the use of resources to fight cyberterrorism: Developing/Procurement and operational costs/Time consuming/ Training**.**

Results: most likely indicated cost was Procurement and operational costs (10), followed by Time consuming (8).

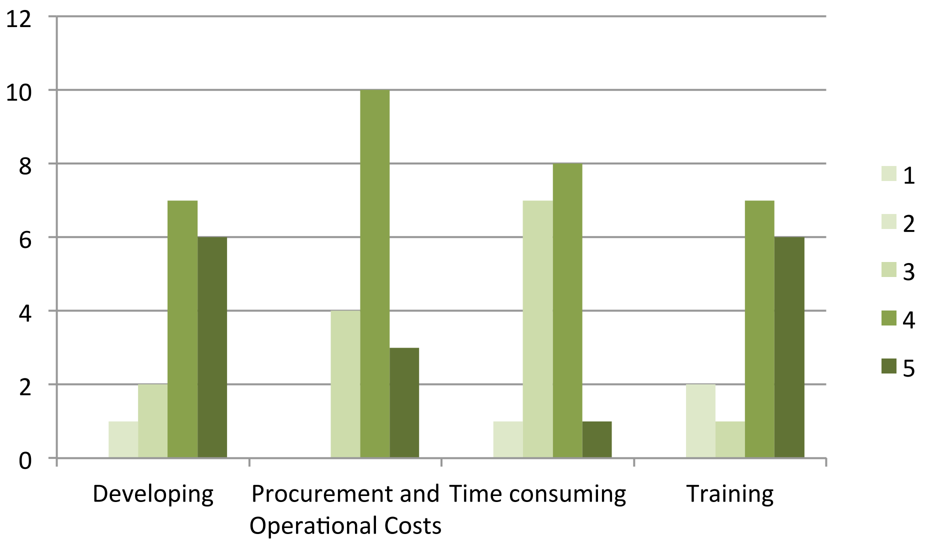


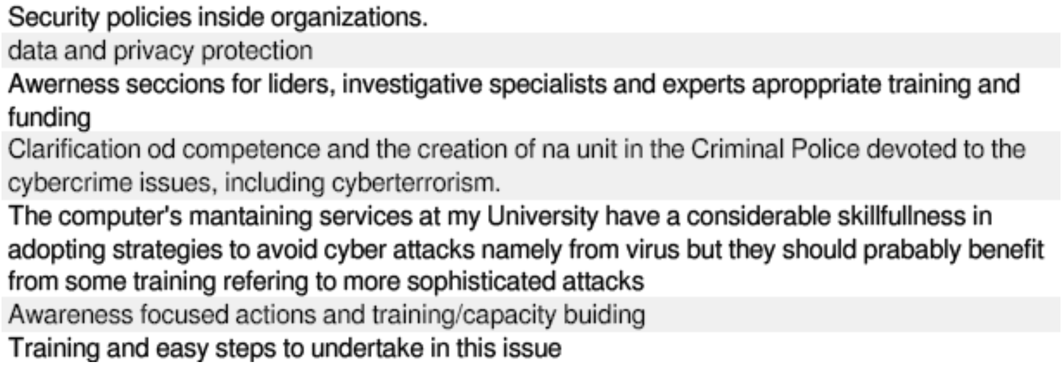
Figure 11 - Resources cost/effectiveness ratio

10.3.4.7 Needs

This topic proposed elaboration on the most important needs that should be taken into account now and in the future.

Results: 15 answers were received from Portugal, Belgium, Spain, Italy, Greece and United Kingdom, summarized in the following description:

Portugal



Security policies inside organizations.

data and privacy protection

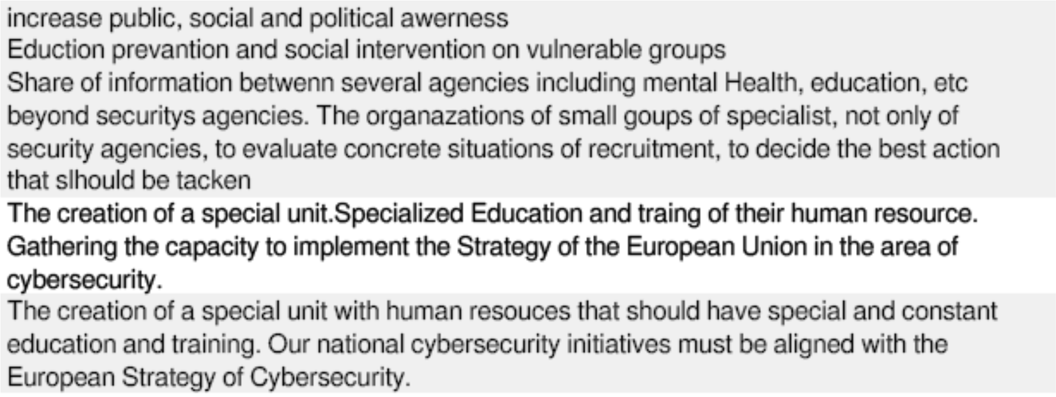
Awerness seccions for liders, investigative specialists and experts aproppriate training and funding

Clarification od competence and the creation of na unit in the Criminal Police devoted to the cybercrime issues, including cyberterrorism.

The computer's mantaining services at my University have a considerable skillfullness in adopting strategies to avoid cyber attacks namely from virus but they should prabably benefit from some training refering to more sophisticated attacks

Awareness focused actions and training/capacity buiding

Training and easy steps to undertake in this issue

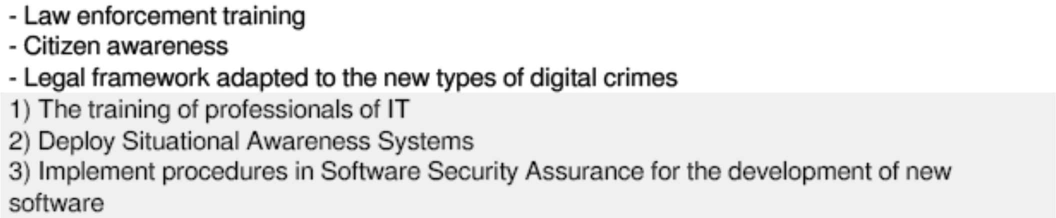


increase public, social and political awerness
Eduction prevantion and social intervention on vulnerable groups
Share of information betwenn several agencies including mental Health, education, etc beyond securitys agencies. The organazations of small goups of specialist, not only of security agencies, to evaluate concrete situations of recruitment, to decide the best action that slhould be tacken

The creation of a special unit.Specialized Education and traing of their human resource. Gathering the capacity to implement the Strategy of the European Union in the area of cybersecurity.

The creation of a special unit with human resouces that should have special and constant education and training. Our national cybersecurity initiatives must be aligned with the European Strategy of Cybersecurity.

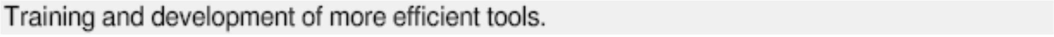
Spain



- Law enforcement training
- Citizen awareness
- Legal framework adapted to the new types of digital crimes

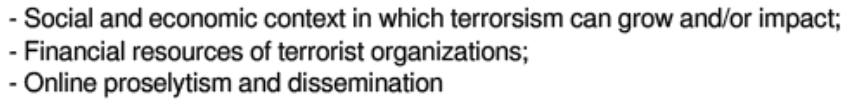
1) The training of professionals of IT
2) Deploy Situational Awareness Systems
3) Implement procedures in Software Security Assurance for the development of new software

Greece



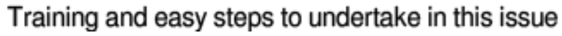
Training and development of more efficient tools.

Italy



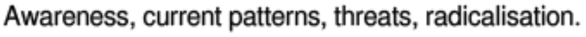
- Social and economic context in which terrorsism can grow and/or impact;
- Financial resources of terrorist organizations;
- Online proselytism and dissemination

Belgium



Training and easy steps to undertake in this issue

United Kingdom



Awareness, current patterns, threats, radicalisation.

10.3.4.8 Cooperation

This topic had the purpose to understand whether the questioned organizations are collaborating or cooperating with the public and/or private sector on cybersecurity technologies, and is do, to state the type of organization/institute, the level and type of collaboration/cooperation and the most important benefits and results.

Results: 17% said yes and 33% said no; from these 17% (5) only 2 countries stated their experience, as follows:

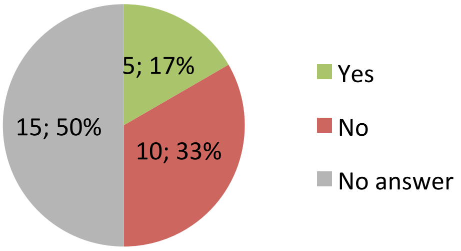
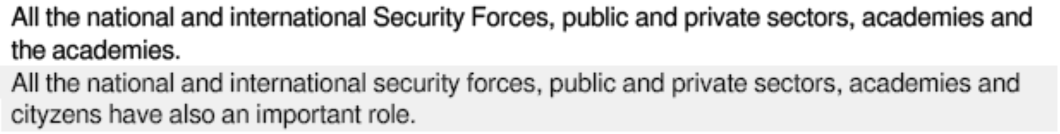


Figure 12 - Collaboration/Cooperation Cybersecurity

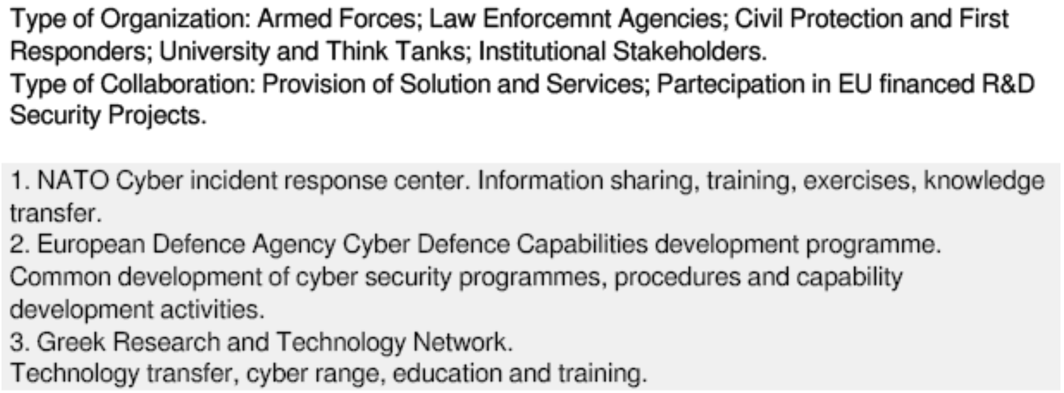
Portugal



All the national and international Security Forces, public and private sectors, academies and the academies.

All the national and international security forces, public and private sectors, academies and cityzens have also an important role.

Italy



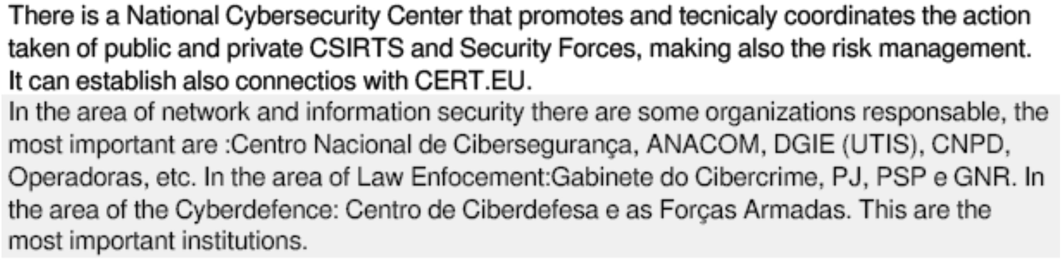
Type of Organization: Armed Forces; Law Enforcemnt Agencies; Civil Protection and First Responders; University and Think Tanks; Institutional Stakeholders.
Type of Collaboration: Provision of Solution and Services; Partecipation in EU financed R&D Security Projects.

1. NATO Cyber incident response center. Information sharing, training, exercises, knowledge transfer.
2. European Defence Agency Cyber Defence Capabilities development programme.
Common development of cyber security programmes, procedures and capability development activities.
3. Greek Research and Technology Network.
Technology transfer, cyber range, education and training.

In accordance to the above mentioned question, respondents were requested to describe the cooperation between governmental institutions and the private sector in relation to cybersecurity.

Answers were also given by Portugal and Italy, as described below:

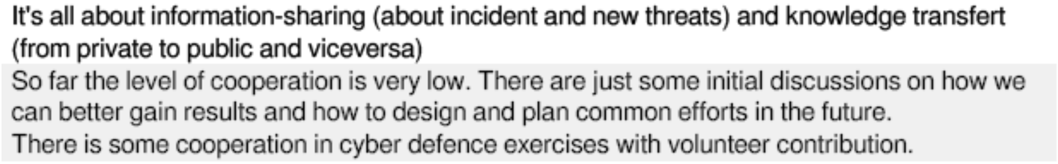
Portugal



There is a National Cybersecurity Center that promotes and tecnicaly coordinates the action taken of public and private CSIRTS and Security Forces, making also the risk management. It can establish also connectios with CERT.EU.

In the area of network and information security there are some organizations responsable, the most important are :Centro Nacional de Cibersegurança, ANACOM, DGIE (UTIS), CNPD, Operadoras, etc. In the area of Law Enfocement:Gabinete do Cibercrime, PJ, PSP e GNR. In the area of the Cyberdefence: Centro de Ciberdefesa e as Forças Armadas. This are the most important institutions.

Italy



It's all about information-sharing (about incident and new threats) and knowledge transfert (from private to public and viceversa)

So far the level of cooperation is very low. There are just some initial discussions on how we can better gain results and how to design and plan common efforts in the future.
There is some cooperation in cyber defence exercises with volunteer contribution.

To the question “What is necessary to build-up an effective PP (Public-Private) cooperation-partnership model? Please describe your experience.”

Results: 11 answers were received from Portugal, Belgium, Italy, Greece and United Kingdom. The main issues stated were:

- Building-up trust;
- Sharing of information to potentiate adequate and timely responses;
- Periodical meetings;
- Need to implement objective cooperation and not get it just by exercising;
- Secure environnements/infrastructures for information exchange;
- PP Cooperation needs well defined rules, outlined by the law, with legislation standards;
- Financial improvement on behalf of the Public Sector.

Afterwards the questionnaire proceeded: “How do you assess the PP cooperation-partnership model in your country?” If **it** is sufficient or needs to be improved.

Results: Only **3%** of the respondents said the PP cooperation-partnership model in their country is sufficient; 34% said there is no need for improvement.

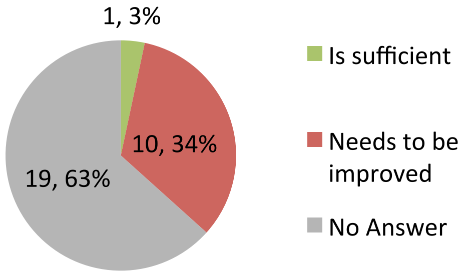


Figure 13 - Cooperation-Partnership Model

10.3.4.9 *Prevention*

In this specific topic respondents were questioned whether their organization follow any guideline(s) to prevent the use of internet by terrorists, and if yes, which one?

Results: Only 3% of the respondents said that their organization follow a guideline, while the other 50% said no. No responses were given as a second answer.

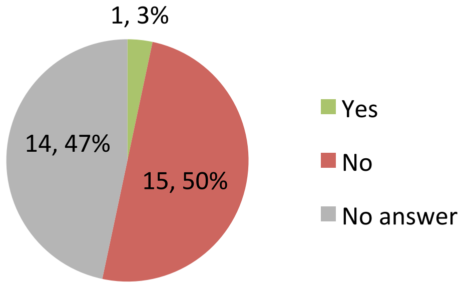


Figure 14 - Guidelines prevent Internet terrorist

10.3.4.10 *Domains*

The last question of the questionnaire was: "What would you consider to be the three-top best domains to counter cyberterrorism?

- Technological Security Techniques
- Social Policies (Education, job opportunities, etc.)
- Legal Framework
- Cooperation between business sector and government
- All the items mentioned above

Results: The domains assessed as the top-best domains to counter cyberterrorism are Cooperation between business sector and government (26%), Legal Framework (26%) and Technological Security Techniques (16%); still there is a common consensus that all items are important to the process of CT.

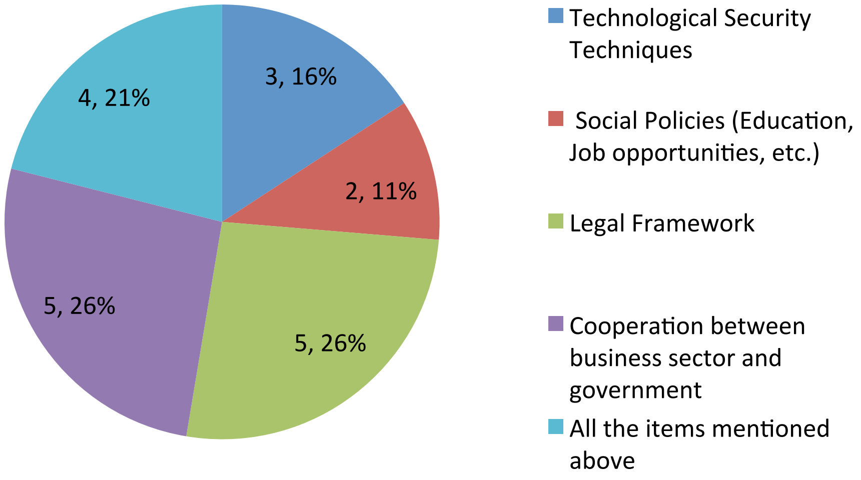


Figure 15 - Domains to counter cyberterrorism

11 CONCLUSIONS

Both the answers to the questionnaire and the literature reviewed allow us to conclude that Europe needs, first of all, a global technological strategic approach. Maybe ENLETS and other European IT approaches could play a role in this subject. It's urgent to identify the technological innovations that may turn it easier to identify the threats in the digital world and easily neutralize it.

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.

Despite the information on the legal frameworks, both in Portugal and in the countries that are members or observers of the Council of Europe, respondents showed a different view on the topic. The legal frameworks must be taken into account and they must be adapted to the various threats and needs identified. The issues of privacy, digital security and data protection must be addressed also from this perspective. For instance, is it legally admissible the use of the digital undercover agent for the purpose of the fight against cyberterrorism?

The cooperation between public and private sectors are a major issue. It is urgent to bridge them. It is also critical and urgent to define a model of public-private partnerships that can reinforce cooperation among all stakeholders, with a view to better identify the threats and better prepare the EU to neutralize those threats, thus enabling an increased protection of the cyberspace. It is urgent to work in close cooperation - private industry, governments, LEA, ISP, social networks, video broadcasting platforms and social media.

Training and police cooperation must be improved, involving all the actors in the detection, prevention, investigation and punishment of cyber offences. It is urgent to increase the development of training programmes for judges, public prosecutors and criminal investigators, so that all the intervenients in the detection and punishment of these crimes may and share have the same level of knowledge and expertise.

It would be of added value for the European society to raise the level of awareness, thus helping LEA to identify signals of possible (cyber)terrorist activity in preparation.

There should be some training programs designed for the social media, trying to reduce or even eliminate some news, which result in the best propaganda campaigns for terrorists.

There should be a special legal instrument that allows for the use of new intrusive methods, like the so-called “remote forensics", the use of a police trojan, which enables the remote access to data, information and suspicious targets, before these may hide behind the encryption of their information.

Following the establishment of the EU IRU at EUROPOL, the establishment of the national IRU should become mandatory as a measure to implement the European strategy on this issue.

Some MS like the UK, have already created specialized police units to monitor the cyber environment, identify contents of a violent extremist or terrorist nature and work closely with the industry to remove them on the basis that it breaches individual companies' user policies. This measure could be extended to all LEA with the mission of fighting (cyber)terrorism.

At the legal dimension, cybercrime is not always considered as a crime, thus resulting in some investigative constraints. This situation should be overcome in the legal frameworks of all EU MS.

Also at the legal level, the surveillance and "takedown" of internet sites with criminal information, either promoting (cyber)terrorism or not, using information and communication technologies, is still dependent on a slow legal and bureaucratic procedure and there are no agile means to suspend a site, a chat or propaganda, with ulterior judicial supervision and ratification. Legislation should include legal provisions on this subject.

At the legal and technical levels, there are some constraints to the use of open source intelligence (OSINT). There are mainly three limitations that require the attention of European and national authorities:

- The high purchase costs of special tools to collect information in open source environment prevent some LEA to have the adequate tools to perform their mission; this means that the tools are not equal among LEA;
- The lack of a legal definition of “open source” (cf. https://www.academia.edu/7301278/OPEN_SOURCES_IN_CYBERCRIME_INVESTIGATION_concept_and_implications);
- The indefinition and the need to review the legal concept of "*call detailed records*" or "*traffic data*", in order to go beyond the IP and IMEI addresses of mobile communications terminals (cf. https://www.academia.edu/743036/traffic_data_from_computer_crime_enforcement_to_future_intelligence_for_a_strategic_vision_)

Also according to the experience gained and collected by CT agencies in European countries, it has been recognized the use of false documents (originally counterfeited) or forged ones (altered) and correspondent travel documents by members of terrorist cells in order to ensure the ability to move across the European soil and furthermore to improve chances for circulation in a way to reach third countries, including the so-called risk ones or the regions where potential for insurgency or conflicts exist or are progressing.

The use of biometric data for the issuance of those ID and travel documents in the most recent years somehow diminished the amount of reported cases but the topic is still a concern for international CT authorities. As a matter of fact, mobility keeps being a critical or core item for terrorism and respective agents and it can only be ensured all over the globe, whenever documents – genuine, false or forged – are available. One could read in the report of the Commission responsible for the investigation of the 9/11 terrorist attacks in the US, that: "*for terrorists, documents are as important as weapons*".

A final topic was included regarding some European fund oportunities for the prevention and fight against cyber offenses – **c**ybercrime and **c**yberterrorism.

12.1 *EUROPEAN FUNDING FOR THE FIGHT AGAINST CYBERCRIME AND CYBERTERRORISM*

From the perspective of a LEA, there are two main funding programs, which have a very strong role in the development of projects towards the improvement of the capacity to fight against cybercrime and cyberterrorism: Internal Security Fund-P (Police) and Horizon 2020 (H2020). LEA should make an effort to take the most advantages from these European funding programmes.

In short, the Internal Security Fund is designed to fight against transnational and organi**s**ed crime, including terrorism.

Beyond the Specific and Direct Actions from the European Commission all EU MS have been working on the preparation of the national programmes, according to the EU Strategy and the national priorities.

This work is the continuation of the Policy Dialogue that ended in September 2013, on the basis of the European Key Policy Issues (KPI). Among the KPI, one is targeted for cybercrime. No reference is made to cyberterrorism, although there are three KPI that are suitable for terrorism (cf. table below). There is also a KPI for training, which can be used for the specialized training that has been referred as a weak point in the fight against cyberterrorism.

It should be considered the possibility to have further direct calls focused on technology, training and cooperation aiming at the prevention and fight against cybercrime and cyberterrorism.

In the current H2020 workprogramme (Secure Societies), there is one specific topic addressed to cyberterrorism, which involves three domains: Fight against cyberterrorism, Training and **c**ritical infrastructures. In the table below, we attribute the following level of relation to the fight against cyberterrorism:

1 – Direct

2 – Indirect

3 – It is possible to exploit synergies

INTERNAL SECURITY FUND POLICE COOPERATION - POLICY DIALOGUE WITH PORTUGAL	
ISF-P (Portugal)	**RELATION**
Participation of Portugal in the EU policy cycle on serious and organised crime	3
Improve capabilities in the fight against cyber-crime at national level and contribute to improvement at the EU level	2
Implementation of the EU Law Enforcement Training Scheme (LETS)	1

Table 4 – ISF-P Level of relation

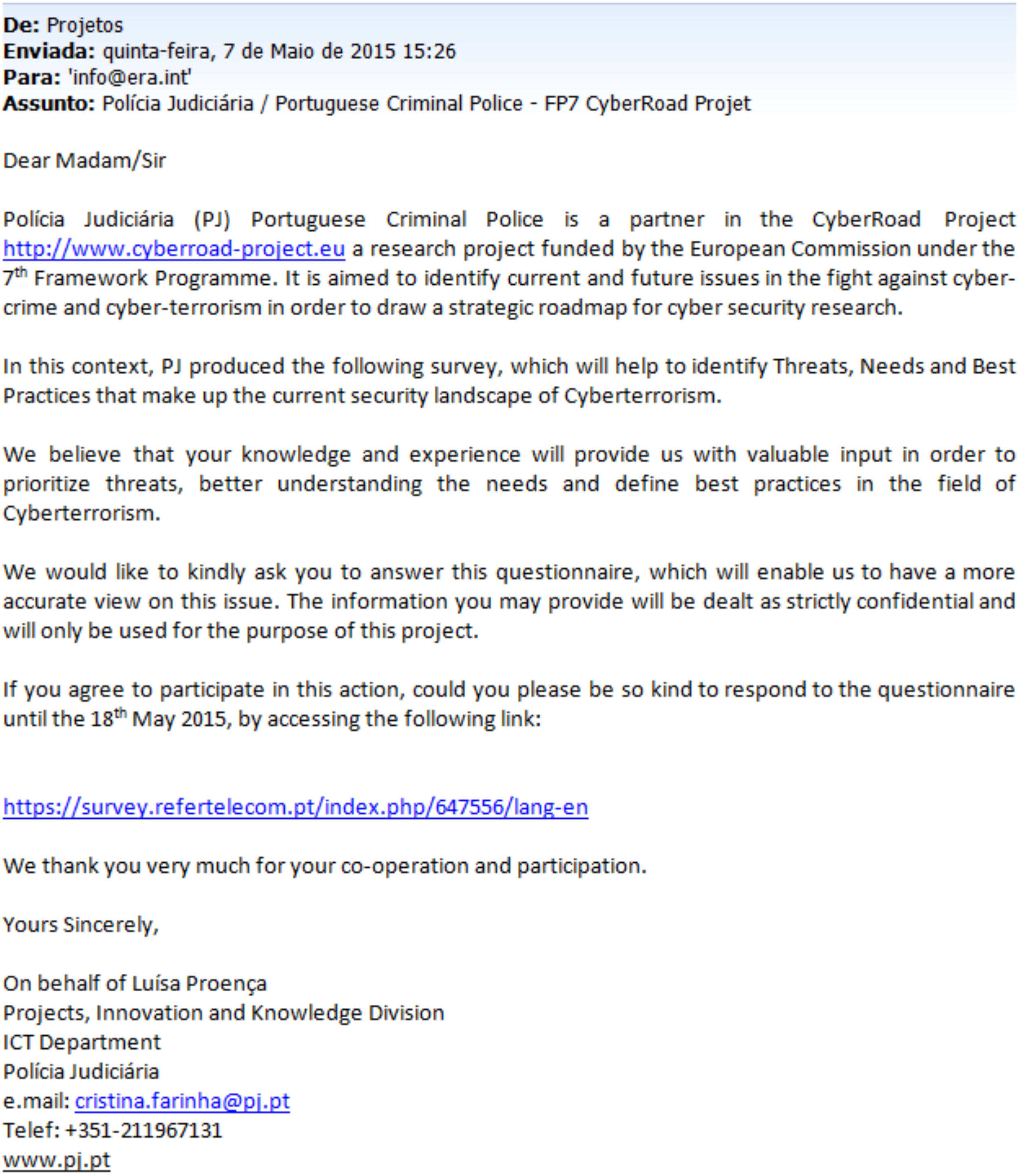
H2020	
5. LEADERSHIP IN ENABLING AND INDUSTRIAL TECHNOLOGIES - I. INFORMATION AND COMMUNICATION TECHNOLOGIES	RELATION
ICT 1 – 2014: Smart Cyber-Physical Systems	3
ICT 4 – 2015: Customised and low power computing	3
ICT 30 – 2015: Internet of Things and Platforms for Connected Smart Objects	3
ICT 32 – 2014: Cybersecurity, Trustworthy ICT	2
14. SECURE SOCIETIES – PROTECTING FREEDOM AND SECURITY OF EUROPE AND ITS CITIZENS	RELATION
Call - Disaster-resilience	
DRS-2-2014: Crisis management topic 2: Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRN contamination and/or exposure	3
DRS-7-2014: Crisis management topic 7: Crises and disaster resilience – operationalizing resilience concepts	3
DRS-14-2015: Critical Infrastructure Protection topic 3: Critical Infrastructure resilience indicator - analysis and development of methods for assessing resilience	2
DRS-15-2015: Critical Infrastructure Protection topic 4: Protecting potentially hazardous and sensitive sites/areas considering multi-sectorial dependencies	2

DRS-16-2014: Critical Infrastructure Protection topic 5: Improving the aviation security chain	2
DRS-20-2014: Ethical/Societal Dimension topic 1: Improving protection of Critical infrastructures from insider threats	2
Call – Fight against crime and Terrorism	
FCT-3-2015: Forensics topic 3: Mobile, remotely controlled technologies to examine a crime scene in case of an accident or a terrorist attack involving CBRNE materials	3
FCT-6-2015: Law Enforcement capabilities 2: Detection and analysis of terrorist - related content on the Internet	1
FCT-7-2014: Law enforcement capabilities topic 3: Pan European platform for serious gaming and training	1
FCT-13-2014: Ethical/Societal Dimension Topic 1: Factors affecting (in-) security	3
FCT-16-2015: Ethical/Societal Dimension Topic 4 - Investigating the role of social, psychological and economic aspects of the processes that lead to organised crime (including cyber related offenses), and terrorist networks and their impact on social cohesion	1
Call – Digital Security: Cybersecurity, Privacy and Trust	
DS-3-2015: The role of ICT in Critical Infrastructure Protection	1

Table 5 – H2020 Level of relation

Europol has been working on the analysis of H2020 topics and released the document “*Specification of topics for R&D Projects, which aims at “providing direction for project proposals for recently published calls under the Horizon 2020 Programme*”. That document is enclosed as ANNEX IV: EUROPOL EC3 FEF - RD H2020 - Specification of Topics for RD Projects

13 Annex I: Presentation of the questionnaire



De: Projetos
Enviada: quinta-feira, 7 de Maio de 2015 15:26
Para: 'info@era.int'
Assunto: Polícia Judiciária / Portuguese Criminal Police - FP7 CyberRoad Projet

Dear Madam/Sir

Polícia Judiciária (PJ) Portuguese Criminal Police is a partner in the CyberRoad Project http://www.cyberroad-project.eu a research project funded by the European Commission under the 7th Framework Programme. It is aimed to identify current and future issues in the fight against cyber-crime and cyber-terrorism in order to draw a strategic roadmap for cyber security research.

In this context, PJ produced the following survey, which will help to identify Threats, Needs and Best Practices that make up the current security landscape of Cyberterrorism.

We believe that your knowledge and experience will provide us with valuable input in order to prioritize threats, better understanding the needs and define best practices in the field of Cyberterrorism.

We would like to kindly ask you to answer this questionnaire, which will enable us to have a more accurate view on this issue. The information you may provide will be dealt as strictly confidential and will only be used for the purpose of this project.

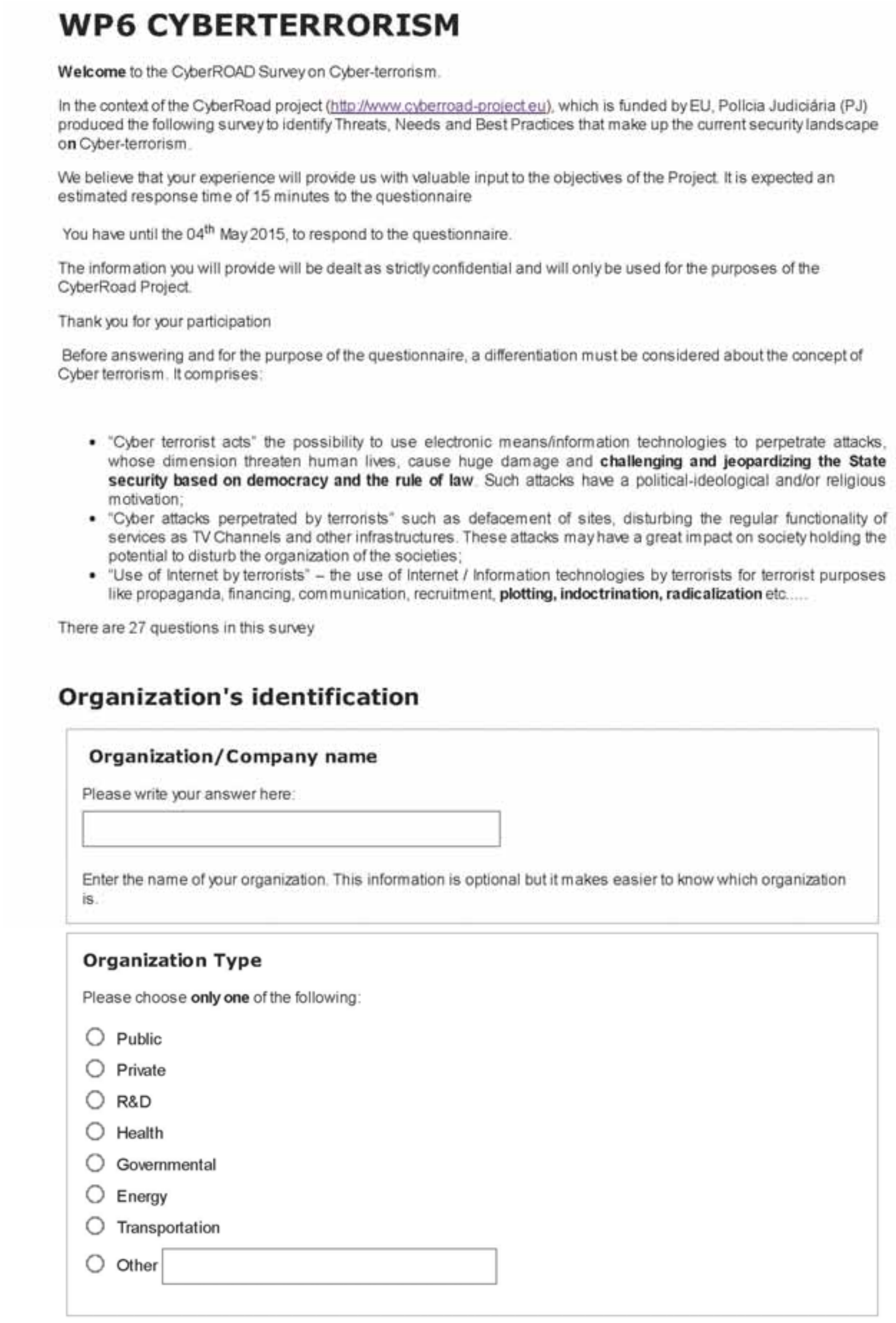
If you agree to participate in this action, could you please be so kind to respond to the questionnaire until the 18th May 2015, by accessing the following link:

https://survey.refertelecom.pt/index.php/647556/lang-en

We thank you very much for your co-operation and participation.

Yours Sincerely,

On behalf of Luísa Proença
Projects, Innovation and Knowledge Division
ICT Department
Polícia Judiciária
e.mail: cristina.farinha@pj.pt
Telef: +351-211967131
www.pj.pt



WP6 CYBERTERRORISM

Welcome to the CyberROAD Survey on Cyber-terrorism.

In the context of the CyberRoad project (http://www.cyberroad-project.eu), which is funded by EU, Policia Judiciária (PJ) produced the following survey to identify Threats, Needs and Best Practices that make up the current security landscape **o**n Cyber-terrorism.

We believe that your experience will provide us with valuable input to the objectives of the Project. It is expected an estimated response time of 15 minutes to the questionnaire

You have until the 04th May 2015, to respond to the questionnaire.

The information you will provide will be dealt as strictly confidential and will only be used for the purposes of the CyberRoad Project.

Thank you for your participation

Before answering and for the purpose of the questionnaire, a differentiation must be considered about the concept of Cyber terrorism. It comprises:

- "Cyber terrorist acts" the possibility to use electronic means/information technologies to perpetrate attacks, whose dimension threaten human lives, cause huge damage and **challenging and jeopardizing the State security based on democracy and the rule of law**. Such attacks have a political-ideological and/or religious motivation;
- "Cyber attacks perpetrated by terrorists" such as defacement of sites, disturbing the regular functionality of services as TV Channels and other infrastructures. These attacks may have a great impact on society holding the potential to disturb the organization of the societies;
- "Use of Internet by terrorists" – the use of Internet / Information technologies by terrorists for terrorist purposes like propaganda, financing, communication, recruitment, **plotting, indoctrination, radicalization** etc.....

There are 27 questions in this survey

Organization's identification

Organization/Company name

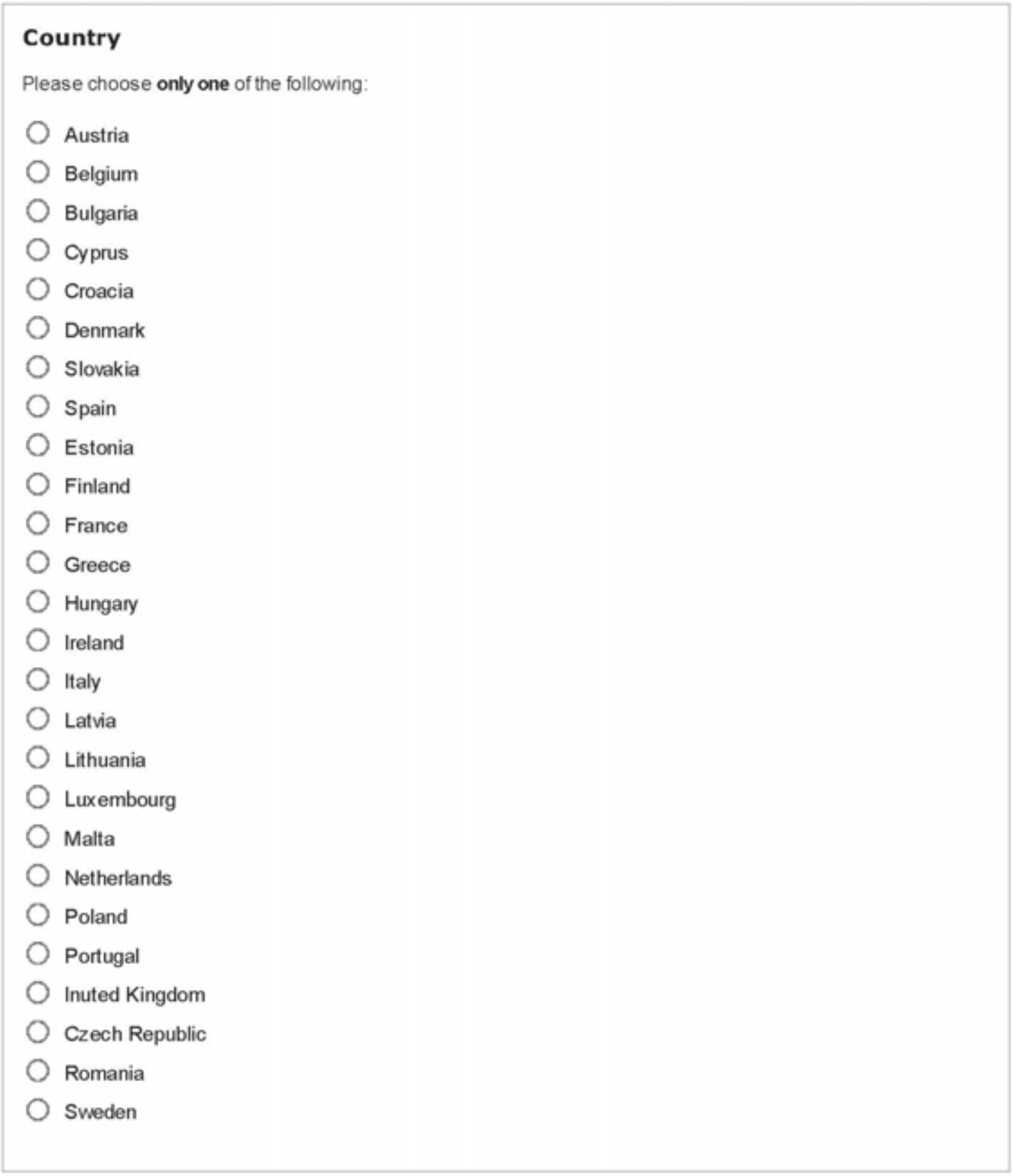
Please write your answer here:

Enter the name of your organization. This information is optional but it makes easier to know which organization is.

Organization Type

Please choose **only one** of the following:

○ Public
○ Private
○ R&D
○ Health
○ Governmental
○ Energy
○ Transportation
○ Other



Country

Please choose **only one** of the following:

○ Austria

○ Belgium

○ Bulgaria

○ Cyprus

○ Croacia

○ Denmark

○ Slovakia

○ Spain

○ Estonia

○ Finland

○ France

○ Greece

○ Hungary

○ Ireland

○ Italy

○ Latvia

○ Lithuania

○ Luxembourg

○ Malta

○ Netherlands

○ Poland

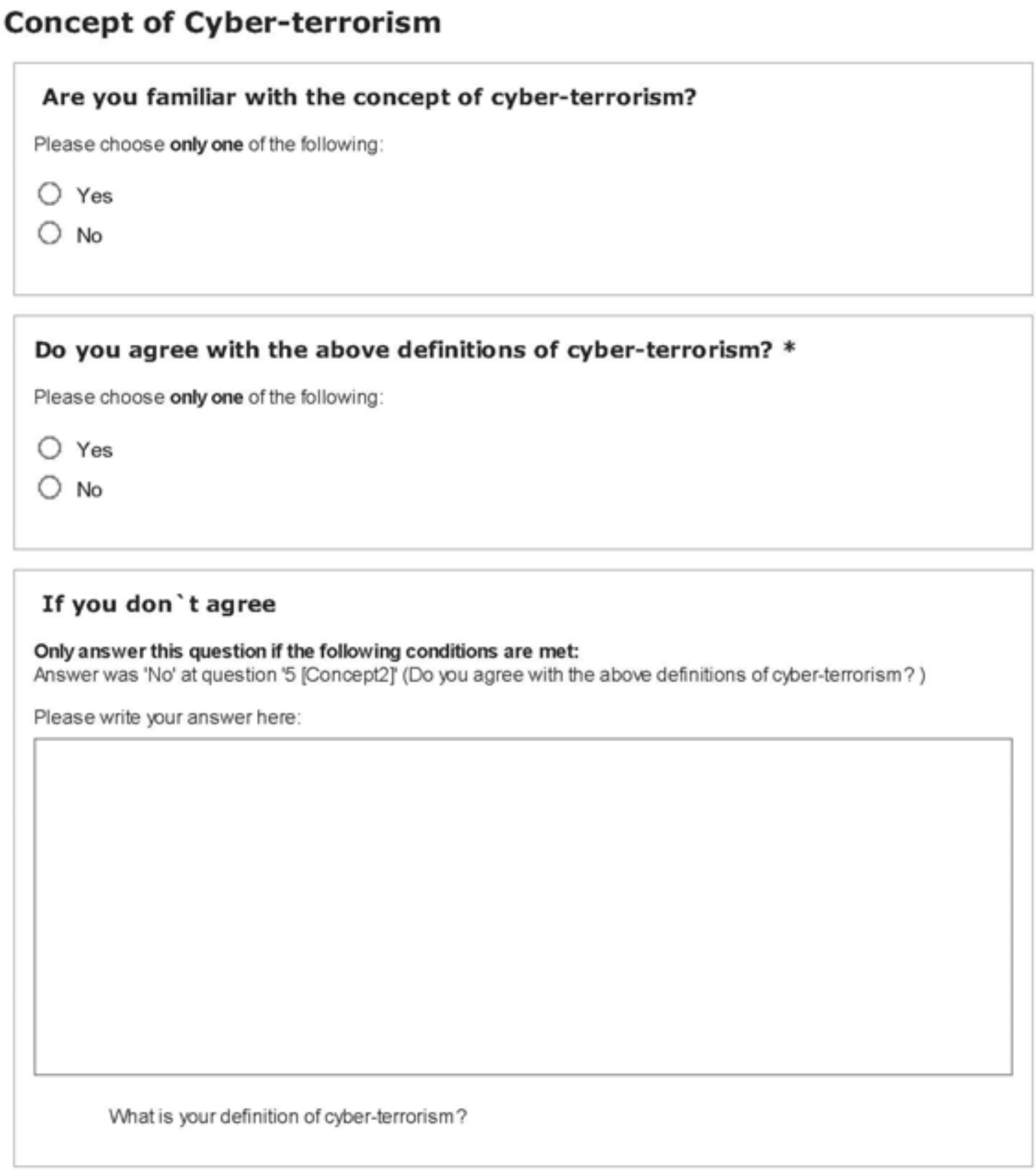
○ Portugal

○ Inuted Kingdom

○ Czech Republic

○ Romania

○ Sweden



Concept of Cyber-terrorism

Are you familiar with the concept of cyber-terrorism?

Please choose **only one** of the following:

○ Yes

○ No

Do you agree with the above definitions of cyber-terrorism? *

Please choose **only one** of the following:

○ Yes

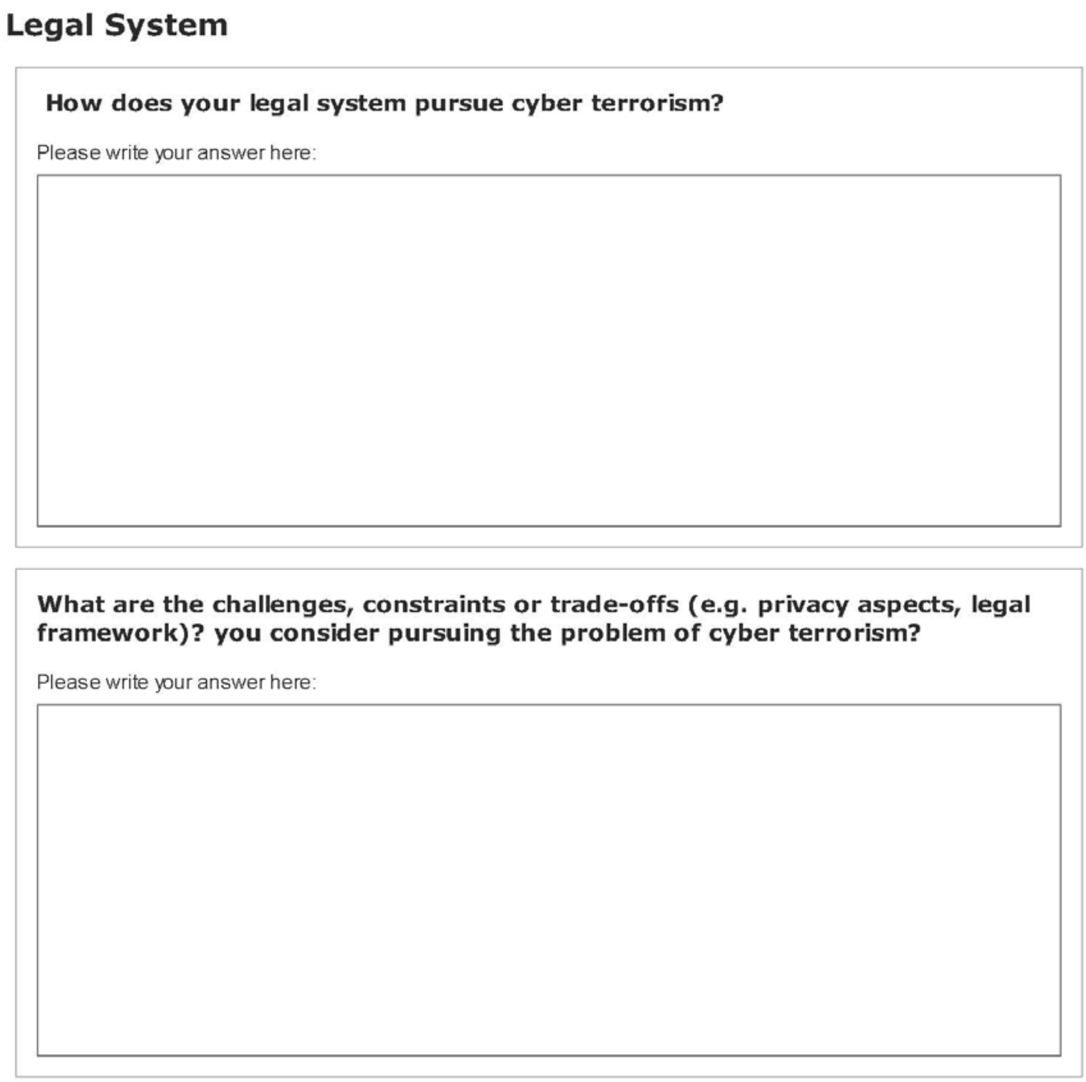
○ No

If you don`t agree

Only answer this question if the following conditions are met:
Answer was 'No' at question '5 [Concept2]' (Do you agree with the above definitions of cyber-terrorism?)

Please write your answer here:

What is your definition of cyber-terrorism?



Legal System

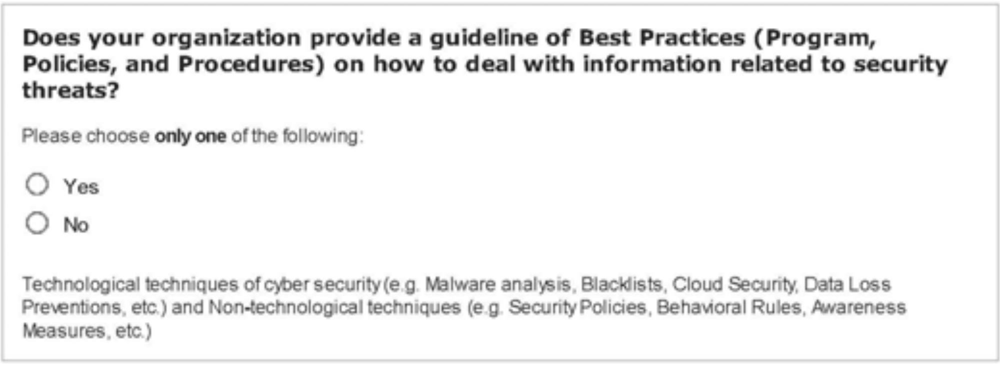
How does your legal system pursue cyber terrorism?

Please write your answer here:

What are the challenges, constraints or trade-offs (e.g. privacy aspects, legal framework)? you consider pursuing the problem of cyber terrorism?

Please write your answer here:

Guidelines



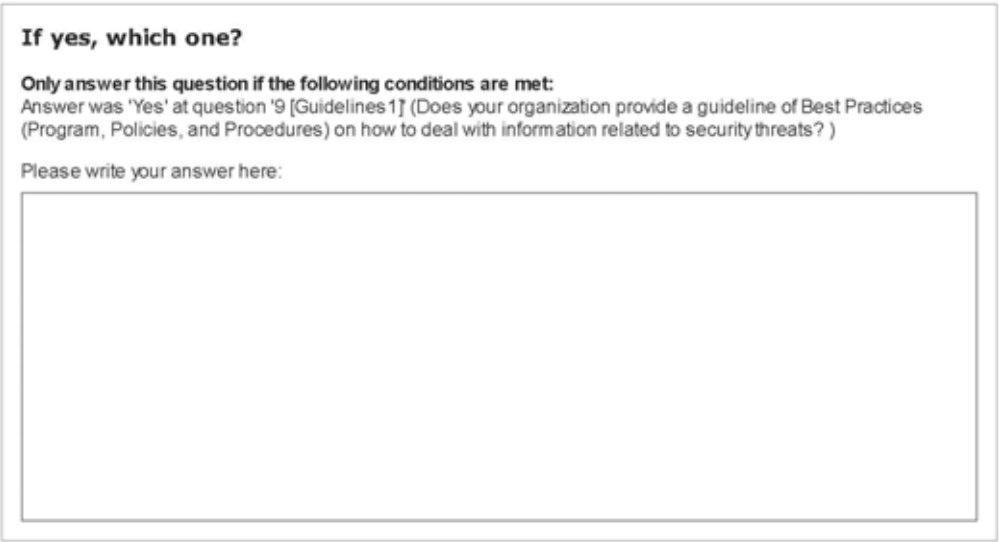
Does your organization provide a guideline of Best Practices (Program, Policies, and Procedures) on how to deal with information related to security threats?

Please choose **only one** of the following:

○ Yes

○ No

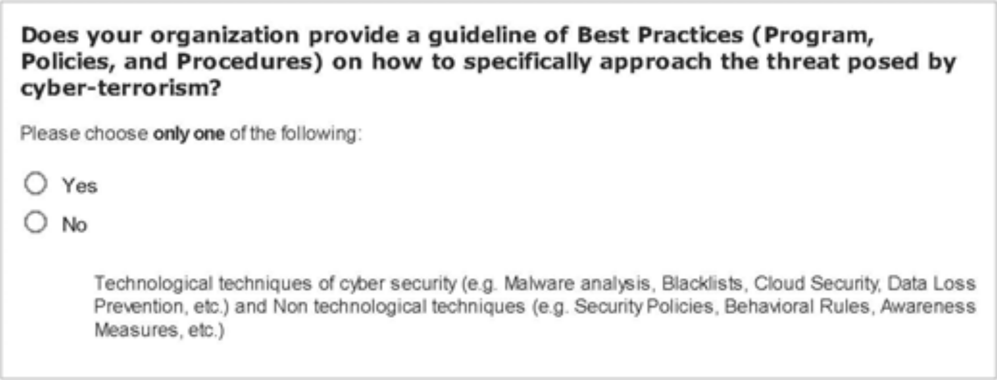
Technological techniques of cyber security (e.g. Malware analysis, Blacklists, Cloud Security, Data Loss Preventions, etc.) and Non-technological techniques (e.g. Security Policies, Behavioral Rules, Awareness Measures, etc.)



If yes, which one?

Only answer this question if the following conditions are met:
Answer was 'Yes' at question '9 [Guidelines1]' (Does your organization provide a guideline of Best Practices (Program, Policies, and Procedures) on how to deal with information related to security threats?)

Please write your answer here:



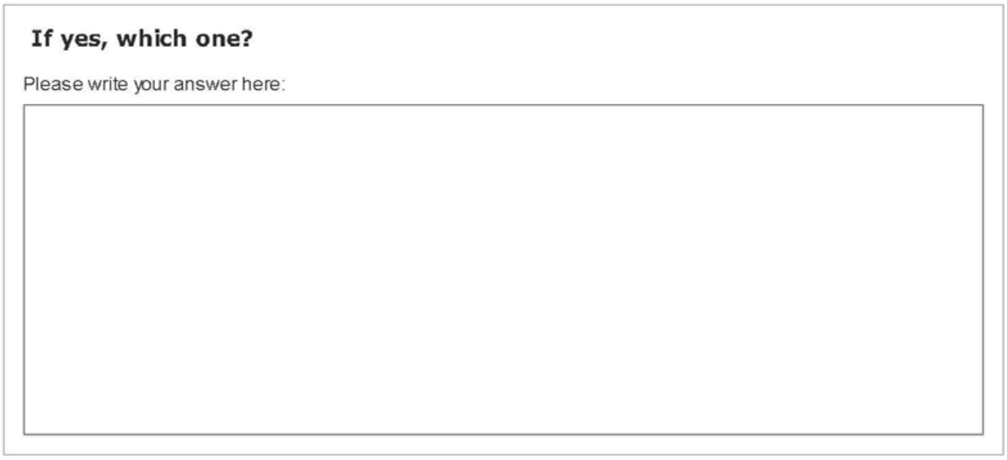
Does your organization provide a guideline of Best Practices (Program, Policies, and Procedures) on how to specifically approach the threat posed by cyber-terrorism?

Please choose **only one** of the following:

○ Yes

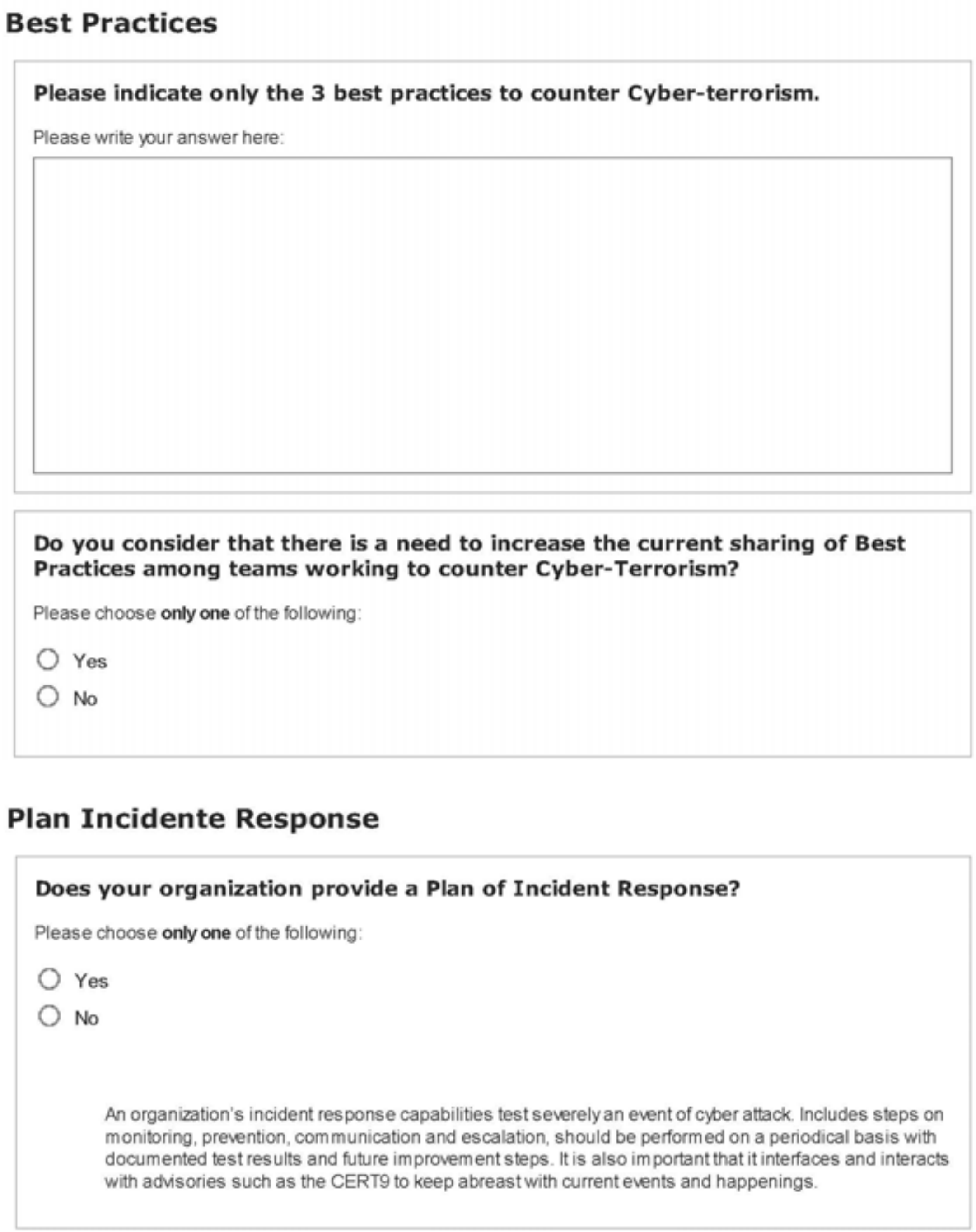
○ No

Technological techniques of cyber security (e.g. Malware analysis, Blacklists, Cloud Security, Data Loss Prevention, etc.) and Non technological techniques (e.g. Security Policies, Behavioral Rules, Awareness Measures, etc.)



If yes, which one?

Please write your answer here:



Best Practices

Please indicate only the 3 best practices to counter Cyber-terrorism.

Please write your answer here:

Do you consider that there is a need to increase the current sharing of Best Practices among teams working to counter Cyber-Terrorism?

Please choose **only one** of the following:

○ Yes

○ No

Plan Incidente Response

Does your organization provide a Plan of Incident Response?

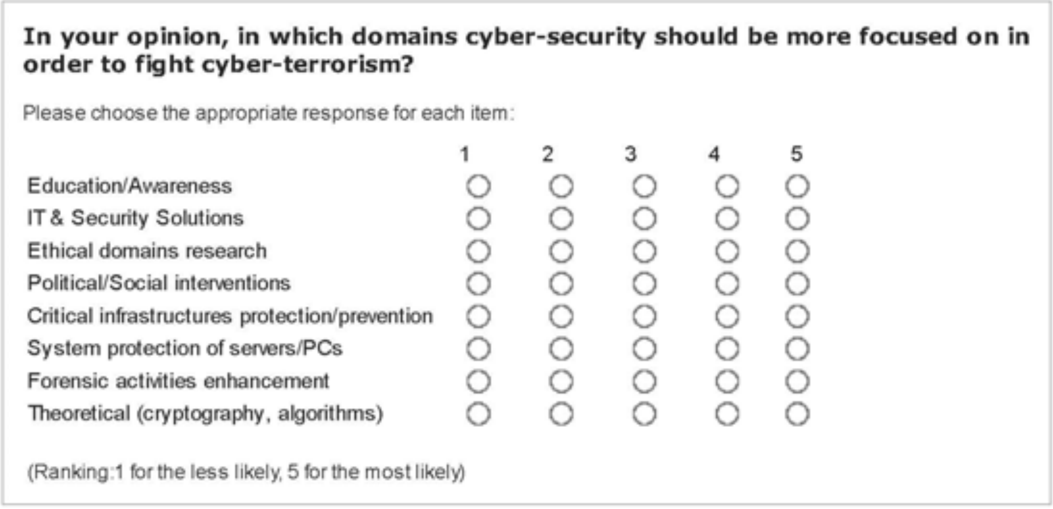
Please choose **only one** of the following:

○ Yes

○ No

An organization's incident response capabilities test severely an event of cyber attack. Includes steps on monitoring, prevention, communication and escalation, should be performed on a periodical basis with documented test results and future improvement steps. It is also important that it interfaces and interacts with advisories such as the CERT9 to keep abreast with current events and happenings.

Domains cyber-security

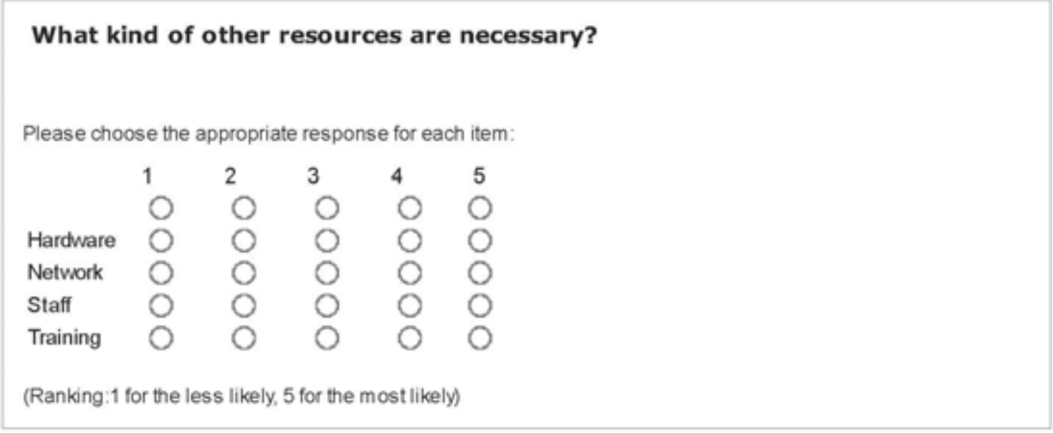


In your opinion, in which domains cyber-security should be more focused on in order to fight cyber-terrorism?

Please choose the appropriate response for each item:

	1	2	3	4	5
Education/Awareness	○	○	○	○	○
IT & Security Solutions	○	○	○	○	○
Ethical domains research	○	○	○	○	○
Political/Social interventions	○	○	○	○	○
Critical infrastructures protection/prevention	○	○	○	○	○
System protection of servers/PCs	○	○	○	○	○
Forensic activities enhancement	○	○	○	○	○
Theoretical (cryptography, algorithms)	○	○	○	○	○

(Ranking:1 for the less likely, 5 for the most likely)

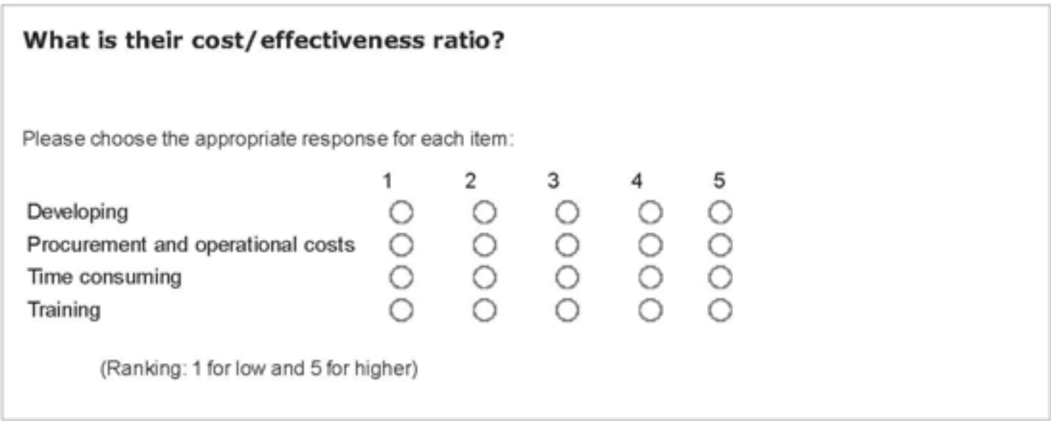


What kind of other resources are necessary?

Please choose the appropriate response for each item:

	1	2	3	4	5
	○	○	○	○	○
Hardware	○	○	○	○	○
Network	○	○	○	○	○
Staff	○	○	○	○	○
Training	○	○	○	○	○

(Ranking:1 for the less likely, 5 for the most likely)



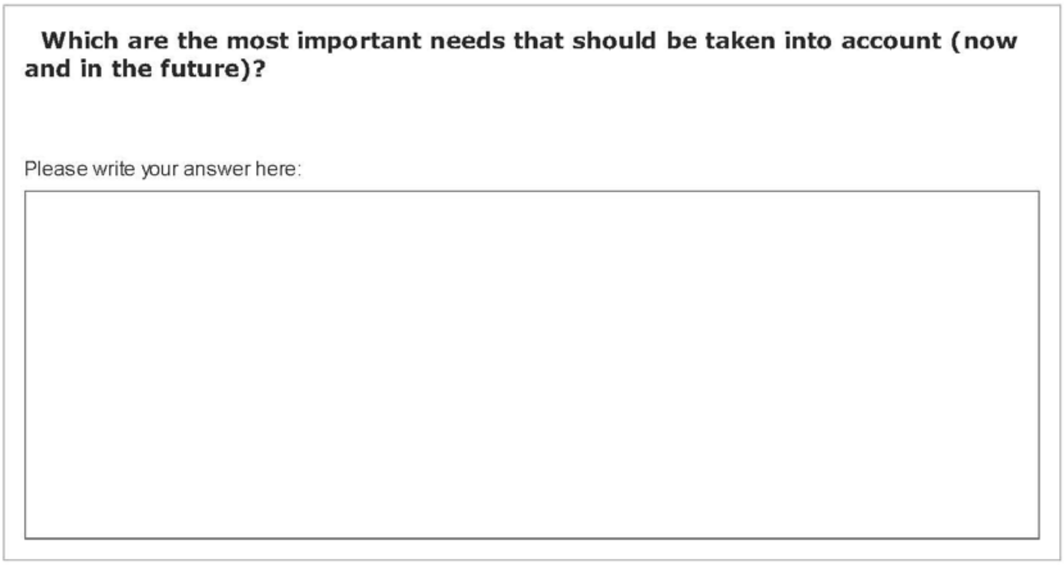
What is their cost/effectiveness ratio?

Please choose the appropriate response for each item:

	1	2	3	4	5
Developing	○	○	○	○	○
Procurement and operational costs	○	○	○	○	○
Time consuming	○	○	○	○	○
Training	○	○	○	○	○

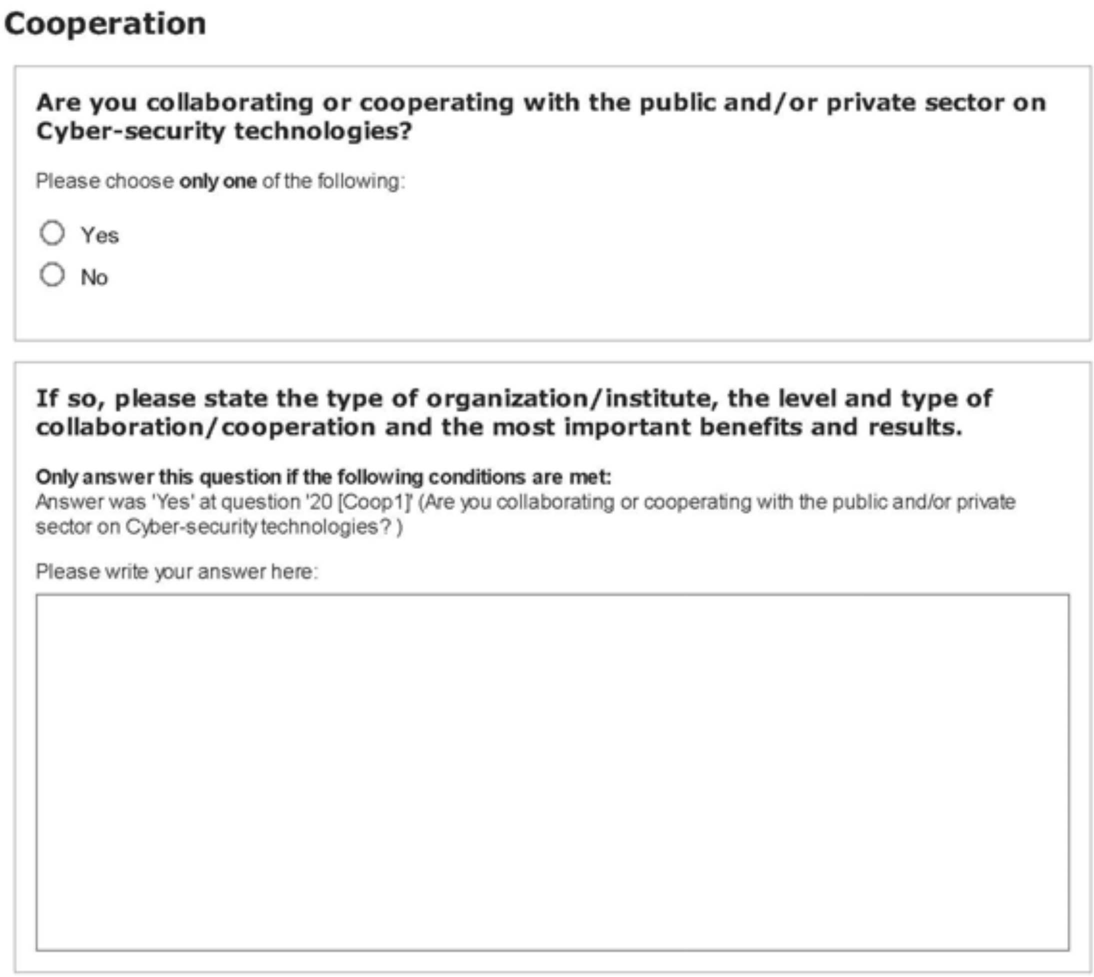
(Ranking: 1 for low and 5 for higher)

Needs



Which are the most important needs that should be taken into account (now and in the future)?

Please write your answer here:



Cooperation

Are you collaborating or cooperating with the public and/or private sector on Cyber-security technologies?

Please choose **only one** of the following:

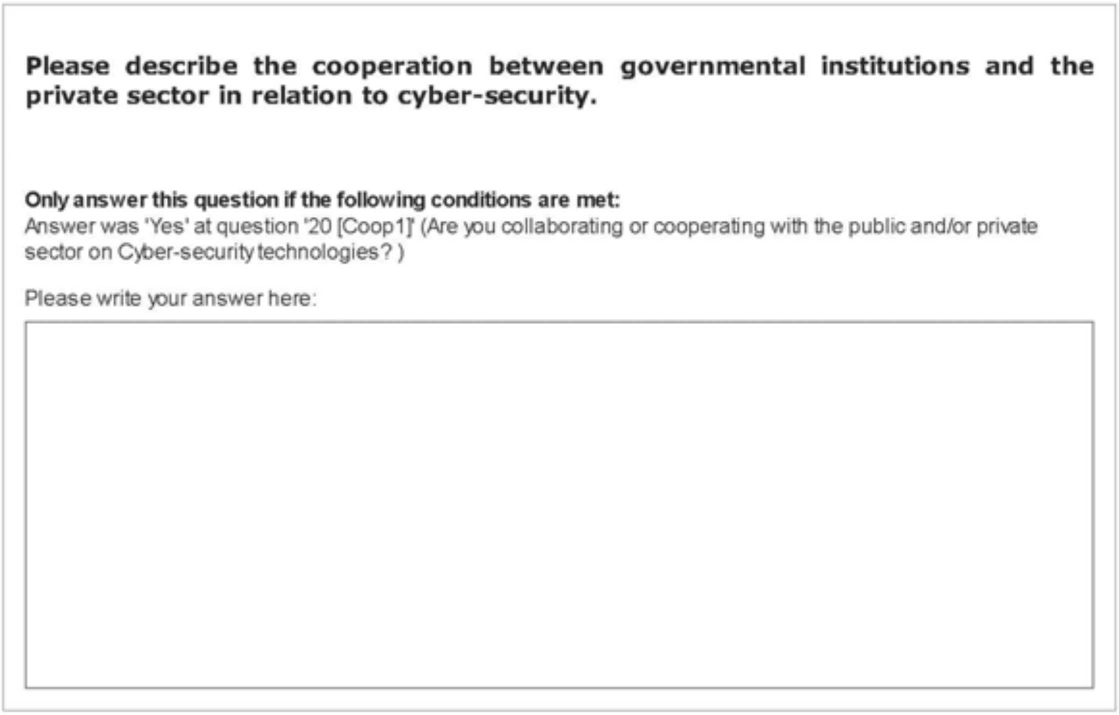
○ Yes

○ No

If so, please state the type of organization/institute, the level and type of collaboration/cooperation and the most important benefits and results.

Only answer this question if the following conditions are met:
Answer was 'Yes' at question '20 [Coop1]' (Are you collaborating or cooperating with the public and/or private sector on Cyber-security technologies?)

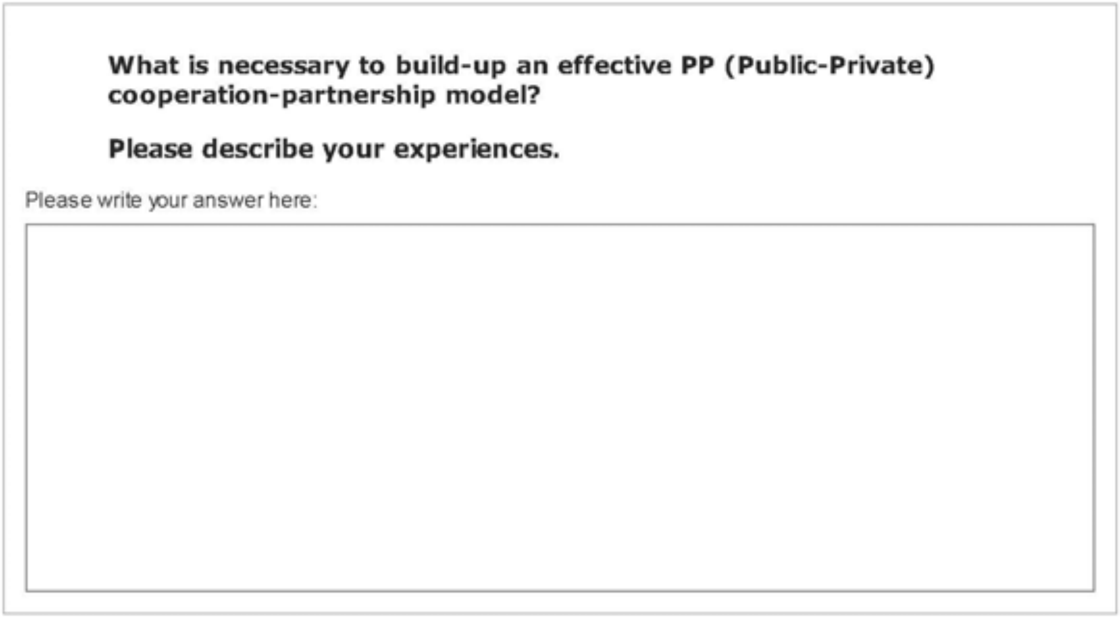
Please write your answer here:



Please describe the cooperation between governmental institutions and the private sector in relation to cyber-security.

Only answer this question if the following conditions are met:
Answer was 'Yes' at question '20 [Coop1]' (Are you collaborating or cooperating with the public and/or private sector on Cyber-security technologies?)

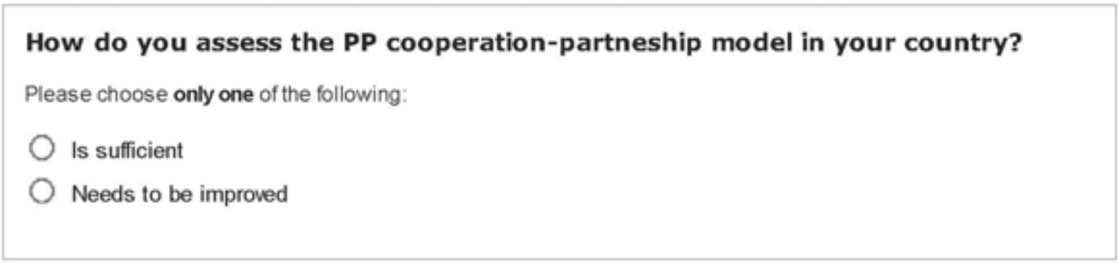
Please write your answer here:



What is necessary to build-up an effective PP (Public-Private) cooperation-partnership model?

Please describe your experiences.

Please write your answer here:

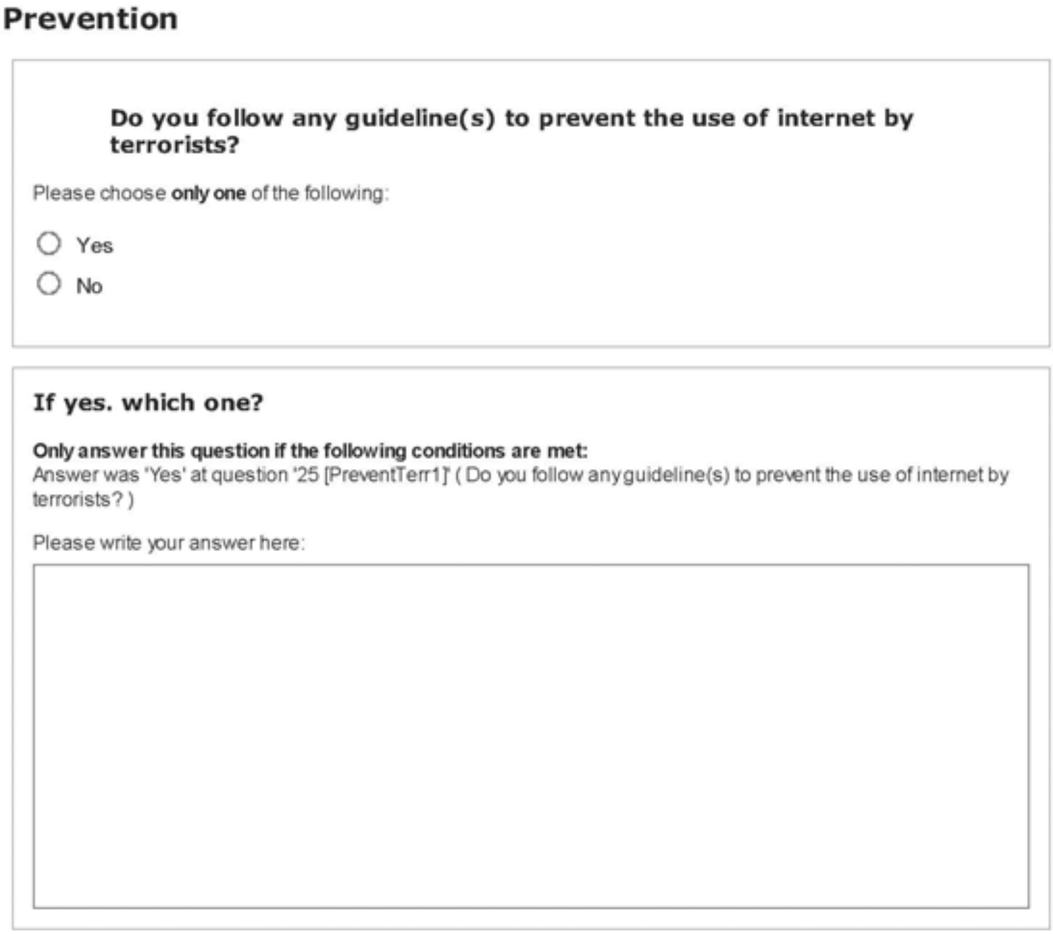


How do you assess the PP cooperation-partneship model in your country?

Please choose **only one** of the following:

○ Is sufficient

○ Needs to be improved



Prevention

Do you follow any guideline(s) to prevent the use of internet by terrorists?

Please choose **only one** of the following:

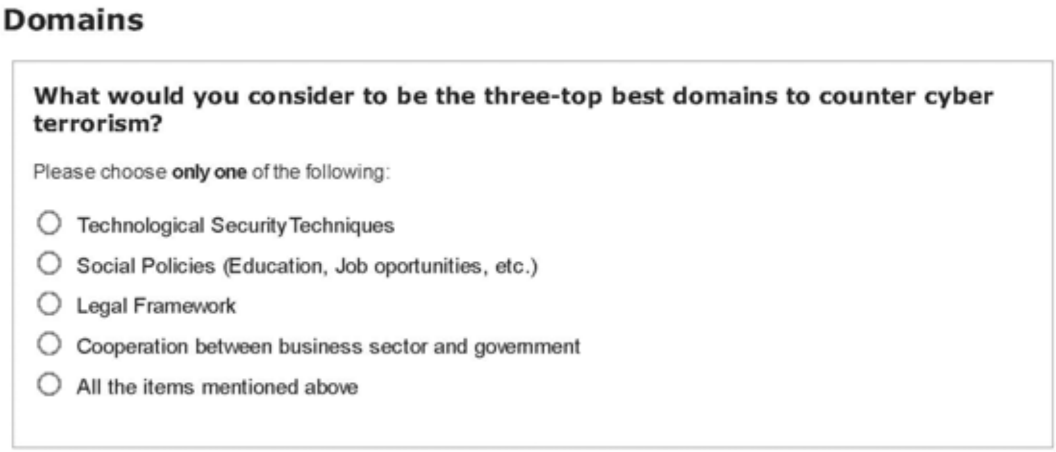
○ Yes

○ No

If yes. which one?

Only answer this question if the following conditions are met:
Answer was 'Yes' at question '25 [PreventTerr1]' (Do you follow any guideline(s) to prevent the use of internet by terrorists?)

Please write your answer here:



Domains

What would you consider to be the three-top best domains to counter cyber terrorism?

Please choose **only one** of the following:

○ Technological Security Techniques

○ Social Policies (Education, Job oportunities, etc.)

○ Legal Framework

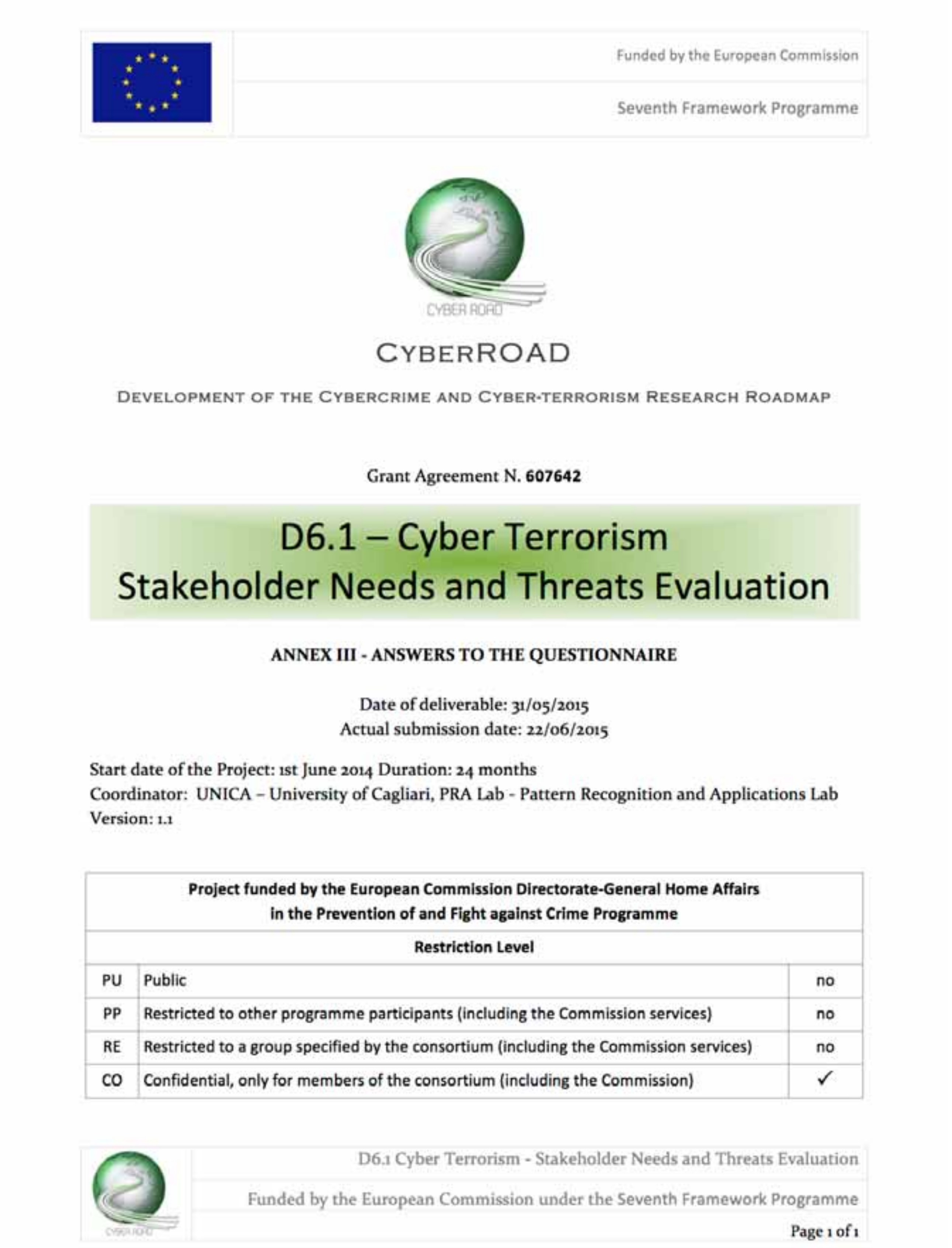
○ Cooperation between business sector and government

○ All the items mentioned above

We thank you very much for your co-operation and participation.

Submit your survey.
Thank you for completing this survey.

15 ANNEX III: CYBERROAD D6 1 – ANSWERS TO TH QUESTIONNAIRE



Funded by the European Commission

Seventh Framework Programme

CYBER ROAD

CYBERROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

D6.1 – Cyber Terrorism Stakeholder Needs and Threats Evaluation

ANNEX III - ANSWERS TO THE QUESTIONNAIRE

Date of deliverable: 31/05/2015
Actual submission date: 22/06/2015

Start date of the Project: 1st June 2014 Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 1.1

Project funded by the European Commission Directorate-General Home Affairs in the Prevention of and Fight against Crime Programme		
Restriction Level		
PU	Public	no
PP	Restricted to other programme participants (including the Commission services)	no
RE	Restricted to a group specified by the consortium (including the Commission services)	no
CO	Confidential, only for members of the consortium (including the Commission)	✓

D6.1 Cyber Terrorism - Stakeholder Needs and Threats Evaluation

Funded by the European Commission under the Seventh Framework Programme

Page 1 of 1

Results

Survey 647556

Number of records in this query:	68
Total records in survey:	68
Percentage of total:	100.00%

Field summary for dataidentification1

Organization/Company name

Answer	Count	Percentage
Answer	24	42.86%
No answer	32	57.14%

ID	Response
4	Infraestruturas de Portugal
3	Infraestruturas de Portugal, SA
5	Autoridade Tributária e Aduaneira
7	Núcleo de Informática Forense-Autoridade Tributária e Aduaneira
9	Polícia Judiciária
15	Ministry of Foreign Affairs
23	Maritime Police
25	Mossos d'Esquadra-Catalan Police
26	Immigration and Borders Service
30	Federal Police Belgium
31	DGS- National Plan For Mental Health
33	National Guard
37	Counter Terrorism Unit of the Grand-Ducal Police (Luxembourg)
41	GNR
42	Guarda Nacional Republicana
47	UNODC
51	Spanish National Police
53	Cefriel
54	INDRA
56	CEFRIEL
62	Vitrociset
63	Hellenic MOD/Cyber Defence Directorate
67	Counter Terrorism Centre
69	Royal Gibraltar Police

Field summary for dataidentification2

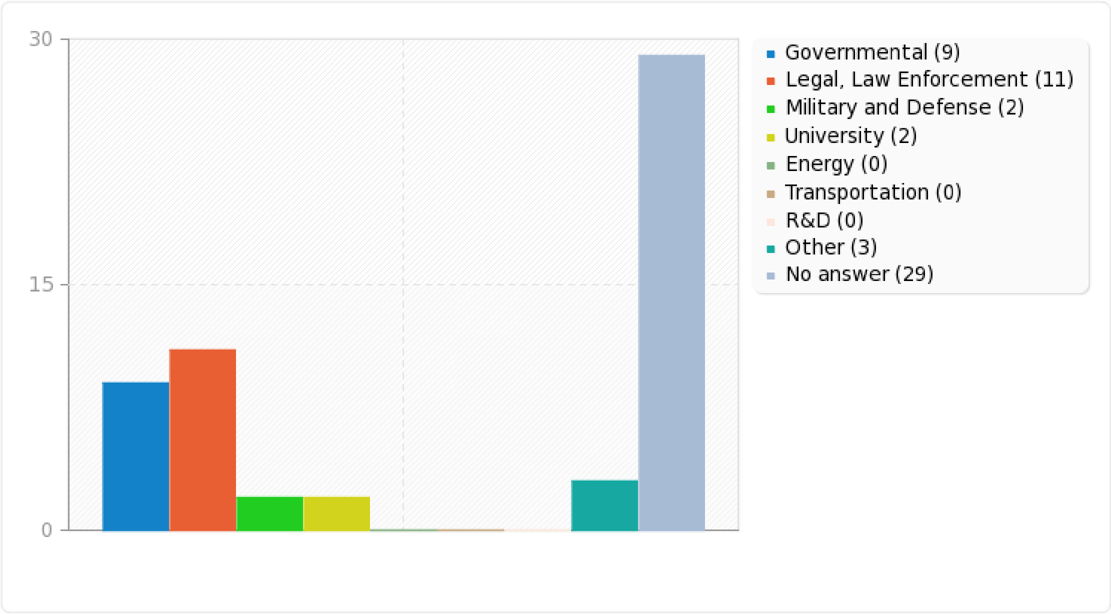
Organization Type

Answer	Count	Percentage
Governmental (2)	9	16.07%
Legal, Law Enforcement (3)	11	19.64%
Military and Defense (9)	2	3.57%
University (4)	2	3.57%
Energy (5)	0	0.00%
Transportation (6)	0	0.00%
R&D (7)	0	0.00%
Other	3	5.36%
No answer	29	51.79%

ID	Response
29	press
47	International
62	Industry (ICT)

Field summary for dataidentification2

Organization Type



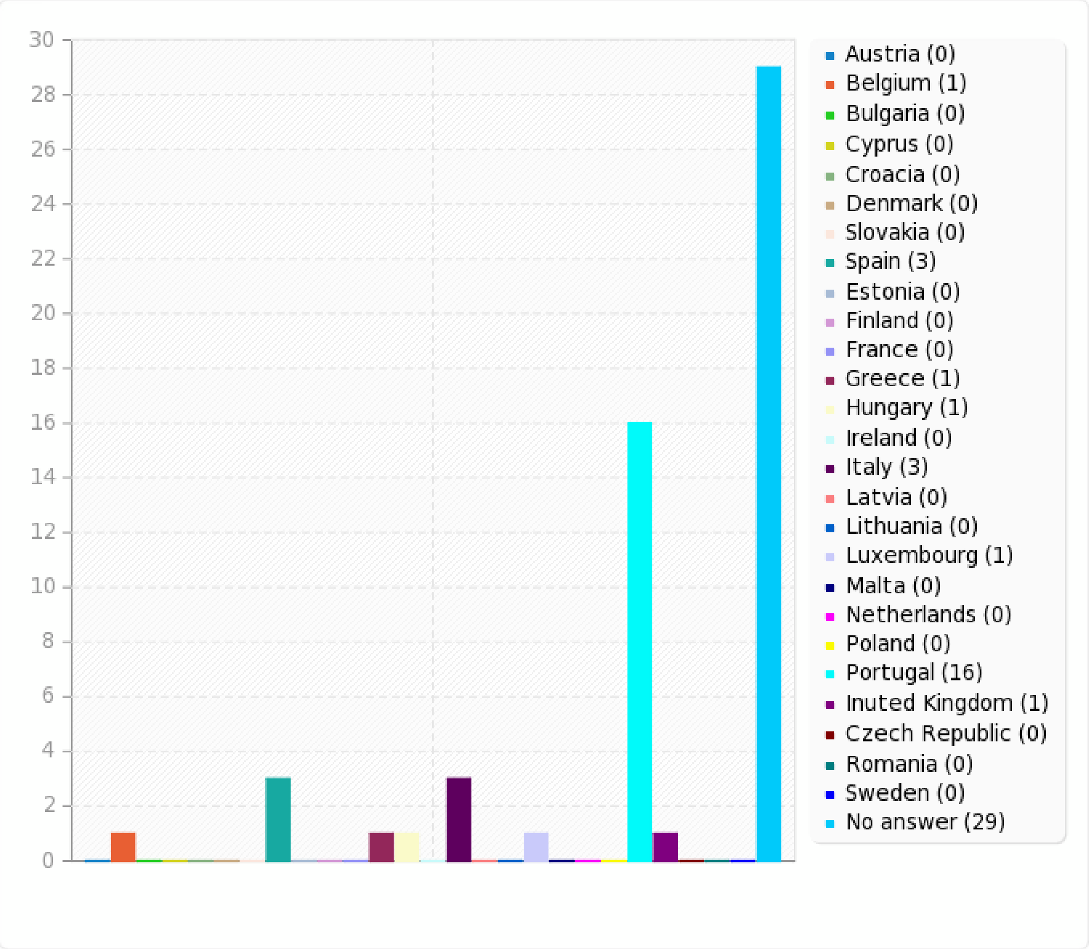
Field summary for dataidentification3

Country

Answer	Count	Percentage
Austria (L001)	0	0.00%
Belgium (L002)	1	1.79%
Bulgaria (L003)	0	0.00%
Cyprus (L004)	0	0.00%
Croacia (L005)	0	0.00%
Denmark (L006)	0	0.00%
Slovakia (L007)	0	0.00%
Spain (L008)	3	5.36%
Estonia (L009)	0	0.00%
Finland (L010)	0	0.00%
France (L011)	0	0.00%
Greece (L012)	1	1.79%
Hungary (L013)	1	1.79%
Ireland (L014)	0	0.00%
Italy (L015)	3	5.36%
Latvia (L016)	0	0.00%
Lithuania (L017)	0	0.00%
Luxembourg (L018)	1	1.79%
Malta (L019)	0	0.00%
Netherlands (L020)	0	0.00%
Poland (L021)	0	0.00%
Portugal (L022)	16	28.57%
Inuted Kingdom (L023)	1	1.79%
Czech Republic (L024)	0	0.00%
Romania (L025)	0	0.00%
Sweden (L026)	0	0.00%
No answer	29	51.79%

Field summary for dataidentification3

Country



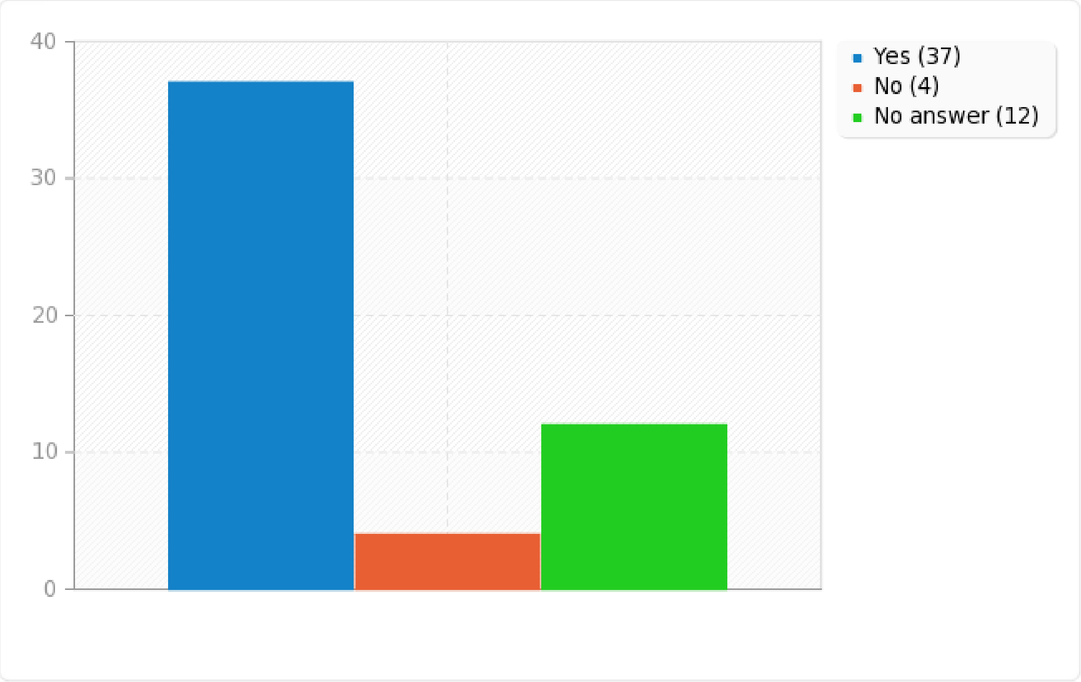
Field summary for Concept2

Before answering and for the purpose of the questionnaire, a differentiation must be considered on the concept of cyberterrorism. It comprises: “Cyberterrorist acts” the possibility to use electronic means/information technologies to perpetrate attacks, whose dimension threaten human lives, may cause huge damage, challenging and jeopardizing the State security based on democracy and the rule of law. Such attacks have a political-ideological and/or religious motivation; “Cyberattacks perpetrated by terrorists” such as defacement of sites, disturbing the regular functionality of services as TV Channels and other infrastructures. These attacks may have a great impact on society holding the potential to disturb the organization of the societies; “Use of Internet by terrorists” – the use of Internet / Information technologies by terrorists for terrorist purposes like propaganda, financing, communication, recruitment, plotting, indoctrination, radicalization etc..... Do you agree with the above definitions of cyberterrorism?

Answer	Count	Percentage
Yes (Y)	37	69.81%
No (N)	4	7.55%
No answer	12	22.64%

Field summary for Concept2

Before answering and for the purpose of the questionnaire, a differentiation must be considered on the concept of cyberterrorism. It comprises: “Cyberterrorist acts” the possibility to use electronic means/information technologies to perpetrate attacks, whose dimension threaten human lives, may cause huge damage, challenging and jeopardizing the State security based on democracy and the rule of law. Such attacks have a political-ideological and/or religious motivation; “Cyberattacks perpetrated by terrorists” such as defacement of sites, disturbing the regular functionality of services as TV Channels and



Field summary for Concept3

If you don`t agree

Answer	Count	Percentage
Answer	2	40.00%
No answer	3	60.00%

ID	Response
15	The definition of cyberterrorist acts should also include a reference to ethnic motivations. The definition of cyberattacks is not adequately develloped. We suggest the following sentence:"...disturbing the regular functionality of public and private organisations, services and infrastructures..."
25	First definition: I would change the concept of"Cyberterrorist acts" for the concept of "Cyberterrorist Threat". I'm agree with the other definitions.

Field summary for Legal1

How does your legal system pursue cyberterrorism?

Answer	Count	Percentage
Answer	18	45.00%
No answer	22	55.00%

ID	Response
4	Do not know
3	.
5	police
9	With a special Rule of Law (legal framework) for the terrorists acts, implementing EU recomendations
16	The portuguese legal system seems to be comprehensive regarding the prevention anf fight against terrorism and cyberterrorism. Law 52/203 and Law 109/2009 apply.
19	There is a special force designed to investigate these acts located at the Judicary Police under the control of the Ministry of Justice. Prosecutors and judges have the power to initiate and conduct the police investigations and bring the offenders to court
30	In the penal code there are some articles that can be used for this topic
31	I think it is security agencies
41	Our legal system pursue the cyberterrorism with de National Strategy in the combat against terrorism.
42	Our legal pursue the cyberterrorism with the National Strategy of combat against terrorism. Aditionally there is the Law nº52/2003, 22 Agoust - Combat of Terrorism and the Penal Code
51	Spanish penal law considers some specific behaviours related to cyberterrorism: - acts to praise terrorist organizations on the Internet, - attacks against computer systems
53	
54	N/A
56	jut applying the existing EU laws
62	Recently, the Italian Government passed a comprehensive bill against terrorist activities, including those perpetrated online. Aggravated penalties are applied for incitement to terrorism through computers and telematics, and against proselytism and radicalization. Website used for terroristic propaganda will be black-listed, monitored and, if necessary, shutted down, under the order of the competent Court.
63	Similar to "common" terrorism. Since there are some gaps in our national legislation about cyberspace, cyber-terrorism isn't addressed individually so far.
67	Cyberterrorist act, and cyberattack is penalized by the Hungarian Penal Code.
69	Cyberterrorism laws are currently being reviewed (draft)

Field summary for Legal2

What are the challenges, constraints or trade-offs (e.g. privacy aspects, legal framework) you consider pursuing the problem of cyberterrorism?

Answer	Count	Percentage
Answer	15	37.50%
No answer	25	62.50%

ID	Response
4	All the usual questions regarding security in a general way; mainly privacy and loss of efficiency.
3	.
5	privacy, legal aspects
9	The legal restrictions concerning privacy protection and human rights are not compatible with the urgency needed for colecting evidence in the Internet or informations systems.
16	In our opinion some constrains exist, like the assumption of competence of the police forces responsible solely for public order in áreas which are of the exclusive competence of the Criminal Police (Polícia Judiciária). This behavior could jeopardize all the efforts in preventig and fighting terrorism and cyberterrorism.
19	I think the principal challenge is being able to communicate in proper time to other police forces of other countries the suspicious so that an effective action can be taken, since the possibilities of fleding to other countries are quite large with our EU free border system
30	Privacy aspects in one thing but more important is that the "cyber terrorist" are always two steps in advance because creating law is a long procedure. So once the law is there it is already "old" and not functional any more
31	lake of Public awerness and discussion of concepts,risks, legal framework, etc. Lake of clear discussion on security issues by governemental agencies Lake of support to specialist in the field, to change knowledge and take action
41	The necessity to create special units where the human resource have the right education and traing; Have the adequate equipments to gather information; a international common legal framework;The various security forces adopt the same safety cyberprevention plan for citizen
42	It is necessary to create special units in this area with adequate human resouces wich must have the right education and trainning in this field. Aditionally its necessary that this units must have adequate and special equipments in the area of forensics and in the domain off gathering and in analysing of information in cyberspace. It´s also fundamental a common international framework. Finally there must be more cooperation between all the police forces (National and International)
51	Legal framework is not agile enough to adapt itself to the new strategies and techniques of digital terrorists. Another relevant issue is the inherently cross-border nature of the Internet which demands a very strong international cooperation.
54	The main constraint is the protection of privacy by the law. For instance the data interception in my country forbids the "Man in the Middle" interception ,even in case of cyberterrorism
62	Privacy is the major issue. Considering mass online surveillance as an investigation tool could hugely impact on individuals' privacy. Previous intelligence and case-by-case investigation must be considered to mitigate risks related to privacy violation.
63	The greatest challenge is attribution. Cyber attacks and impacts can be measured effectively. However the greatest issue is how/if we can reliably attribute any attack and then procced to further actions
69	Human and IT resources

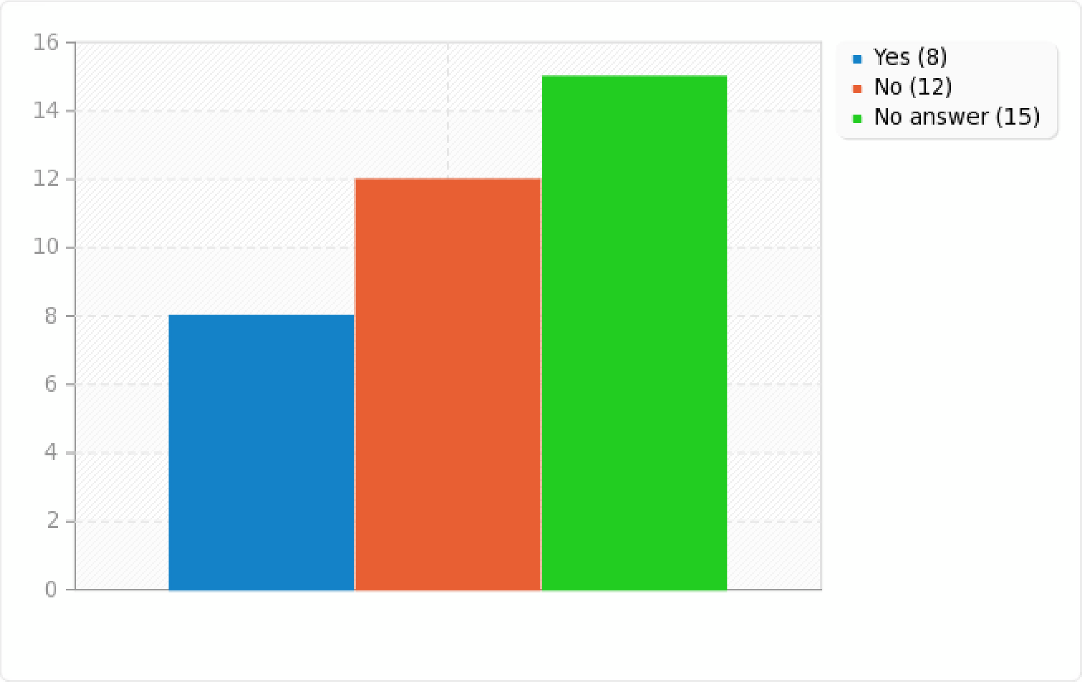
Field summary for Guidelines1

Does your organization provide a guideline of best practices (program, policies, and procedures) on how to deal with information related to security threats?

Answer	Count	Percentage
Yes (Y)	8	22.86%
No (N)	12	34.29%
No answer	15	42.86%

Field summary for Guidelines1

Does your organization provide a guideline of best practices (program, policies, and procedures) on how to deal with information related to security threats?



Field summary for Guidelines2

If yes, which one?

Answer	Count	Percentage
Answer	7	77.78%
No answer	2	22.22%

ID	Response
25	We have a
42	Regulation in the area of security policies, Behavioral rules and measures.
51	awareness measures, security policies, behavioral rules
54	INDRA has deployed tools in security fields like: anomaly detection, pattern analysis, malware analysis, blacklists, cloud security, data loss preventions. Non-technical aspects include: ISO 27001 cetification, policies, awareness measures and others.
56	derived from best practices in literature about crime and threat preventions. Them are more related to avoid exploits thant cyber crime in general.
62	The company is UNI-ISO 27001 compliant, so it could manage sensitive and classified information regarding its customers and programmes.
63	Best practices for user awareness, computer system hardening, safe browsing, email handling.

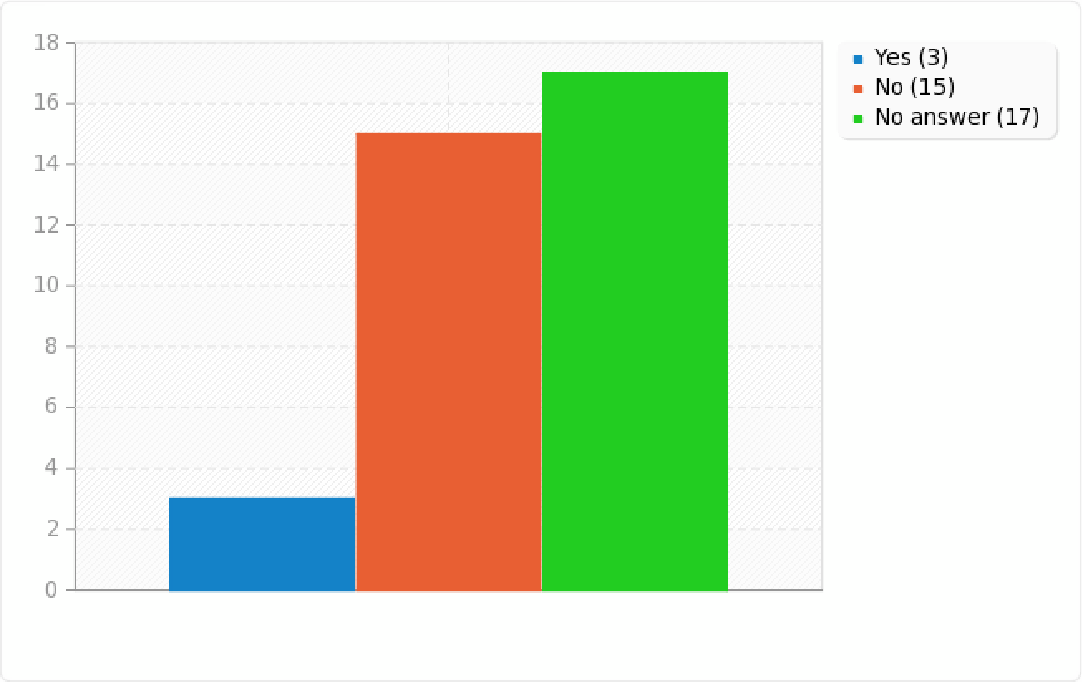
Field summary for Guidelines3

Does your organization provide a guideline of best practices (programs, policies, and procedures) on how to specifically approach the threat posed by cyberterrorism?

Answer	Count	Percentage
Yes (Y)	3	8.57%
No (N)	15	42.86%
No answer	17	48.57%

Field summary for Guidelines3

Does your organization provide a guideline of best practices (programs, policies, and procedures) on how to specifically approach the threat posed by cyberterrorism?



Field summary for Guidelines4

If yes, which one?

Answer	Count	Percentage
Answer	2	50.00%
No answer	2	50.00%

ID	Response
42	Data loss prevention. We are ending Security Policies.
54	INDRA has deployed tools in security fields like: anomaly detection, pattern analysis, malware analysis, blacklists, cloud security, data loss preventions. Non-technical aspects include: ISO 27001 cetification, policies, awareness measures and others.

Field summary for BP1

Please indicate only the 3 best practices to counter cyberterrorism.

Answer	Count	Percentage
Answer	5	55.56%
No answer	4	44.44%

ID	Response
42	Cooperation and eficient Coordination between Security Forces; Exange of information and a efective risk management.
51	- Enhancement of international cooperation - Adapting legal framework to fight against cyberterrorism - Enhancement of law enforcement capabilities to fight against cyberterrorism
54	1.-Situational Awareness: deploy systems to identify the state of security across the network 2.-Software Security Assurance 3.-Security Training
62	1- Prevent and suppress combating terrorist financing; 2- Improving legal practice and law enforcement (in order to prevent the commission of terrorist acts); 3- Information-sharing and cooperation (at national and international level)
63	Cyber Intelligence - info gathering. Cyber defence in depth. Synergies and collaboration with other stakeholders.

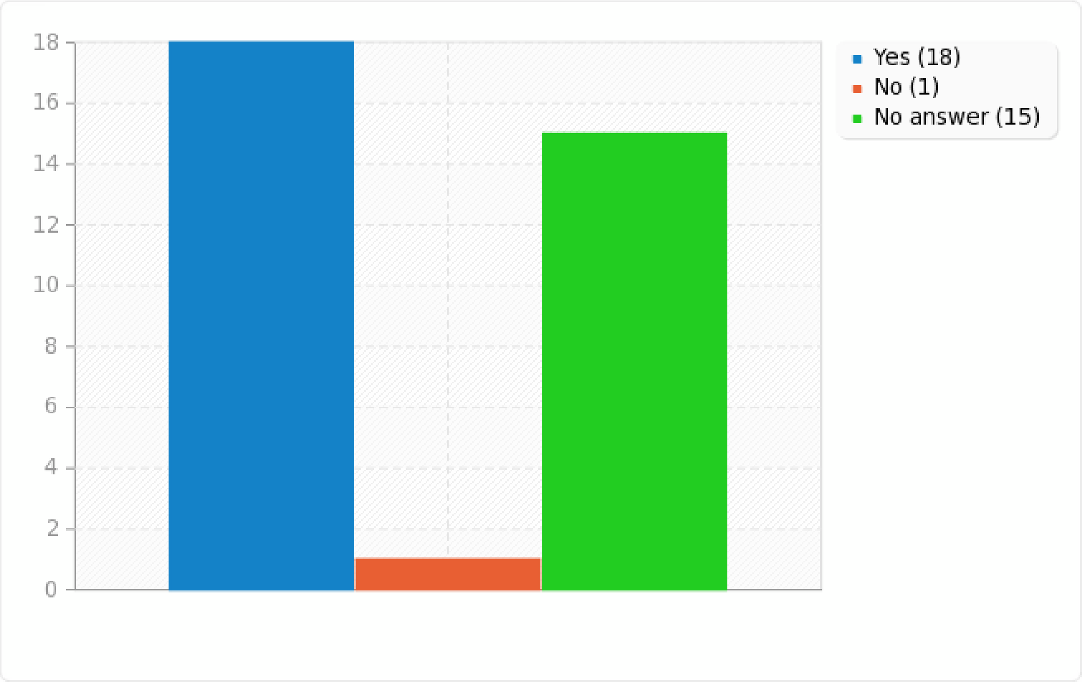
Field summary for BP2

Do you consider that there is a need to increase the current sharing of best practices among teams working to counter cyberterrorism?

Answer	Count	Percentage
Yes (Y)	18	52.94%
No (N)	1	2.94%
No answer	15	44.12%

Field summary for BP2

Do you consider that there is a need to increase the current sharing of best practices among teams working to counter cyberterrorism?



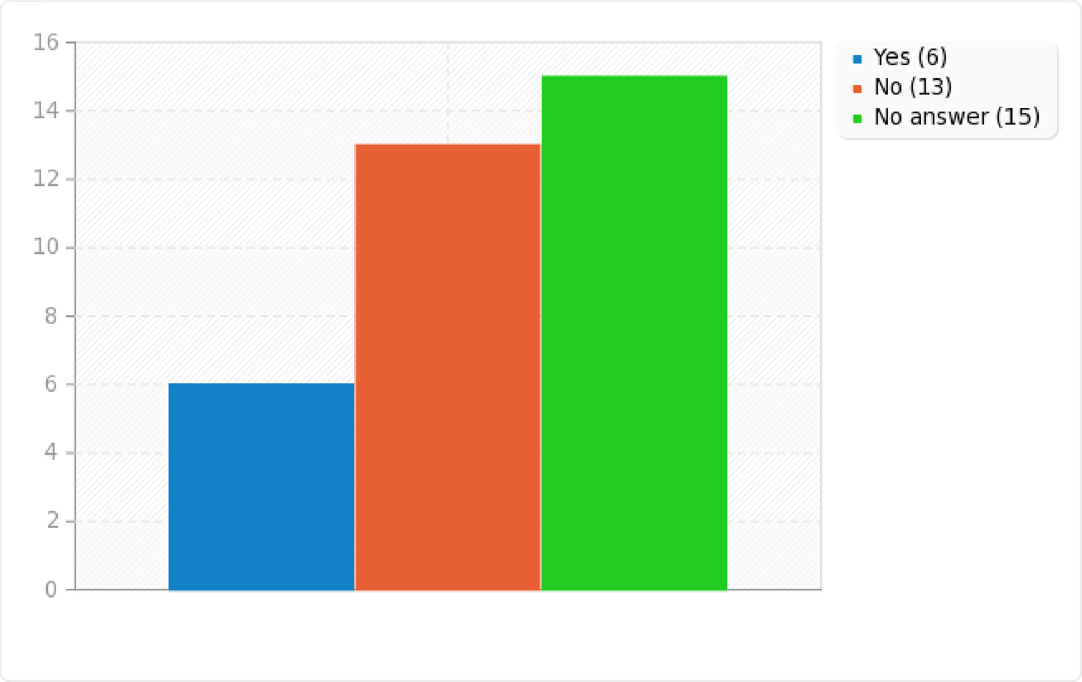
Field summary for PlaneIncR1

Does your organization provide a Plan of Incident Response?

Answer	Count	Percentage
Yes (Y)	6	17.65%
No (N)	13	38.24%
No answer	15	44.12%

Field summary for PlaneIncR1

Does your organization provide a Plan of Incident Response?



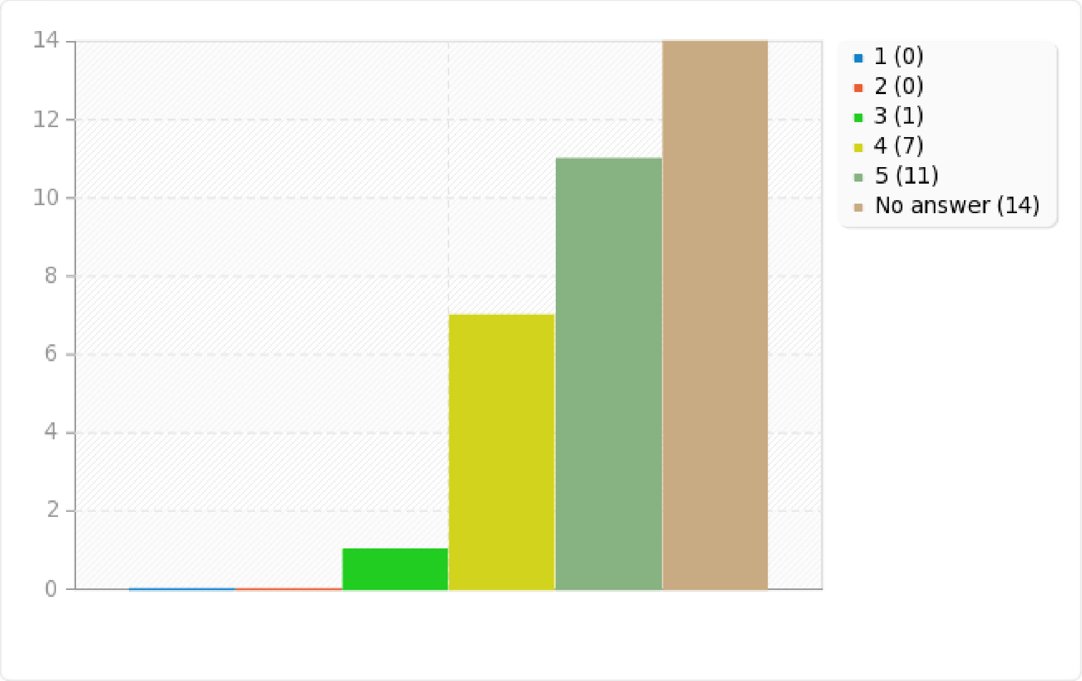
Field summary for DomCyberSec1(1)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Education/Awareness]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	0.00%
2 (2)	0	0.00%	
3 (3)	1	1.85%	1.85%
4 (4)	7	12.96%	
5 (5)	11	20.37%	33.33%
No answer	14	20.59%	
Arithmetic mean	4.53		
Standard deviation	0.61		
Sum (Answers)	19	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec1(1)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Education/Awareness]



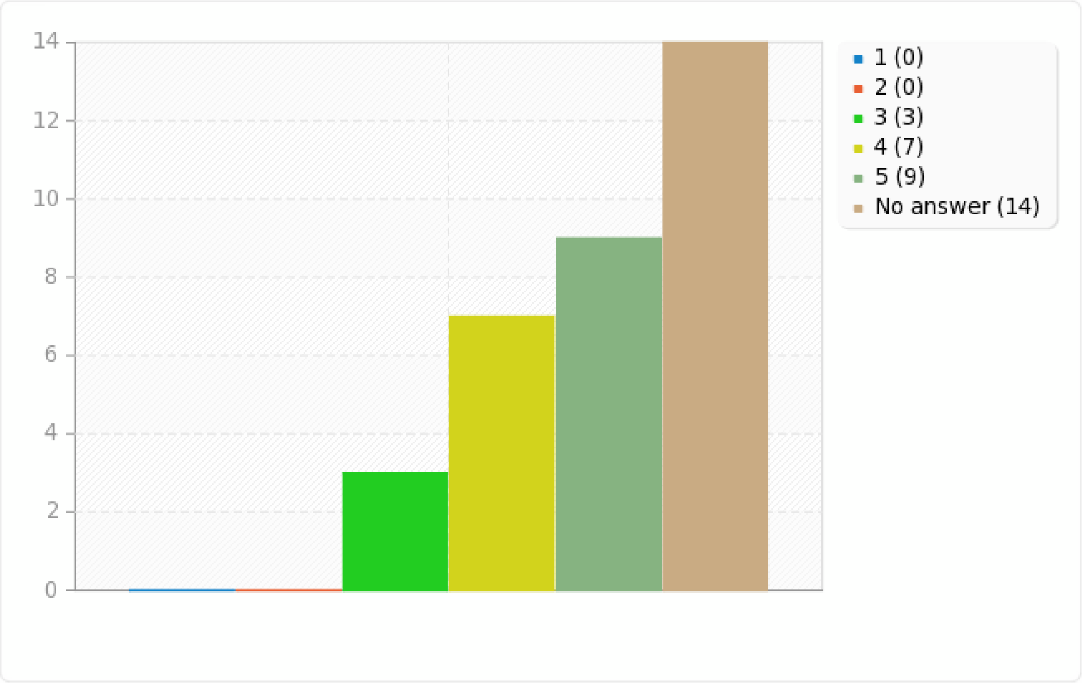
Field summary for DomCyberSec1(2)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [IT & Security Solutions]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	0.00%
2 (2)	0	0.00%	
3 (3)	3	5.56%	5.56%
4 (4)	7	12.96%	
5 (5)	9	16.67%	29.63%
No answer	14	20.59%	
Arithmetic mean	4.32		
Standard deviation	0.75		
Sum (Answers)	19	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec1(2)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [IT & Security Solutions]



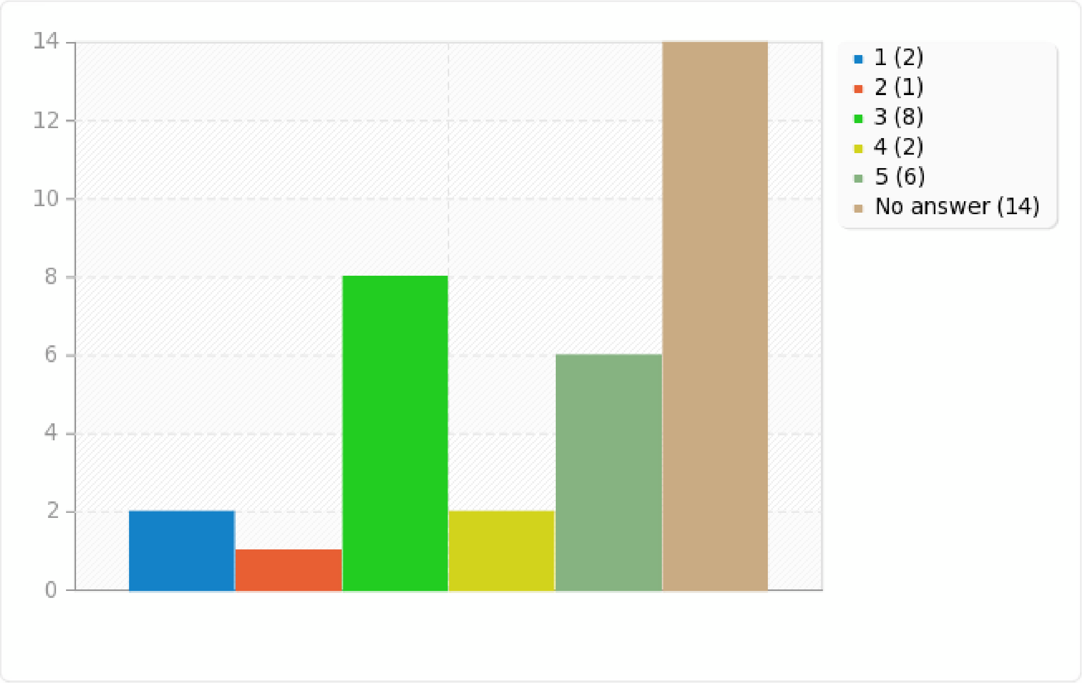
Field summary for DomCyberSec1(3)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Ethical domains research]

Answer	Count	Percentage	Sum
1 (1)	2	3.70%	5.56%
2 (2)	1	1.85%	
3 (3)	8	14.81%	14.81%
4 (4)	2	3.70%	
5 (5)	6	11.11%	14.81%
No answer	14	20.59%	
Arithmetic mean	3.47		
Standard deviation	1.31		
Sum (Answers)	19	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec1(3)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Ethical domains research]



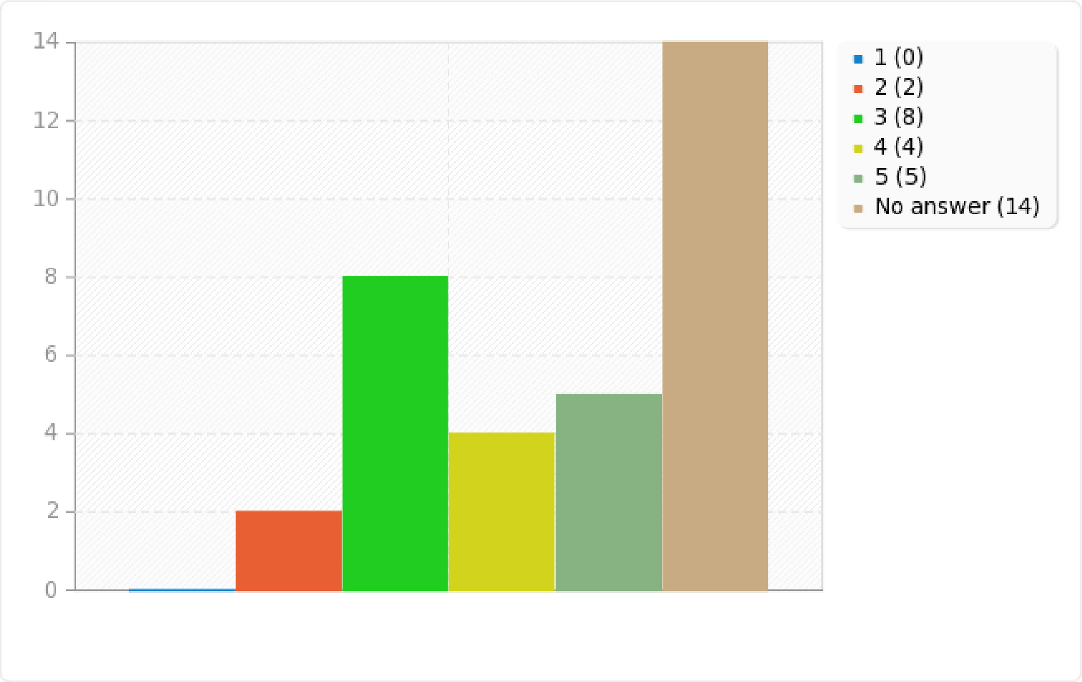
Field summary for DomCyberSec1(4)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Political/Social interventions]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	3.70%
2 (2)	2	3.70%	
3 (3)	8	14.81%	14.81%
4 (4)	4	7.41%	
5 (5)	5	9.26%	16.67%
No answer	14	20.59%	
Arithmetic mean	3.63		
Standard deviation	1.01		
Sum (Answers)	19	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec1(4)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Political/Social interventions]



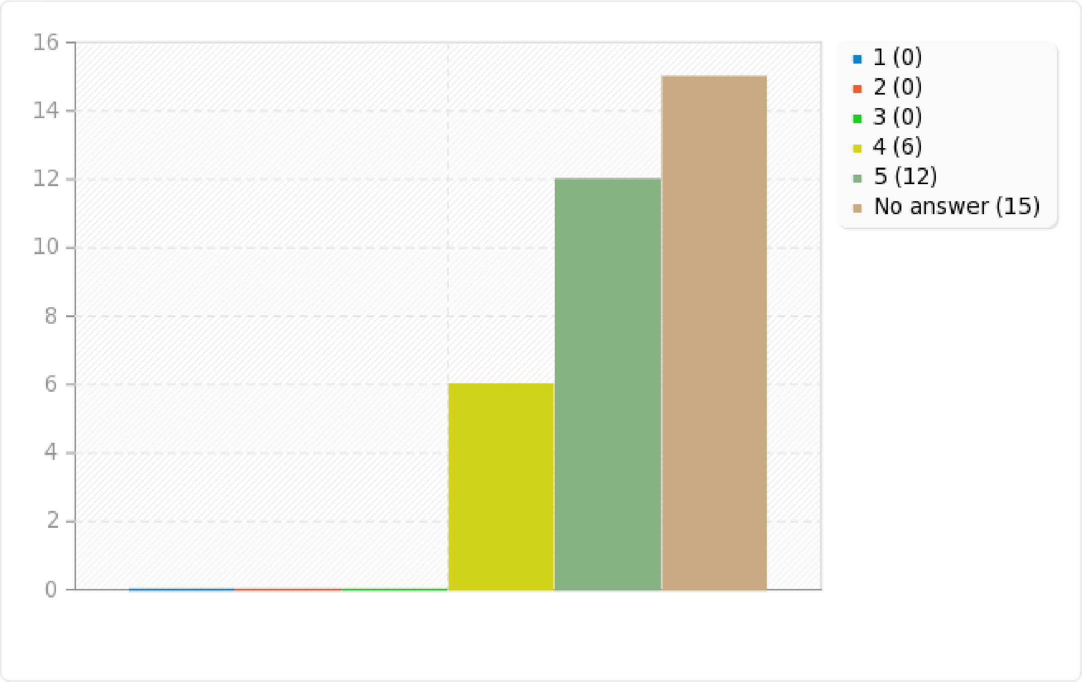
Field summary for DomCyberSec1(5)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Critical infrastructures protection/prevention]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	0.00%
2 (2)	0	0.00%	
3 (3)	0	0.00%	0.00%
4 (4)	6	11.32%	
5 (5)	12	22.64%	33.96%
No answer	15	22.06%	
Arithmetic mean	4.67		
Standard deviation	0.49		
Sum (Answers)	18	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec1(5)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Critical infrastructures protection/prevention]



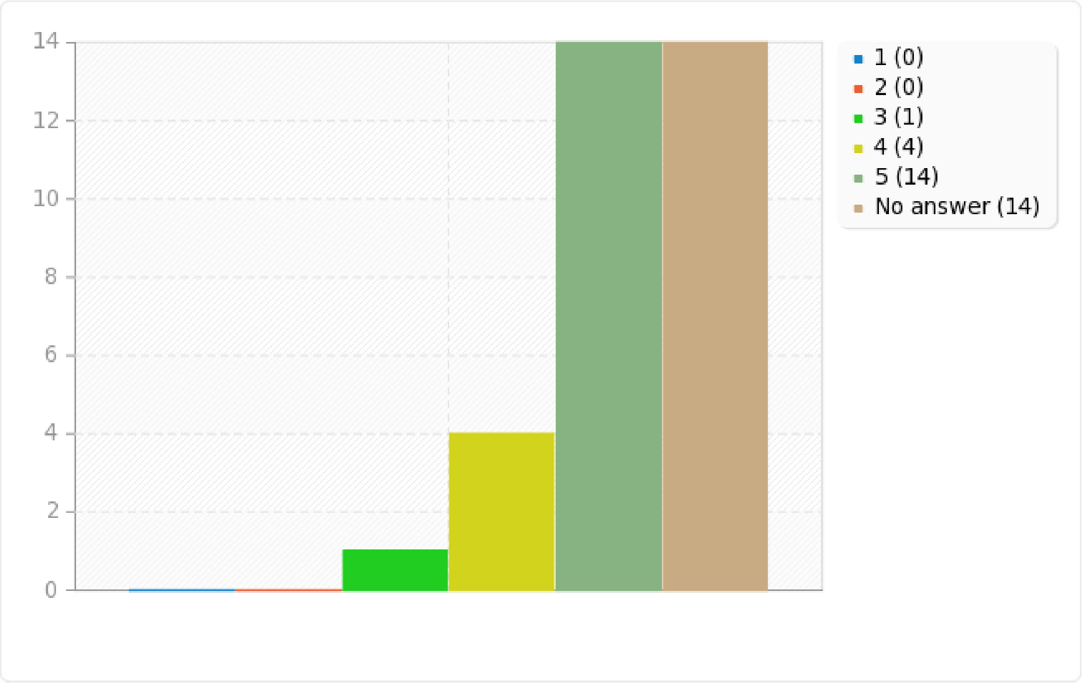
Field summary for DomCyberSec1(6)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [System protection of servers/PCs]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	0.00%
2 (2)	0	0.00%	
3 (3)	1	1.85%	1.85%
4 (4)	4	7.41%	
5 (5)	14	25.93%	33.33%
No answer	14	20.59%	
Arithmetic mean	4.68		
Standard deviation	0.58		
Sum (Answers)	19	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec1(6)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [System protection of servers/PCs]



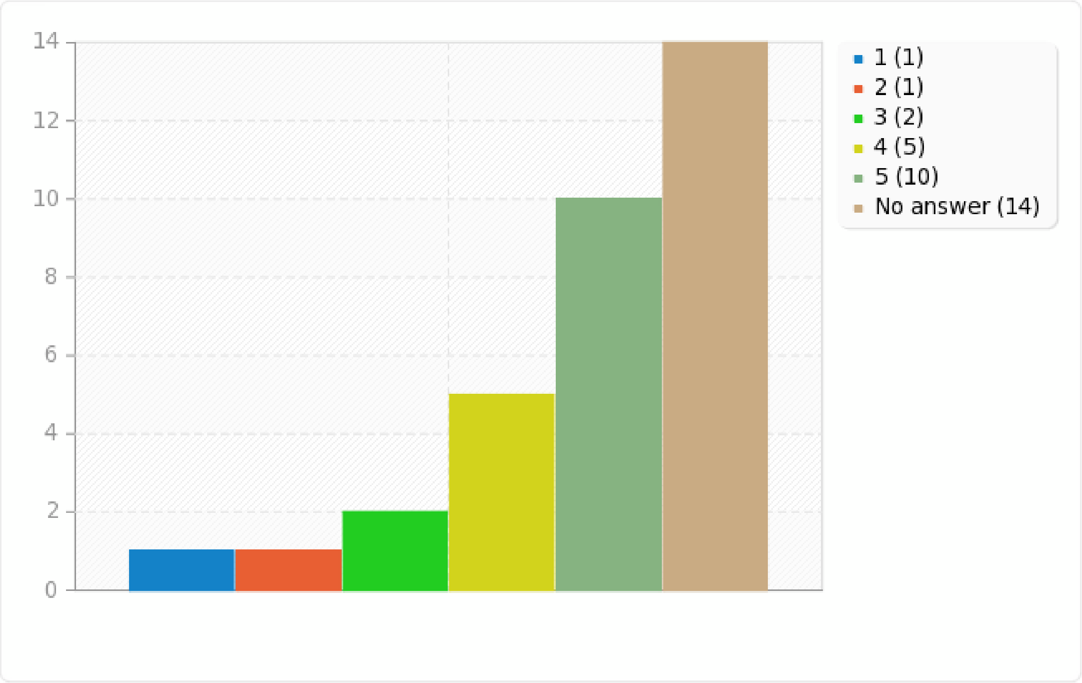
Field summary for DomCyberSec1(7)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Forensic activities enhancement]

Answer	Count	Percentage	Sum
1 (1)	1	1.85%	3.70%
2 (2)	1	1.85%	
3 (3)	2	3.70%	3.70%
4 (4)	5	9.26%	
5 (5)	10	18.52%	27.78%
No answer	14	20.59%	
Arithmetic mean	4.16		
Standard deviation	1.17		
Sum (Answers)	19	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec1(7)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Forensic activities enhancement]



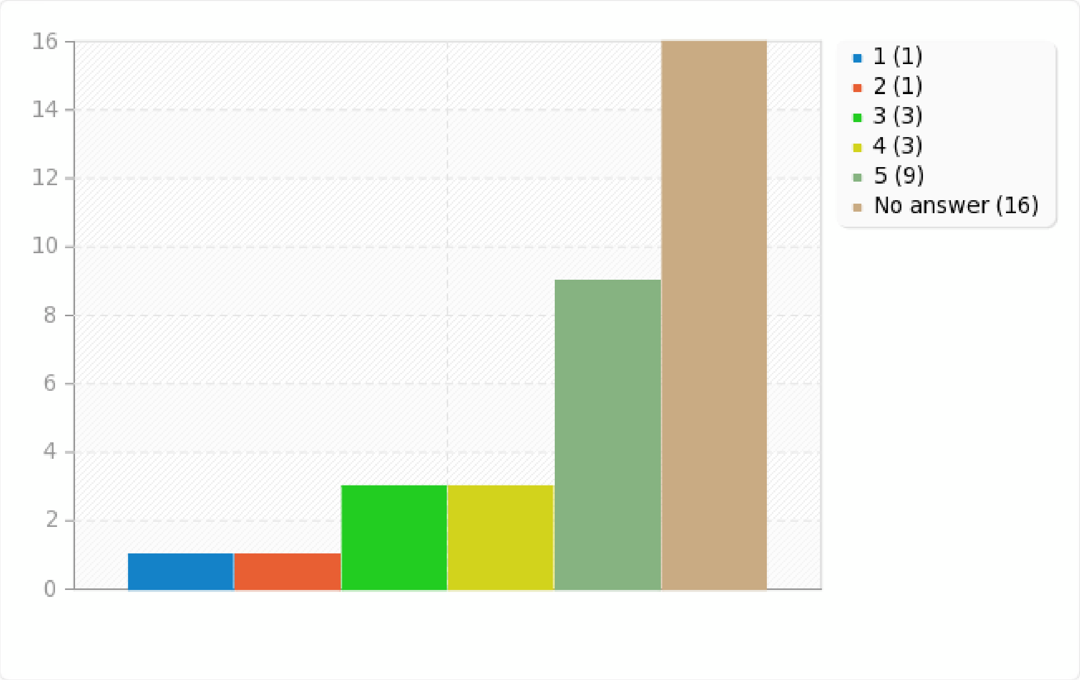
Field summary for DomCyberSec1(8)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Theoretical (cryptography, algorithms)]

Answer	Count	Percentage	Sum
1 (1)	1	1.92%	3.85%
2 (2)	1	1.92%	
3 (3)	3	5.77%	5.77%
4 (4)	3	5.77%	
5 (5)	9	17.31%	23.08%
No answer	16	23.53%	
Arithmetic mean	4.06		
Standard deviation	1.25		
Sum (Answers)	17	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec1(8)

In your opinion, in which domains cybersecurity should be more focused on in order to fight cyberterrorism? [Theoretical (cryptography, algorithms)]



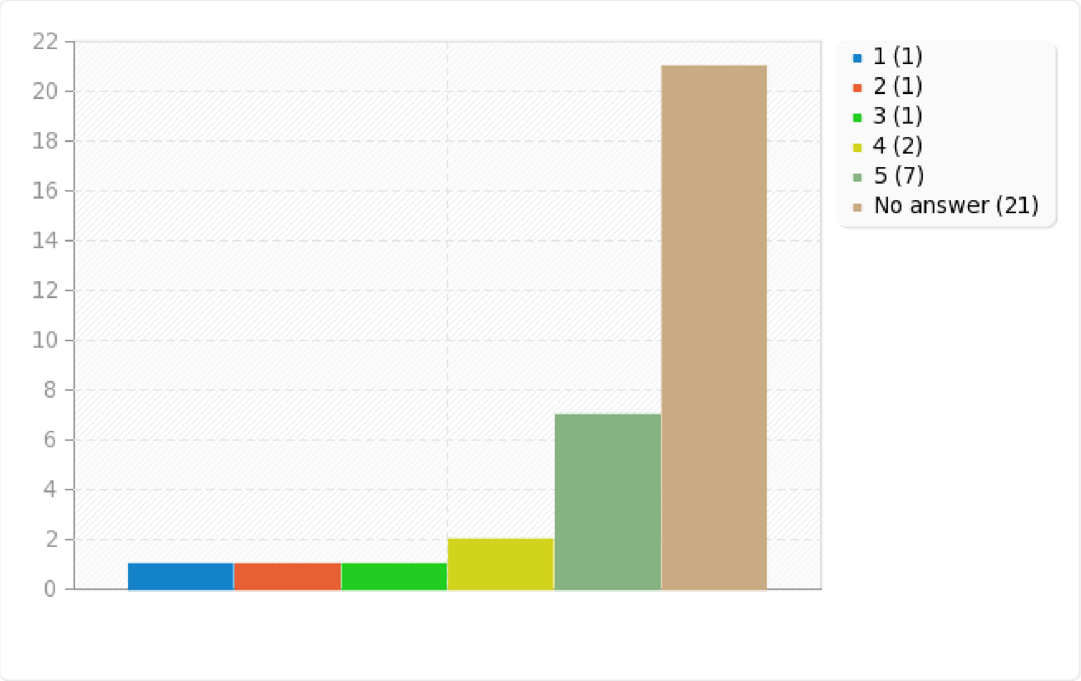
Field summary for DomCyberSec2(SQ001)

What kind of other resources are necessary? [Financial]

Answer	Count	Percentage	Sum
1 (1)	1	2.13%	4.26%
2 (2)	1	2.13%	
3 (3)	1	2.13%	2.13%
4 (4)	2	4.26%	
5 (5)	7	14.89%	19.15%
No answer	21	30.88%	
Arithmetic mean	4.08		
Standard deviation	1.38		
Sum (Answers)	12	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec2(SQ001)

What kind of other resources are necessary? [Financial]



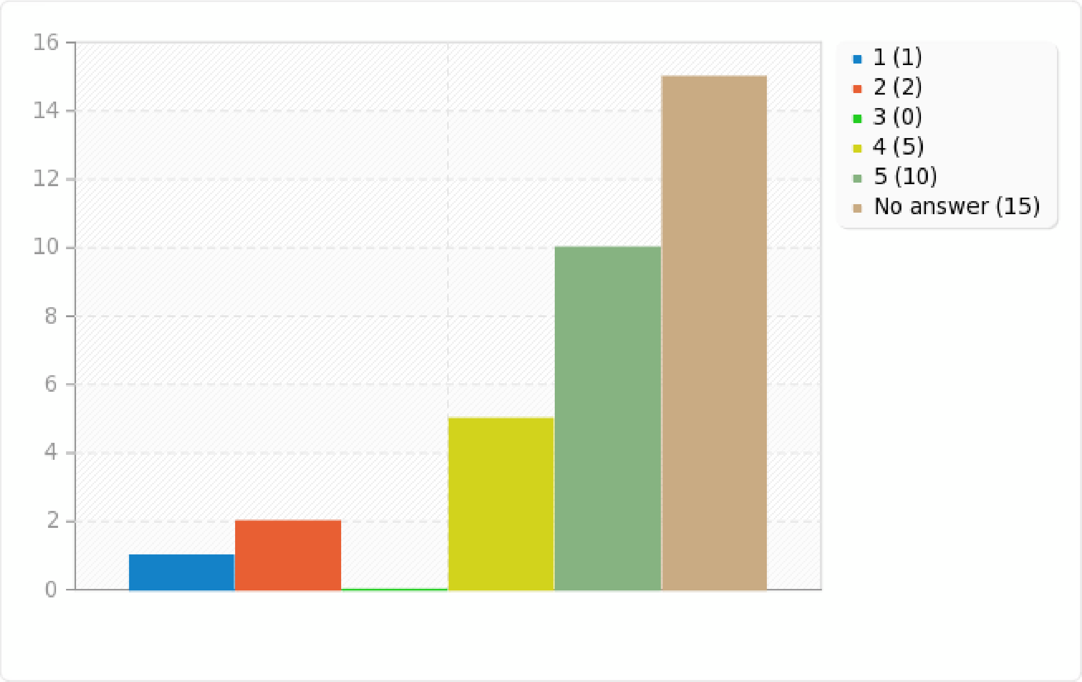
Field summary for DomCyberSec2(1)

What kind of other resources are necessary? [Hardware]

Answer	Count	Percentage	Sum
1 (1)	1	1.89%	5.66%
2 (2)	2	3.77%	
3 (3)	0	0.00%	0.00%
4 (4)	5	9.43%	
5 (5)	10	18.87%	28.30%
No answer	15	22.06%	
Arithmetic mean	4.17		
Standard deviation	1.25		
Sum (Answers)	18	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec2(1)

What kind of other resources are necessary? [Hardware]



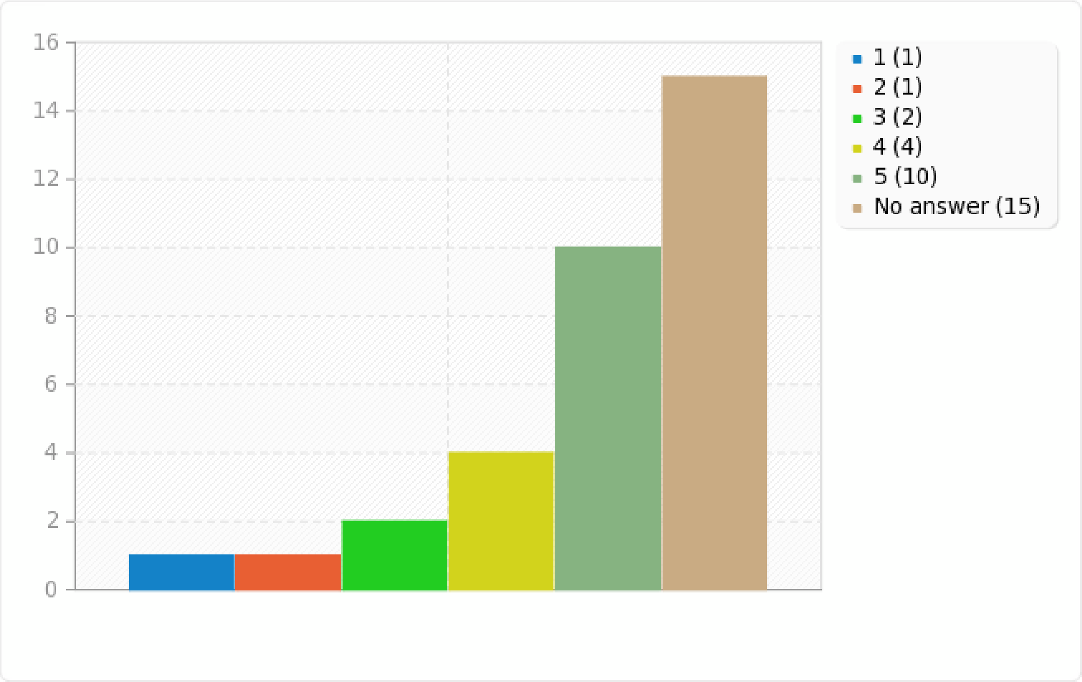
Field summary for DomCyberSec2(2)

What kind of other resources are necessary? [Network]

Answer	Count	Percentage	Sum
1 (1)	1	1.89%	3.77%
2 (2)	1	1.89%	
3 (3)	2	3.77%	3.77%
4 (4)	4	7.55%	
5 (5)	10	18.87%	26.42%
No answer	15	22.06%	
Arithmetic mean	4.17		
Standard deviation	1.2		
Sum (Answers)	18	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec2(2)

What kind of other resources are necessary? [Network]



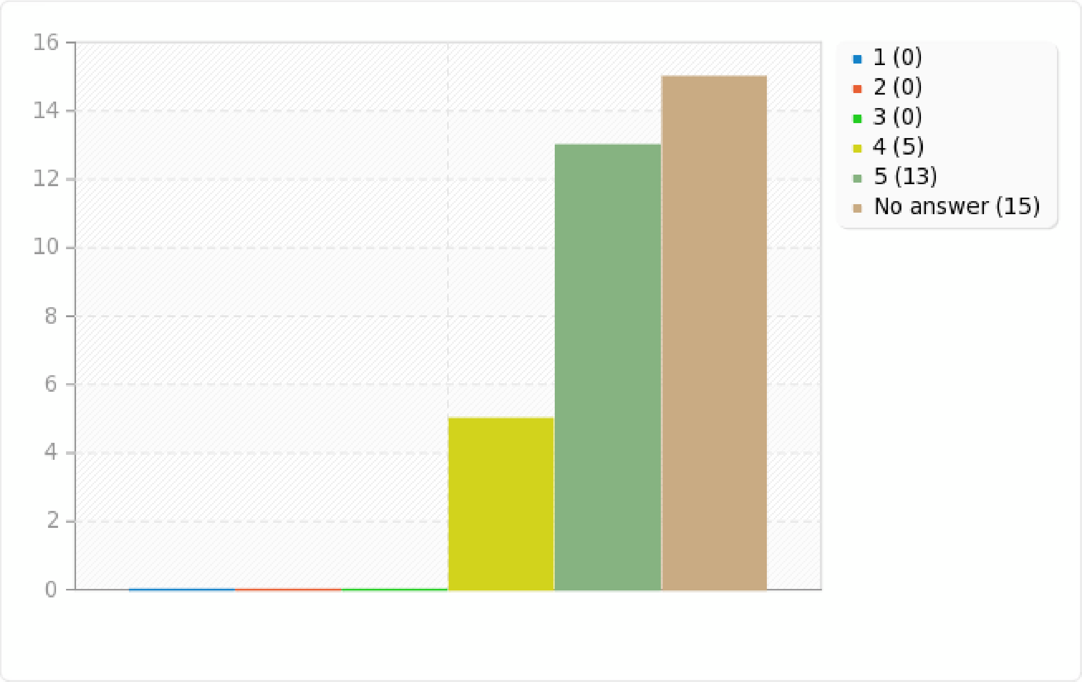
Field summary for DomCyberSec2(3)

What kind of other resources are necessary? [Staff]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	0.00%
2 (2)	0	0.00%	
3 (3)	0	0.00%	0.00%
4 (4)	5	9.43%	
5 (5)	13	24.53%	33.96%
No answer	15	22.06%	
Arithmetic mean	4.72		
Standard deviation	0.46		
Sum (Answers)	18	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec2(3)

What kind of other resources are necessary? [Staff]



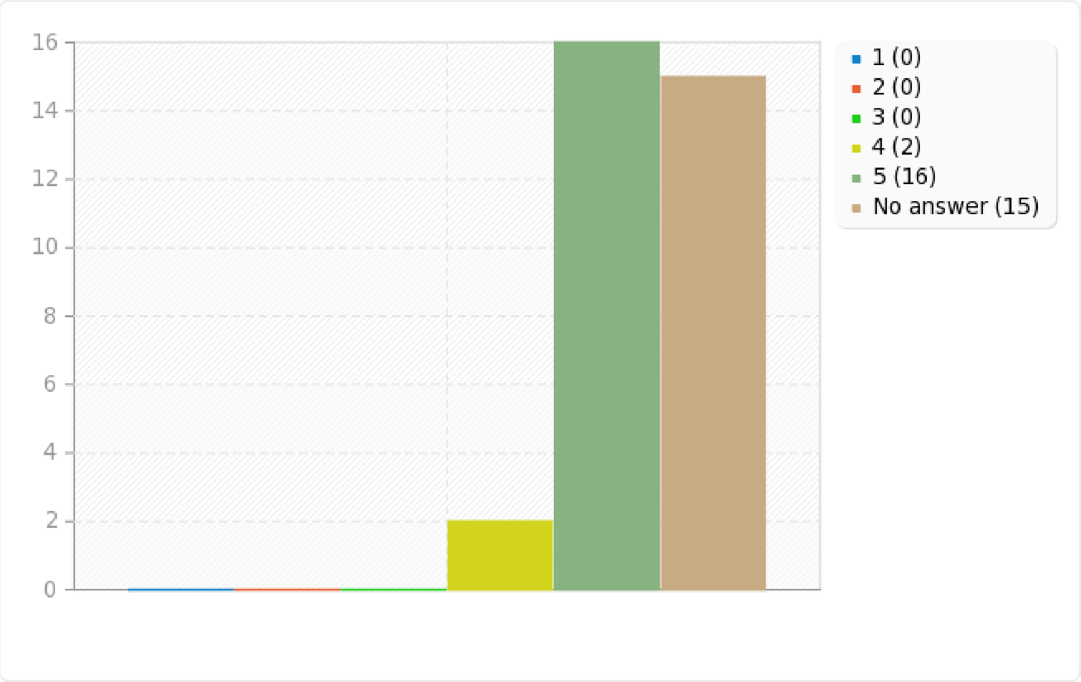
Field summary for DomCyberSec2(4)

What kind of other resources are necessary? [Training]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	0.00%
2 (2)	0	0.00%	
3 (3)	0	0.00%	0.00%
4 (4)	2	3.77%	
5 (5)	16	30.19%	33.96%
No answer	15	22.06%	
Arithmetic mean	4.89		
Standard deviation	0.32		
Sum (Answers)	18	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec2(4)

What kind of other resources are necessary? [Training]



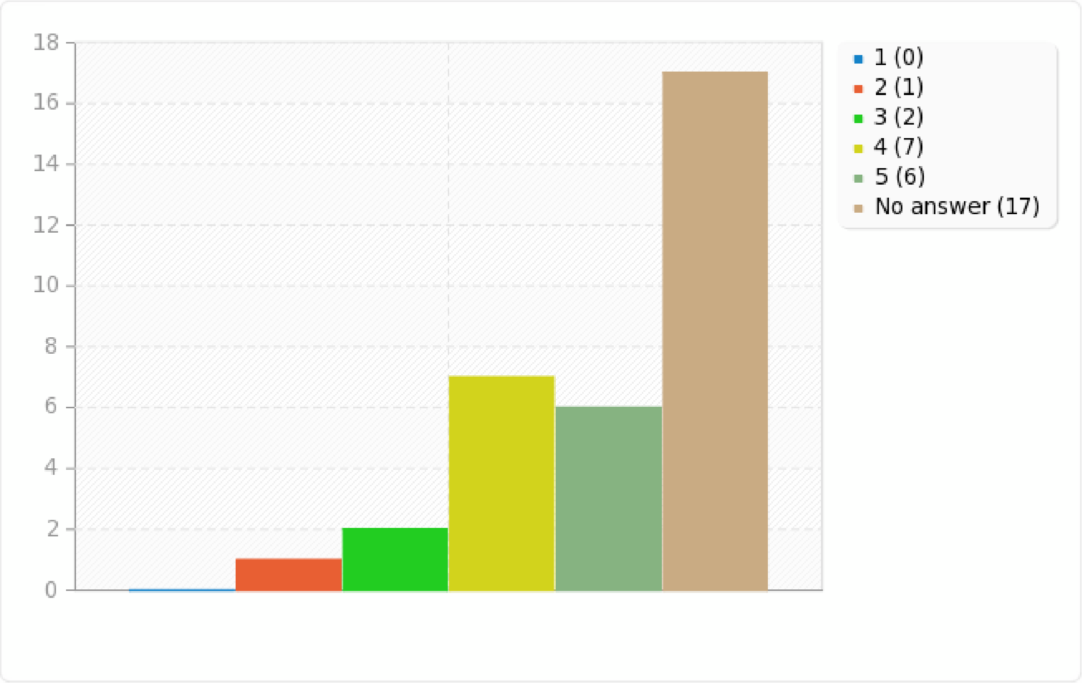
Field summary for DomCyberSec3(1)

What is their cost/effectiveness ratio? [Developing]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	1.96%
2 (2)	1	1.96%	
3 (3)	2	3.92%	3.92%
4 (4)	7	13.73%	
5 (5)	6	11.76%	25.49%
No answer	17	25.00%	
Arithmetic mean	4.13		
Standard deviation	0.89		
Sum (Answers)	16	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec3(1)

What is their cost/effectiveness ratio? [Developing]



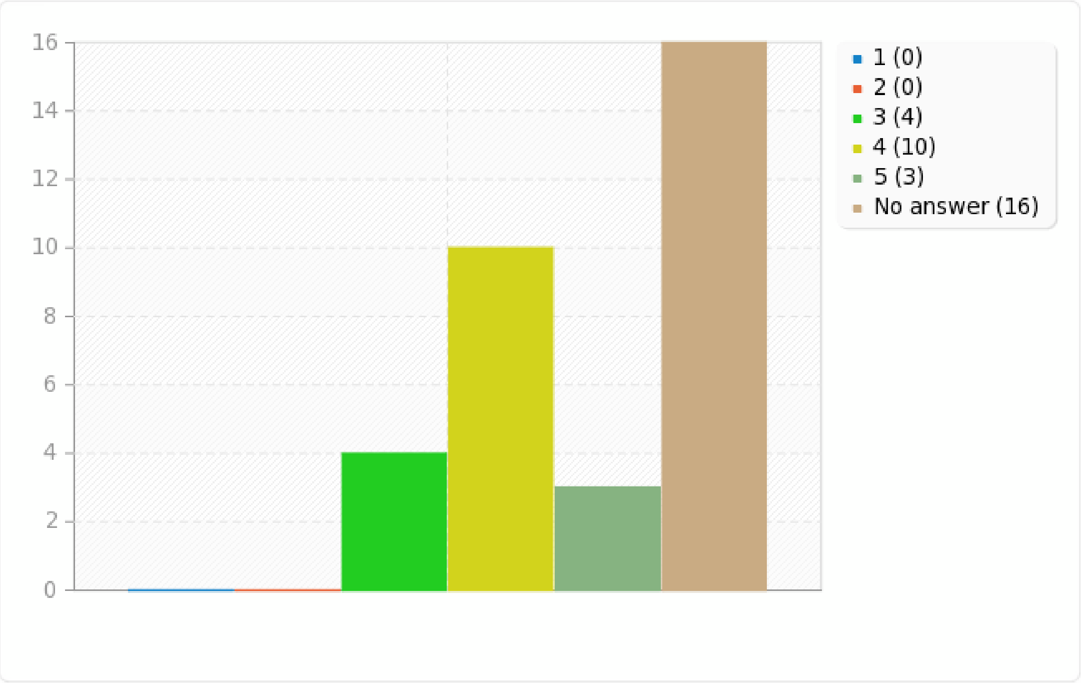
Field summary for DomCyberSec3(2)

What is their cost/effectiveness ratio? [Procurement and operational costs]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	0.00%
2 (2)	0	0.00%	
3 (3)	4	7.69%	7.69%
4 (4)	10	19.23%	
5 (5)	3	5.77%	25.00%
No answer	16	23.53%	
Arithmetic mean	3.94		
Standard deviation	0.66		
Sum (Answers)	17	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec3(2)

What is their cost/effectiveness ratio? [Procurement and operational costs]



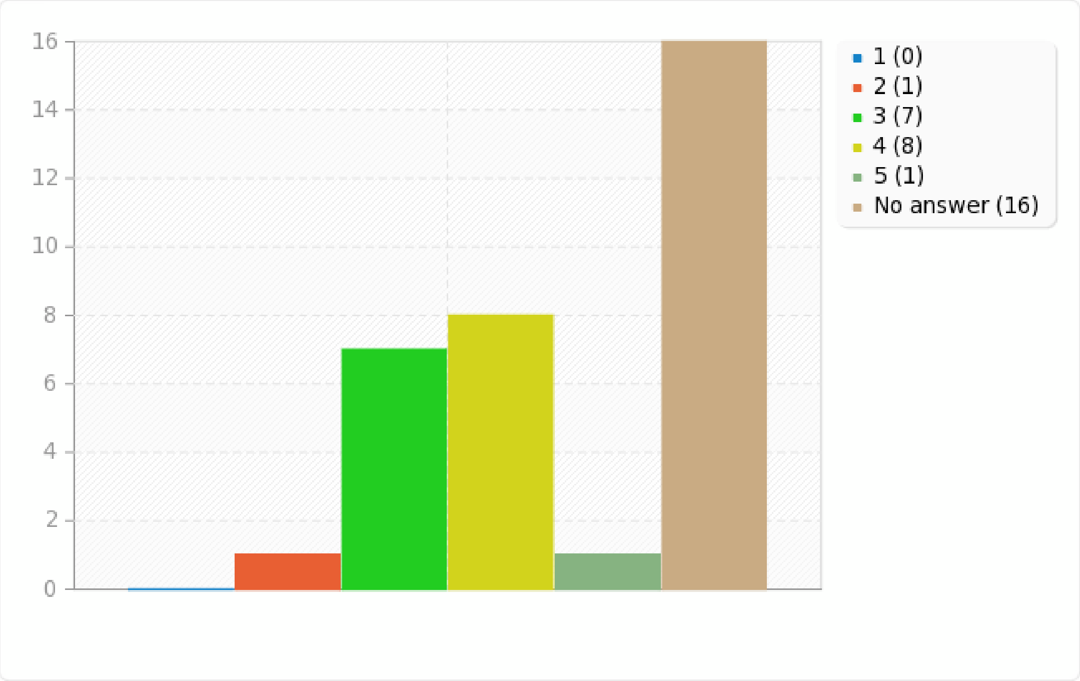
Field summary for DomCyberSec3(3)

What is their cost/effectiveness ratio? [Time consuming]

Answer	**Count**	**Percentage**	**Sum**
1 (1)	0	0.00%	1.92%
2 (2)	1	1.92%	
3 (3)	7	13.46%	13.46%
4 (4)	8	15.38%	
5 (5)	1	1.92%	17.31%
No answer	16	23.53%	
Arithmetic mean	3.53		
Standard deviation	0.72		
Sum (Answers)	17	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec3(3)

What is their cost/effectiveness ratio?   [Time consuming]



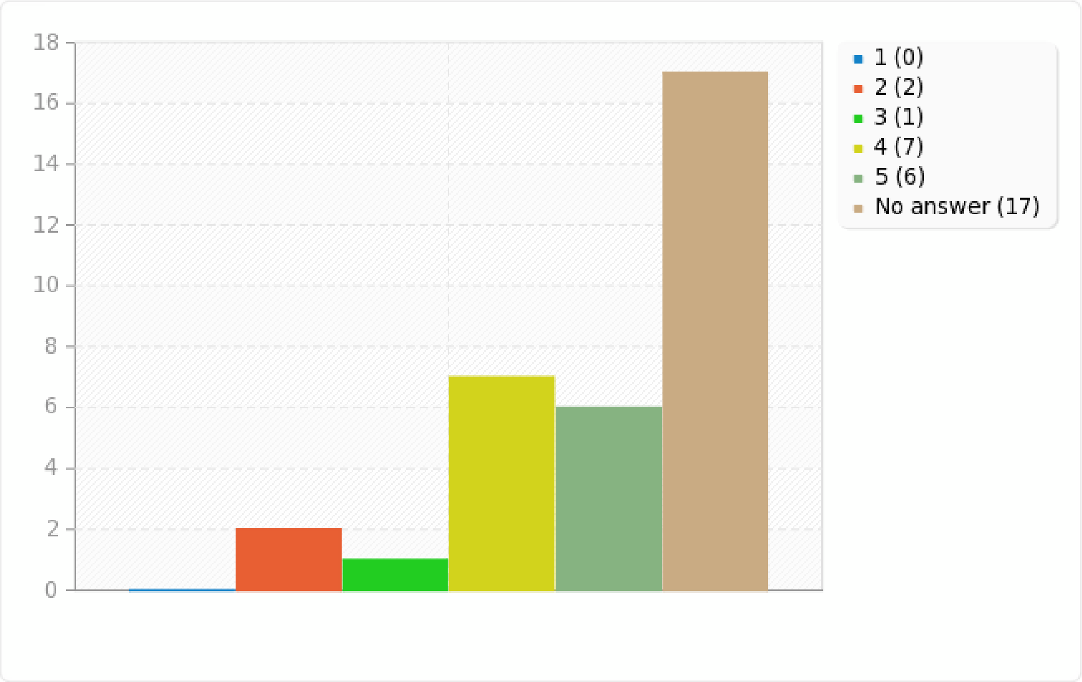
Field summary for DomCyberSec3(4)

What is their cost/effectiveness ratio? [Training]

Answer	Count	Percentage	Sum
1 (1)	0	0.00%	3.92%
2 (2)	2	3.92%	
3 (3)	1	1.96%	1.96%
4 (4)	7	13.73%	
5 (5)	6	11.76%	25.49%
No answer	17	25.00%	
Arithmetic mean	4.06		
Standard deviation	1		
Sum (Answers)	16	100.00%	100.00%
Number of cases	33	100.00%	

Field summary for DomCyberSec3(4)

What is their cost/effectiveness ratio? [Training]



Field summary for Need1

Which are the most important needs that should be taken into account (now and in the future)?

Answer	Count	Percentage
Answer	15	50.00%
No answer	15	50.00%

ID	Response
4	Security policies inside organizations.
5	data and privacy protection
9	Awerness seccions for liders, investigative specialists and experts aproppriate training and funding
16	Clarification od competence and the creation of na unit in the Criminal Police devoted to the cybercrime issues, including cyberterrorism.
19	The computer's mantaining services at my University have a considerable skillfullness in adopting strategies to avoid cyber attacks namely from virus but they should prabably benefit from some training refering to more sophisticated attacks
26	Awareness focused actions and training/capacity buiding
30	Training and easy steps to undertake in this issue
31	increase public, social and political awerness Eduction prevantion and social intervention on vulnerable groups Share of information betwenn several agencies including mental Health, education, etc beyond securitys agencies. The organazations of small goups of specialist, not only of security agencies, to evaluate concrete situations of recruitment, to decide the best action that slhould be tacken
41	The creation of a special unit.Specialized Education and traing of their human resource. Gathering the capacity to implement the Strategy of the European Union in the area of cybersecurity.
42	The creation of a special unit with human resouces that should have special and constant education and training. Our national cybersecurity initiatives must be aligned with the European Strategy of Cybersecurity.
51	- Law enforcement training - Citizen awareness - Legal framework adapted to the new types of digital crimes
54	1) The training of professionals of IT 2) Deploy Situational Awareness Systems 3) Implement procedures in Software Security Assurance for the development of new software
62	- Social and economic context in which terrorsism can grow and/or impact; - Financial resources of terrorist organizations; - Online proselytism and dissemination
63	Training and development of more efficient tools.
69	Awareness, current patterns, threats, radicalisation.

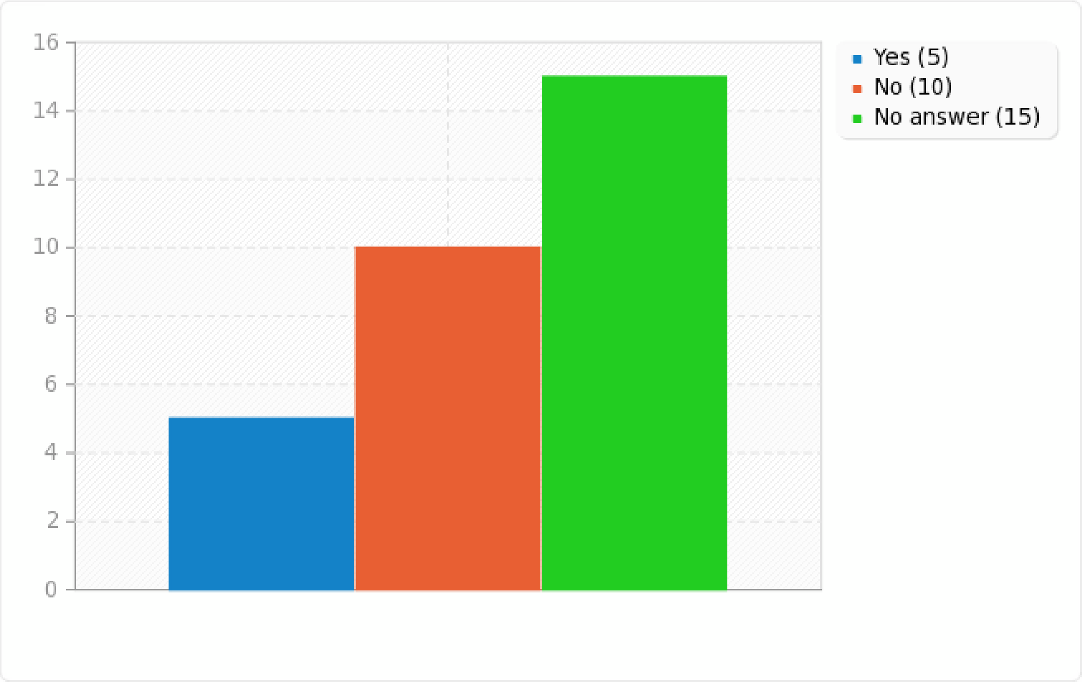
Field summary for Coop1

Are you collaborating or cooperating with the public and/or private sector on cybersecurity technologies?

Answer	Count	Percentage
Yes (Y)	5	16.67%
No (N)	10	33.33%
No answer	15	50.00%

Field summary for Coop1

Are you collaborating or cooperating with the public and/or private sector on cybersecurity technologies?



Field summary for Coop2

If so, please state the type of organization/institute, the level and type of collaboration/cooperation and the most important benefits and results.

Answer	Count	Percentage
Answer	4	66.67%
No answer	2	33.33%

ID	Response
41	All the national and international Security Forces, public and private sectors, academies and the academies.
42	All the national and international security forces, public and private sectors, academies and cityzens have also an important role.
62	Type of Organization: Armed Forces; Law Enforcemnt Agencies; Civil Protection and First Responders; University and Think Tanks; Institutional Stakeholders. Type of Collaboration: Provision of Solution and Services; Partecipation in EU financed R&D Security Projects.
63	1. NATO Cyber incident response center. Information sharing, training, exercises, knowledge transfer. 2. European Defence Agency Cyber Defence Capabilities development programme. Common development of cyber security programmes, procedures and capability development activities. 3. Greek Research and Technology Network. Technology transfer, cyber range, education and training.

Field summary for Coop3

Please describe the cooperation between governmental institutions and the private sector in relation to cybersecurity.

Answer	Count	Percentage
Answer	4	66.67%
No answer	2	33.33%

ID	Response
41	There is a National Cybersecurity Center that promotes and tecnicaly coordinates the action taken of public and private CSIRTS and Security Forces, making also the risk management. It can establish also connectios with CERT.EU.
42	In the area of network and information security there are some organizations responsable, the most important are :Centro Nacional de Cibersegurança, ANACOM, DGIE (UTIS), CNPD, Operadoras, etc. In the area of Law Enfocement:Gabinete do Cibercrime, PJ, PSP e GNR. In the area of the Cyberdefence: Centro de Ciberdefesa e as Forças Armadas. This are the most important institutions.
62	It's all about information-sharing (about incident and new threats) and knowledge transfert (from private to public and viceversa)
63	So far the level of cooperation is very low. There are just some initial discussions on how we can better gain results and how to design and plan common efforts in the future. There is some cooperation in cyber defence exercises with volunteer contribution.

Field summary for Coop4

What is necessary to build-up an effective PP (Public-Private) cooperation-partnership model?   Please describe your experience.

Answer	Count	Percentage
Answer	11	36.67%
No answer	19	63.33%

ID	Response
4	no experience
9	Information share is a "must have" on fighting cyberterrorism so a close PP cooperation or partnership with well defined rules is very important.
16	(...)
19	I'm not competent to answer this question
30	No experience on this topic
31	Unfortenly i dont know any portugueas e experience on tha subject, however i believe that partnership it is the best model for complexe issues
41	Specially a common sharing of information and procedures to potentiated, in time, adquated responses against Cyber terrorim initiaves.
42	There is a National Cybersecurity Center that has the principal mission to promoting, coordinating in the tecnical domain the initiatives of the public and private sector, CSIRTS and Security Forces in the area of Cybersecurity. This center also coordinates management risk of this entities, helping them build their own cybercapacities.
62	An effective PPP model needs to be precisely outlined by the law. It also needs secure environment/infrastructure for the information exchange and periodically meeting.
63	Legislation standards. Building-up trust. Financial improvement on behalf of public sector. My experience is that there is always an identification of this need (either as lessons learned of exercises or workshops findings) and usually there are some initial follow-up discussions but always when it comes to the real development it fails to proceed further.
69	Would have to research in the UK, which could be the nearest policing procedures that we adopt in Gibraltar

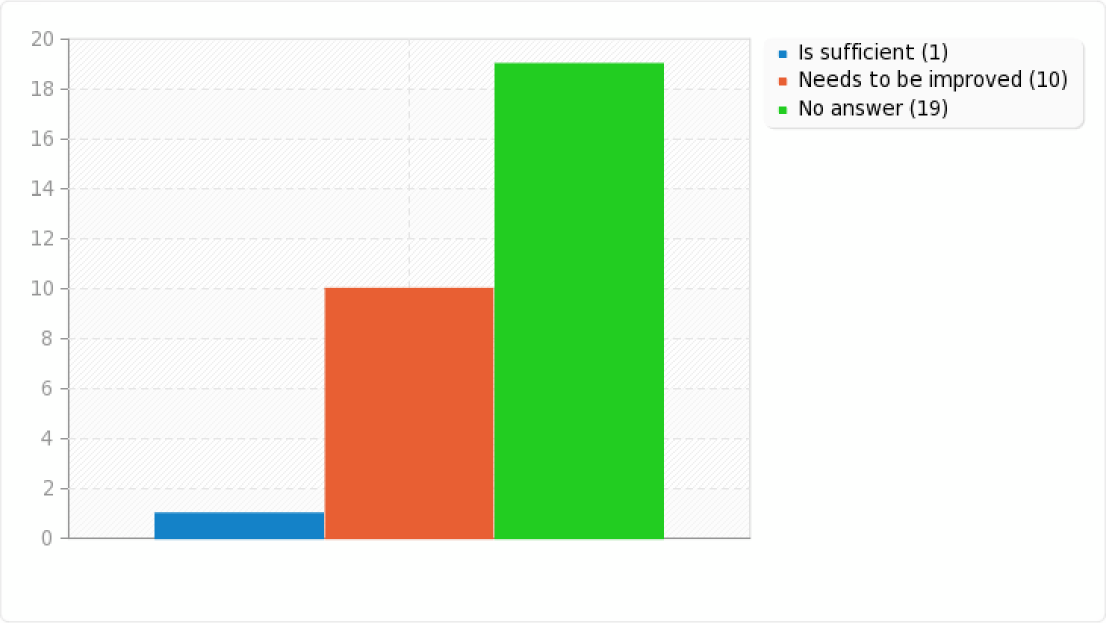
Field summary for AssessPP1

How do you assess the PP cooperation-partneship model in your country?

Answer	Count	Percentage
Is sufficient (1)	1	3.33%
Needs to be improved (2)	10	33.33%
No answer	19	63.33%

Field summary for AssessPP1

How do you assess the PP cooperation-partneship model in your country?



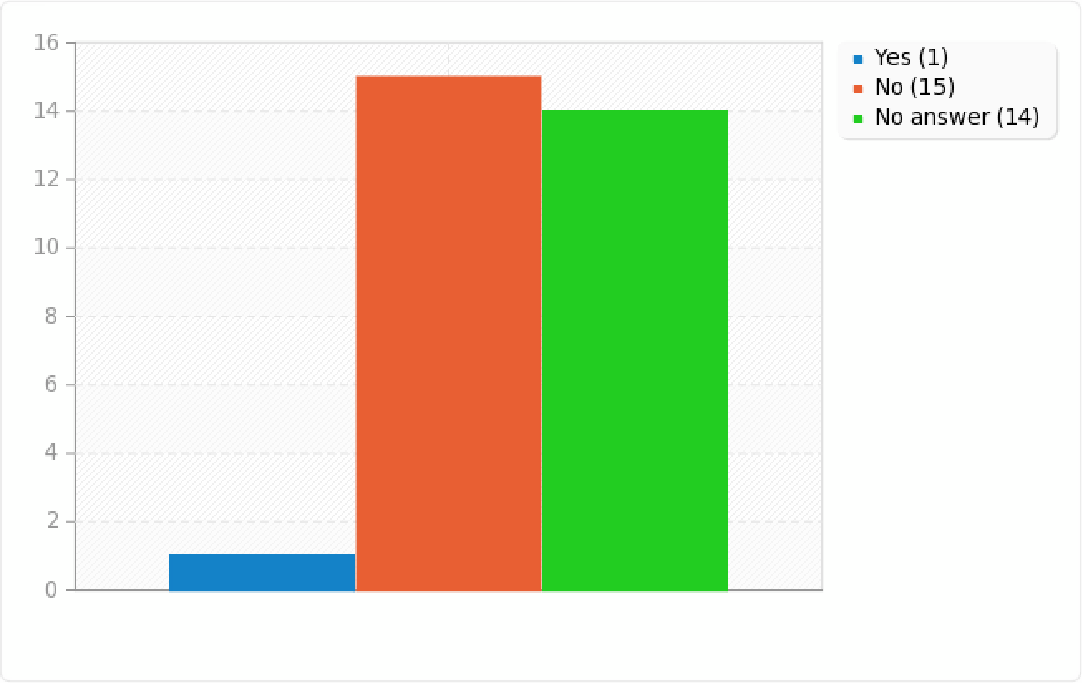
Field summary for PreventTerr1

Do you follow any guideline(s) to prevent the use of internet by terrorists?

Answer	Count	Percentage
Yes (Y)	1	3.33%
No (N)	15	50.00%
No answer	14	46.67%

Field summary for PreventTerr1

Do you follow any guideline(s) to prevent the use of internet by terrorists?



Field summary for PreventTerr2

If yes. which one?

Answer	Count	Percentage
Answer	0	0.00%
No answer	2	100.00%

ID	Response

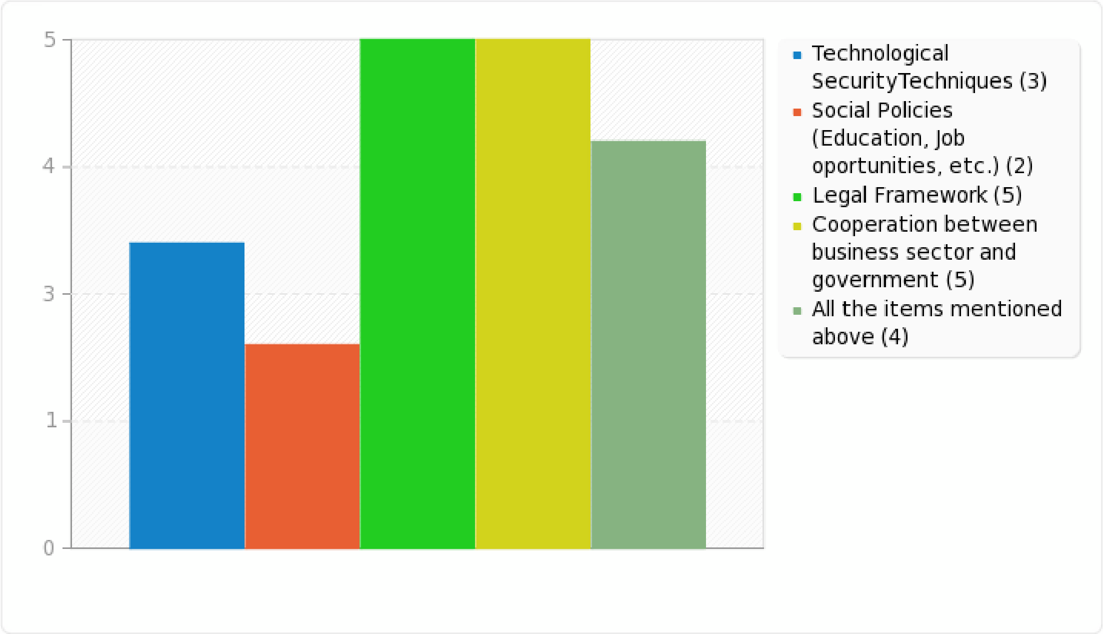
Field summary for Domain1

What would you consider to be the three-top best domains to counter cyberterrorism?

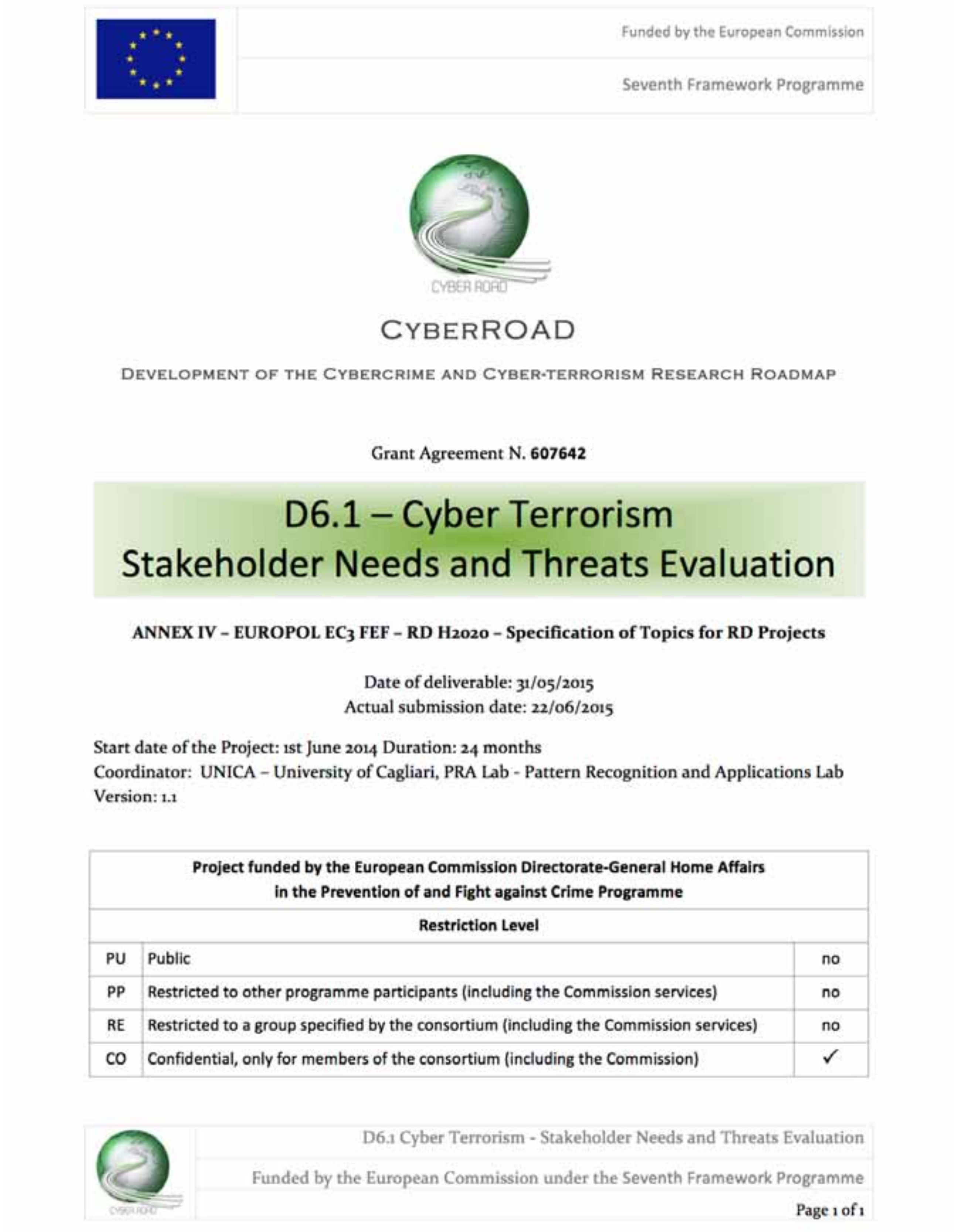
Answer	Count	Percentage
Technological SecurityTechniques (SQ001)	3	17.65%
Social Policies (Education, Job oportunities, etc.) (1)	2	11.76%
Legal Framework (2)	5	29.41%
Cooperation between business sector and government (3)	5	29.41%
All the items mentioned above (4)	4	23.53%

Field summary for Domain1

What would you consider to be the three-top best domains to counter cyberterrorism?



16 ANNEX IV: CYBERROAD D6 1 - EUROPOL EC3 FEF - RD H2020 - SPECIFICATION OF TOPICS FOR RD PROJECTS



Funded by the European Commission

Seventh Framework Programme

CYBERROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

D6.1 – Cyber Terrorism Stakeholder Needs and Threats Evaluation

ANNEX IV – EUROPOL EC3 FEF – RD H2020 – Specification of Topics for RD Projects

Date of deliverable: 31/05/2015
Actual submission date: 22/06/2015

Start date of the Project: 1st June 2014 Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 1.1

Project funded by the European Commission Directorate-General Home Affairs in the Prevention of and Fight against Crime Programme		
Restriction Level		
PU	Public	no
PP	Restricted to other programme participants (including the Commission services)	no
RE	Restricted to a group specified by the consortium (including the Commission services)	no
CO	Confidential, only for members of the consortium (including the Commission)	✓

D6.1 Cyber Terrorism - Stakeholder Needs and Threats Evaluation

Funded by the European Commission under the Seventh Framework Programme

Page 1 of 1

Europol Unclassified – Basic Protection Level

Releasable to the Members States, non-EU Cooperation Partners and selected non-law enforcement entities

The Hague, 6 May 2015

EDOC# 772992-v1

Forensic Expert Forum

Specification of topics for R&D Projects

1. Introduction

This document aims to provide direction for project proposals for recently published calls under the Horizon 2020 Programme of the European Commission. The topics have been selected on the basis of relevance for digital forensic activities of the EU law enforcement community.

The document is intended to share the interests of EU law enforcement in specific tools and solutions that police services are lacking in their daily work with potential partners in Industry, research institutes and academia. Hopefully, this will result in the establishment of new partnerships, in which law enforcement can collaborate with interested external partners to develop and deliver the desired forensic tools.

The topics for Research & Development projects presented in this paper are the result of two rounds of consultation of the Forensic Experts Forum (FEF). The FEF consists of digital forensic experts from the EU Member States that convene on a regular basis to align priorities in the development of forensic tools.

The FEF and potential R&D partners will be brought together at a conference on 9 June. At that event the topics will be presented and participants can present proposals for concrete projects addressing these subjects.

2. Horizon 2020 calls for proposals in 2015

Horizon 2020 (H2020) is the funding programme of the European Commission aimed at stimulating investments in innovative programmes in relevant sectors of society and economy. Significant amounts of money are allocated to projects that serve specific development objectives. A part of the reserved budget is specifically aimed at strengthening the fight against crime and terrorism (FCT).

In the next chapter four specific calls for projects are presented. These are of particular interest to the FEF. For each of the calls the specific challenge, the scope and the expected impact are described in the original wording as published by the Commission. At the end of each call the proposed R&D topics of the FEF are presented to the extent that they fall within the scope of the call in question. One topic has been added as a consequence of recent developments regarding terrorism/extremism-related Internet content.

In terms of timing, all four calls referenced in this document have opened on 25 March 2015 and the deadline for submission of projects is on 27 August 2015. This means that after the conference of 9 June 2015 there will be 11 weeks left to develop and submit projects.

3. Topics for Research & Development

In the following paragraphs the four H2020 calls of interest to the FEF will be presented, each followed by the concrete suggestions for R&D products. The aim of those suggestions is to give sufficient direction to obtain an end-product that actually meets the needs and, on the other hand, to allow enough flexibility for potential project partners to tweak proposals in accordance with their own views on how to best approach the delivery, obviously while remaining within the outlined scope.

3.1. FCT-01-2015

Forensics topic 1: Tools and infrastructure for the extraction, fusion, exchange and analysis of big data including cyber-offenses generated data for forensic investigation

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1113-fct-01-2015.html

Specific challenge:

The availability of petabytes of on-line and off-line information being open to the public owned by the Law Enforcement Agencies (LEA), such as police forces and/or custom authorities or the result of the investigation of a (cyber-) offence, represents a valuable resource but also a management challenge. Access to huge amounts of data, structured (data-bases), unstructured (multilingual text, multimedia), semi-structured (HTML, XML, etc.), heterogeneous data collected by LEA sensors such as Video, Audio, GSM and GPS, all possibly obfuscated or anonymized, available locally or over private LEA owned/shared networks or over the Internet, can easily result in an information overload and represent a problem instead of a useful asset.

Scope:

Proposals under this topic should aim to provide solutions at and beyond the state-of-the-art in the areas of intelligent use and management of complex and large amount of data for the discovery of correlated evidences to support forensic investigation on one hand and for the operational and situational awareness of law enforcement agencies on the other. The problem of extracting, integrating, exchanging, analysing and exploiting large complex, structured and unstructured (Natural Language Text, SMS, multimedia) heterogeneous data, as well as that of exploiting unstructured data (Natural Language Text, SMS) and adding intelligence (trends analysis, scenarios, etc.), has to be solved by means of at and beyond state-of-the-art technologies in the areas of Big Data, Data Analytics, Multimedia Analysis, Data Modelling, Data mining, Visualization, Intelligent User's Interfaces, Information Retrieval, Automatic Language Translation, Weak Signal Analysis, Ontologies, High Level Fusion Techniques for Context Awareness and Knowledge Representation. Digital intelligence capabilities should also enable smart pre-processing and filtering of sensor data and stored data in order to improve their reliability, accuracy, accessibility and transmission volume.

The scope of this topic is threefold:

Firstly, tools and platforms should be developed for sampling, analysing, evaluating, interpreting, reasoning over, and recording forensic evidence from big data with a view to achieve solid and court-proof forensic evidence that can be used during legal prosecution. Applications should provide certainty with respect to the time and location of multimedia content and tests for authenticity and integrity of digital identities. Platforms should also provide users with semi-interactive techniques for understanding and visualizing data, including interdisciplinary approaches based on common, possibly standardized, ontologies and the exploitation of automated reasoning, information retrieval, and filtering tools. Human and organisational factors like multilingualism/multiculturalism as well as other trans-border issues (different terminologies, legislations, procedures) must be properly addressed.

Secondly, tools and platforms should be developed to enable LEAs to store, process, analyse, share, and exchange large amounts of heterogeneous data, including data arising from various types of sensors, with the aim of improving operational and situational awareness more efficiently. Data exchange between LEA and network operators shall be standardized for fast and efficient processing. These should include applications which can provide early warning signs (e.g. predictions of future trends). Vendor locking has to be excluded. The development of a base line system for current and future end users should also be envisaged and the solution should follow Open Source concepts. This will enable transparency, and continuous maintenance and development after the end of the project. The software should provide fine-grained authorisation mechanisms to regulate data access. Support for logging and in general maintain the chain of custody is also required.

Thirdly, tools and platform should allow reaching a significant speed-up in the whole process of analysing (cyber) offenses. The main challenges are the automation of as many analysis steps as possible; the countering of the obfuscation used by the attacker. The finding of an efficient way to identify an attacker despite use of anonymisation, , performing automatic deep analysis of all data in the offense, and making optimal use of the capabilities of man and machine.

Proposals addressing this topic should address the three aspects of the scope and take previous research at European and national level into account. Methodologies, standards, expertise and procedures for training, simulation, and testing investigations to empower the experts and stream-line the processes involved in the fusion, exchange and analysis of big data for forensic investigation and operational/situational awareness for law enforcement purposes should be considered.

The proposal will have to deal with the management of personal data, and related ethical and legal issues. Therefore considerable attention will have to be given to privacy and data protection, and to the adherence to European regulations. For each proposed solution, potential issues vis-à-vis these rights and regulations will have to be analysed, and recommendations on the best solutions to these issues must be proposed.

Proposals addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

Proposals for this topic should take into account the existing EU and national projects in this field.

The Commission considers that proposals requesting a contribution from the EU of between €9m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

The outcome of the proposal is expected to lead to development from Technology Readiness Levels (TRL) 6 or above; please see part G of the General Annexes.

Expected impact:

Proposals should lead to:

- improved capabilities for the LEA to conduct investigations and analysis;
- higher efficiency in accessing relevant data sources and retrieving information significant for forensic investigation; and
- improved capabilities for trans-border LEA data-exchange and collaboration.

The outcome of the proposal is expected to lead to development from Technology Readiness Levels (TRL) 6 or above; please see part G of the General Annexes.

FEF topics of interest under FCT-01-2015:

The processing of large quantities of data is becoming an ever increasing challenge for law enforcement. This applies to the collection, the storage and in particular the processing to extract forensic evidence.

There are in essence three areas in which relevant projects could be considered to improve the effectiveness of law enforcement in dealing with Big Data.

The first dimension is related to the processing of seized and intercepted data. The quantities of data that are collected as part of criminal investigations have increased tremendously over the past decade. There is a continuous need for new tools that become more powerful and able to integrate the various new data types and formats. The lawful collection of internet-based communication requires real-time interception and the storage of such data for analysis and as evidence. Efficient processing and extraction tools also require multi-lingual capabilities. The processing of sound recordings and images demands much more processing capacity than alphanumeric data.

The second area of interest is related to the availability of massive quantities of Open Source data that can be of relevance for criminal analysis. Privacy-proof processing capabilities are needed for the strategic analysis that helps to understand the effect of large-scale criminal activity on the community and online commerce. This relates to sensor and honeypot information on malware distribution and botnet operation, but also to payment fraud, spamming and social engineering.

The third direction for Big Data studies and solutions is related to the ever-growing connectivity. The number of technical devices that are interconnected creates a huge opportunity for additional services and end-user comfort. At the same time, the connectivity of refrigerators, heating systems, garage doors, cars, medical devices and other equipment also poses security vulnerabilities. Research envisaged on this subject would focus on the detection and prevention of cybercrimes that seek to abuse the multitude of interconnected devices and the access they provide to the private lives and assets of citizens.

3.2. FCT-02-2015

Forensic topic 2: Advanced easy to use in-situ forensic tools at the scene of crime

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1114-fct-02-2015.html#tab1

Specific challenge:

Rapid developments in technologies and communication in various fields go hand in hand with new opportunities for forensic science to investigate more and a greater variety of traces, to extract more information from less material, quicker than ever before. In order to keep the standards of forensic science in Europe at a high level regarding juridical and technological questions. Meanwhile, organised crime and criminals do not limit themselves to regional or national borders. Their crimes are thus leaving traces in multiple countries. Cross border access to evidence has become an absolute necessity for Law Enforcement Agencies (LEA) and judicial authorities.

Evidence gathering, collection and exchange at EU level should be usable from the field to the judge, independently of the technology used to commit the crimes and of where the crimes have taken place. Rapid developments in technologies and communications in various fields go hand in hand with new opportunities for forensic science.

Proposals for this topic should take into account the existing EU and national projects in this field, such as the Council Conclusions on the vision for European Forensic Science 2020 which foresee the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe."

Scope:

Proposals for this topic should focus on the development methodologies of tools and EU-wide standards for the secure storage, smart visualisation, access and the rapid exchange of forensic data supporting evidence.

A multianalytical platform integrating different techniques should be proposed in order to achieve better strategies for gathering and analyzing evidence in the field of forensic research. Relying on knowledge-based fields such as artificial intelligence, machine learning, different procedures, tools and algorithm should be developed within this platform, based on the standard outlined above.

Specific areas of research could be:

- Development of an analysis platform that could be deployed at the scene of the crime and which can be validated against the currently used forensic guidelines and standards.

- The establishment of a EU-wide databases on, for instance, new synthetic drugs and drug precursors,The creation of tools for tracking virtual currencies implicated in criminal transactions.

- Other types of pan-Eu databases on recognition.

In addition due to the variability and the wide range of crime types, procedures or methodologies should be developed or adapted to the specific crime features. Moreover, horizontal strategies could be proposed for profiling crimes or offenders and matching and predicting different type of crimes. This should lead to the establishment of a catalogue of these procedures or methodologies.

The development of a base line system for current and future end users should also be envisaged and the solution should follow Open Source concepts.

Where necessary new technologies should be developed for sampling, analysing, evaluating, interpreting and recording forensic evidence, with a view to achieve solid and court-proof forensic evidence that can be used during legal prosecution.

The use of the most advanced information technologies should allow improving and upgrading the current forensic systems in the European police institutions. The scope of the proposed tool should involve law enforcement bodies from the design phase to the prototyping and test phase.

Proposals addressing this topic may involve the use of classified background information (EU or national) or the production of security sensitive results. As such, certain project deliverables may require security classification. The final decision on the classification of projects is subject to the security evaluation.

The Commission considers that proposals requesting a contribution from the EU of between €9m and €12m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Projects under this topic should lead to the development of novel easy to use in-situ forensic tools, customised to the specific needs of EU LEA. Better profiling of crimes and offenders. Quicker matching of different types of crime. Shorter court cases due to the availability of more solid court proof forensic evidence.

For industry better understanding of modern operational LEA requirements, thus increasing their competitiveness.

Considerable improvement in the field of public security and improved trust of the citizen in the work of police forces in the EU.

The outcome of the proposal is expected to lead to development up to Technology Readiness Level (TRL) 8; please see part G of the General Annexes.

FEF topics of interest under FCT-02-2015:

The present needs of law enforcement for specific **digital forensic tools** are manifold. From the consultation of the FEF there were 4 main clusters of requirements that came out, apart from the need for big data analysis that were already mentioned under FCT-01-2015.

The first group of requirements is centred around the capturing of the RAM of devices. A tool that would support this capturing for a range of systems, including mobile RAM, and the subsequent analysis thereof would be warmly welcomed.

The second group relates to the present challenges around the virtualisation of machines. Also in this case, a tool that would support the virtualisation of multiple types of computers as well as mobile devices is very much needed.

The third group, calls for an integration platform of the analysis results of various analysis tools. This integration platform should make it easy to link the results and display them in an easy fashion that also helps to explain the case and sequence of events to a non-technical audience. Ideally, it should come with case management functionality and multi-lingual features as well.

The last category of requirements specifically addresses the digital forensics around **virtual currencies**. These are used increasingly by criminals for the anonymity they offer in criminal transactions and money laundering. For some currency schemes the block-chain information is public, but still obfuscation techniques are continuously improved to mask the origin and direction of money flows. Tools required in this regard should enable the tracing of money flows and the attribution to end-users. This may include the tagging of wallets to criminal forums, the dissolving of re-direction on the Darknet and linking of series of transactions.

3.3. FCT-04-2015

Forensics topic 4: Internet Forensics to combat organized crime

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1116-fct-04-2015.html

Specific challenge:

The Internet is nowadays at the core of any business activity. All large and distributed organisations rely on the Internet for the exchange of data, information, and knowledge, both internally and externally, so as to organise and run their activities. Organized crime is no exception. The Internet has become an important tool for criminal organisations to carry out illegal activities. Research under this topic should refer to Internet Forensics as the set of investigation techniques concerned with Internet as a media used by organised crime in general - mainly to communicate and exchange data and information. A further and specific challenge is represented by the camouflage of the real nature of the concerned data and information. Due to the borderless nature of the Internet, specific trans-border aspects should be considered when dealing with Internet Forensics. Therefore, aside from the relevant technological aspects, legal and organisational issues like the co-ordination of different Law Enforcement Authorities (LEA) and the harmonisation of the different legal frameworks have to be addressed.

Scope:

Proposals should focus on how to extract, compare, correlate, filter, reason over and/or interpret suspect information, data, communications stored and/or transferred on the Internet including on the deepweb, darknet and other less easily accessible parts of networks, obtained under a lawful warrant, in order to discover facts and evidence to support forensic investigations (including e.g. resolving identities in social networks, authorship identification on webfora, shared media, etc.). Software and, if necessary, hardware tools, methods and guidelines should be proposed. They should tackle all the layers of analysis, from the data-packet level to the data mining, to language interpretation, semantic analysis, and information retrieval, including the multi-lingual aspects, and video and picture analysis. Investigative techniques on any kind of crime using the Internet to some extent (to communicate, transfer data, etc.) should be concerned. The proposed solutions should enable accelerated searches of the huge amount of data-transfer that occurs on the Internet, and to discover and make clear (interpret) out of it the relevant data and information. At the same time, limited, or at least controlled, pervasiveness of the proposed solutions must be guaranteed, in order guarantee the privacy of all the internet users. Ethical issues have to be clearly addressed. Appropriate solutions to fulfil the legitimate request of privacy by the citizens should be embedded in the very core of the proposed solutions. Also, all the developed tools, methods and guidelines should be supported by training support and curricula.

Where necessary new technologies should be developed for sampling, analysing, evaluating, interpreting and recording forensic evidence with a view to achieve solid and court-proof forensic evidence that can be used during legal prosecution.

The development of a base line system for current and future end users should also be envisaged and the solution should follow Open Source concepts.

Proposals will have to deal with the management of personal data, and related ethical and legal issues. Therefore considerable attention will have to be given to privacy and data protection, and to the adherence to European regulations. For each proposed solution, potential issues vis-à-vis these rights and regulations will have to be analysed, and recommendations on the best solutions to these issues must be proposed.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

- improved LEA capabilities to conduct investigations by using information travelling and stored on the Internet obtained under a lawful warrant ;

- improved training of LEA staff able to perform these investigations. increased crime prosecution capabilities;

- shorter court cases due to the availability of more solid court proof forensic evidence;

- increased privacy and data protection during forensic investigations;

- for industry better understanding of modern operational LEA requirements, thus increasing their competitiveness.

The outcome of the proposal is expected to lead to development from Technology Readiness Levels (TRL) 6 or above; please see part G of the General Annexes.

FEF topics of interest under FCT-04-2015:

- Law enforcement agencies throughout the EU rely on the **lawful interception of communications** between criminals to collect evidence. Telephone interception has traditionally given tremendous support to investigations of organised crime, murders and terrorism.

Since many years the telecommunication technology has evolved and shifted from being entirely telephone-based to a variety of communication systems, mainly based on internet technology. Currently, criminals have understood the opportunities offered by this evolution and are widely using the Internet and mobile apps to avoid lawful interception. Classical interception provides hardly any investigative results anymore.

For the lawful interception of contemporary and developing communication technologies the key focus should be on Internet-based systems. Yet, also radio-based deployments should not be forgotten. Various forms of targeted interception of internet traffic, including skype and live streaming should be captured. In addition, also traces of communication left on the suspects' devices and computers should be included.

There are two main approaches that can be considered for the interception: on the one hand the interception could use the so called 'man in the middle' set up. This can either be done through wifi interception or through an ISP. Both options obviously have their limitations and risks. On the other hand, the interception can be organised by means of malware infection of suspects' devices or other forms of hacking. The risks associated with this approach are losing control and leaving traces that criminals can pick up. Clearly, these risks need to be taken into account in the design of the envisaged R&D solutions.

- The obfuscation techniques used on the **Darknet** to hide identities for the best possible objectives are unfortunately also abused at an increasing scale by criminals that benefit from the anonymity it offers them while conducting their criminal businesses online.

When there are clear indications that crimes are committed and the legal basis for police intervention is established to investigate, then appropriate tools are required to attribute those crimes to the actual suspects despite the anonymisation techniques used in the communication.

The tools would ideally build on and combine several avenues to unmask the criminals. These include the use of exit nodes, security software vulnerabilities, 'policeware' injections, fake Darknet sites, social engineering and carelessness of criminals leaving traces.

In addition to finding the real IP addresses of criminals, there is also and perhaps even more importantly, an interest to trace criminal infrastructure used in particularly for the hosting of criminal sites and forums. Also the development of Darknet surveillance tools to monitor criminal activities on the Darknet would be welcomed.

Key challenges for the development of tools assisting police operations on the Darknet are the speedy evolution of security software and its patching, the importance of remaining stealthy at any time of a tool's operation, the multilingual dimension and even the diversity of characters that languages consist of. A continuous development with short-interval deliveries that continue to be state-of-the-art and ready to deploy, would seem the most ideal prospect.

- Furthermore, the FEF has expressed an interest for several R&D investments in **decryption tools**. Criminals seek refuge and protection by using increasingly sophisticated encryption techniques. There are at present in particularly problems with accessing files and accessing RAM, whilst future challenges are looming with fully encrypted phones and other devices.

Several directions for R&D can be considered in order to resolve current and emerging difficulties for law enforcement. Some of these are technical, others more psychological. In the technical realm, solutions can be sought by boosting processing power to resolve encryption. Quantum computing specifically deserves attention in this regard. Very little is known, other than that it can multiply processing speed/capacity immensely compared to the present forms of computing used for decryption. For accessing RAM the right balance needs to be sought between increased RAM access and RAM preservation by maintaining system stability.

In the non-technical dimension, the human/psychological aspects of password composition can be studied in more depth. The results should enable a better targeting of processing power at likely directions for password possibilities.

An important dimension of the envisaged tools is the use on site as part of live forensics. A tremendous difference in results can be achieved if uninterrupted access to computers and infrastructure can be gained.

In terms of deliverables, it must be understood that the encryption techniques evolve rapidly. Therefore, as was argued for the attribution on the Darknet, the output of the R&D project should come in regular updates that are tuned to the latest encryption techniques, as opposed to resulting in a single end-product that is outdated by the time it is in use.

3.4. FCT-06-2015

Law Enforcement capabilities 2: Detection and analysis of terrorist-related content on the Internet

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1117-fct-06-2015.html

Specific challenge:

Due to the ease of publishing information on the Internet (Web site, blogs, social networks, newsgroups, forums, etc.), terrorists increasingly exploit the Internet as a communication, intelligence, training, recruitment and propaganda tool where they can safely communicate with their affiliates, coordinate action plans, raise funds, and introduce new supporters or recruits into their networks. In order to cope with the dangers involved in the use of Internet by global terrorist organizations and grassroots terrorist cells, more efficient and effective automated techniques are required. Despite the often explicit (or at least not disguised) content of these web-sites, especially when used for propaganda, the huge amount of somehow related, yet not illegal, sites, represents a major obstacle to the reliable and fast analysis of their contents. Research should therefore develop and apply new and/or improved data and text and multimedia mining methods to detect, categorize, analyse, reason over, and summarize terrorist-generated content group information from several sources that supports same history, and isolate potential sources describing different ideas, that could be intended to generate "disinformation" or fake evidences to distract LEA from real scenarios. Aside this, modes of finding sources of data, capturing and preserving data for forensic analysis, authenticating images and linking videos and conversely proving multimedia data falsification, should be investigated.

Scope:

Proposals should focus on the accurate identification of terrorist online communities (even hiding their real identity), accurate and fast categorization of malicious content published by terrorists and their supporters in multiple languages, large-scale temporal analysis of terrorism trends, and real-time summarization of multilingual and multimedial information published by terrorists, including content filtering for mis- and disinformation and framing. In addition, linking pseudonyms and finding the original author should be part of the research. The developed methodologies should be able to handle massive amounts of multilingual and multimedial web content in minimal time. The scope of the proposed tool should involve law enforcement bodies from the design phase to the prototyping and test phase.

The proposals should address the management of personal data, and related ethical and legal issues. Therefore considerable attention will have to be given to privacy and data protection, and to the adherence to European regulations. For each proposed solution, potential issues vis-à-vis these rights and regulations will have to be analysed, and recommendations on the best solutions to these issues must be proposed.

The development of a base line system for current and future end users should also be envisaged and the solution should follow Open Source concepts.

The Commission considers that proposals requesting a contribution from the EU of between €3m and €5m would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected impact:

Projects under this topic should lead to:

- More effective prevention of terrorist activities planned and organized via the Internet through automated analysis of terrorist-generated content.

- Faster detection of grassroots terrorist cells from their online activities. Faster and more accurate detection and analysis of malicious content published by terrorists.

- Faster detection and analysis of terrorism trends. Reduction of the "information overload" on web intelligence experts due to automated summarization of the relevant content.

- Increased privacy and data protection.

- Contribution to a considerable improvement in the field of public security.

- For industry better understanding of modern operational Law Enforcement Agency requirements, thus increasing their competitiveness.

The outcome of the proposal is expected to lead to development from Technology Readiness Levels (TRL) 6 or above; please see part G of the General Annexes.

FEF topics of interest under FCT-06-2015:

Recent developments have urged for a steep increase of attention for the presence of violent extremism/terrorism related content on openly accessible parts of the Internet. Whilst highly respecting the freedom of speech, the publication of propaganda for violent extremism/terrorism with a view to spread disinformation and/or recruit new people calls for lawful intervention by competent authorities as well as any other parties involved in the hosting or transmission of such content.

Major challenges for law enforcement and hosting services are the quantity of posted content, the absence of consistent criteria for assessing (non-) compliance, language barriers, jurisdictional differences and the huge spread of the content over numerous sites, forums and platforms.

State-of-the-art tools are needed to take up the recent tasking of Europol to set up an EU Internet Referral Unit for the coordination of action against controversial Internet publications and the interaction with national referral units in that regard. Those tools should help to find data related to violent extremism/terrorism online and to analyse it for further action. The search, identification and analysis must support the integrated digestion of large volumes of data in multiple languages and formats, including audio and visual material.

4. Envisaged partnerships

The form of cooperation between the FEF and partners in industry, research centres and academia that is aimed for, is that projects on the R&D topics that the FEF has prioritised are developed in close collaboration between the FEF and the non-law enforcement partners.

The lead for the projects should be taken up by the external partners. This includes the project administration, the design and elaboration of project plans and the application for funding under the H2020 Programme. On the side of the FEF the work and activities are coordinated by the European Cybercrime Centre within Europol, which will also act as the central point of contact for the preparation of the calls on behalf of the FEF partners.

The involvement of digital forensic experts of the FEF should last throughout the entire lifecycle of projects. This includes the first conceptualisation, requirements definition, feedback on progress, testing and acceptance of end-products. This should stimulate the result-orientation and improve the alignment of delivery and user needs, so that the tools are more likely to operate successfully in the real situations they are designed for.

Europol can only take part in projects as an associated, non-beneficiary partner. This means that it can take part, but not obtain any benefits, such as the reimbursement of costs it incurs for projects or staff that is allocated to those. However, the costs for travel, accommodation and other costs related to the participation of digital forensic experts of Member States can be funded and as such be taken up in the budgetary planning of the projects.

(2014 йил 10-July). Retrieved 2015 йил 24-February from RT - Russian Today: http://rt.com/news/171724-norway-banks-anonymous-ddos/

(2014, July 25). Retrieved February 24, 2015, from RT - Russian Today: http://rt.com/news/175432-ecb-cyber-attack-data/

Ahkgar, B., & Yates, S. (2013). *Strategic Intelligence Management.* Elsevier Edition.

Awan, I. (2014). *DEBATING THE TERM CYBER-TERRORISM: ISSUES AND PROBLEMS.* Retrieved 05 12, 2015, from InternetJournalofcriminology: www.internetjournalofcriminology.com

BBC News. (2010) Retrieved 05 08, 2015, from Internet access is 'a fundamental right': http://news.bbc.co.uk/2/hi/technology/8548190.stm

Bravo, R. (2010). *From the Spectrum of conflict within information networks:Towards a conceptual reconstruction of terrorism in cyberspace.* Retrieved from https://www.academia.edu/943512/From_the_Spectrum_of_conflict_within_information_networks_Towards_a_conceptual_reconstruction_of_terrorism_in_cyberspace

Braz, J. (2009). *Investigação Criminal – A Organização, o Método e a Prova – Os Desafios da Nova Criminalidade.* Editora Almedina.

Cohen, F. (2015). *Deception and Perception Management in Cyber-Terrorism.* Retrieved 02 25, 2015, from All.net: http://all.net/journal/deception/terror-pm.html

Collin, B. C. (1997). *Crime Research.* Retrieved 4 23, 2015, from The Future of CyberTerrorism: http://www.crime-research.org/library/Cyberter.htm

Comission, European. (2013). *Reducing terrorist use of the internet.* Retrieved 05 15, 2015, from Cleanit Project: http://www.cleanitproject.eu/files/wp-content/uploads/2013/01/Reducing-terrorist-use-of-the-internet.pdf

Conway, M. (2011). *Privacy and Security Against Cyberterrorism* (Vols. 54, N.2, pp.26-28). Communications of the ACM.

Correio da Manhã. (2015). *Correio da Manhã.* Retrieved 05 16, 2015, from EUA admitem nova fase de ameaça terrorista: http://www.cmjornal.xl.pt/mundo/detalhe/eua_admitem_nova_fase_de_ameaca_terrorista.html

Cottle, S. (2006). *Mediatized Conflict.* Berkshire: Open University Press.

Dictionary.com (25 May 2015). Obtido de http://dictionary.reference.com/browse/terrorism

Dictionary.com. (20 May 2015).

ENISA. (2013). *ENISA.* Retrieved from Threat Landscape 2014: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/sgtl/smart-grid-threat-landscape-and-good-practice-guide/at_dow.

ENISA. (2014). *ENISA.* Retrieved from Threat Landscape 2014.

ENISA. (2014). *ENISA.* Retrieved from Threat Landscape 2014: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport

Council of Europe. (2007). *Cyberterrorism – the use of the Internet for Terrorist Purposes.* Counter-Terrorism Task Force. Council of Europe.

European Comission. (2012). *Methodologies or Adapted Technological Tools to Efficiently detesct violent radical content on the Internet.* Brussels.

Europol. (12 March 2015). EU Internet Referral Unit at Europol - 7266/15 . Brussels, Belgium.

Europol. (2015). EU Internet Referral Unit at Europol: concept note. Brussels: Council of European Union.

Foxworth, D. (2015,). *FBI - Federal Bureau of Investigation.* Retrieved 05 16, 2015, from FBI Warns Public of Disaster Scams: http://www.fbi.gov/sandiego/press-releases/2015/fbi-warns-public-of-disaster-scams

Godinho, D. (2014). *Acesso à internet, por parte dos jovens, duplicou nos últimos três anos.* Retrieved 05 12, 2015, from Tecnologia.pt: http://www.tecnologia.com.pt/2014/12/acesso-internet-por-parte-dos-jovens-duplicou-nos-ultimos-tres-anos/

Greengard, S. (2010). *AGNU 2020 - Mídia e Terrorismo* (Vols. 53, N.12, pp.20-22). Communications of the ACM.

Greengard, S. (2010). *The New face of War* (Vols. 53, N.12, pp.20-22). Communications of the ACM.

Internet Word Stats, Usage and Populating Statistics. (n.d.). Retrieved 05 2015, 08, from http://www.internetworldstats.com/stats.htm.

Jalil, S. A. (2003). *Countering Cyber Terrorism Effectively:.* Retrieved 02 25, 2015, from GIAC - Global Information Assurance Certification Paper: http://goo.gl/odGsNj

Janczewski, L. (2007). *Cyber warfare and cyber terrorism.* Information Science Reference.

Kasperkevic, J. (2012). *The FBI Tells Us How They're Handling America's Newest Threat — Cyber Terrorism*. Retrieved 05 15, 2015, from Business Insider: http://www.businessinsider.com/cyber-terrorism-is-keeping-the-fbi-on-their-toes-2012-4#ixzz1rVwaE69D

Lazari, A. (2014). *European Critical Infrastructures and the Directive 114/08/EC. European Critical Infrastructure Protection.* Retrieved from http://doi.org/10.1007/978-3-319-07497-9_3

Lemos, A. (2015). *Cibercultura e Mobilidade: a Era da Conexão.* Retrieved 05 12, 2015, from razonypalabra: http://www.razonypalabra.org.mx/anteriores/n41/alemos.html

Lewis, J. A. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats:.* Retrieved from http://www.enhyper.com/content/0211_lewis.pdf

Lipovetsky, G., & Juvin, H. (2010). *L´Occident Mondializé - Controverse sur la culture planétaire.* Grasset & Fasquelle.

LUSA. (2009). *DN Ciências*. Retrieved 3 10, 2015, from Diário Notícias: http://goo.gl/NnN5N5

LUSA. (2015). *SICNOTICIAS*. Retrieved 3 10, 2015, from http://goo.gl/jGe9DV

Mariani, J.-P. (2015). Cyberterrorisme? Réflexion autour d`une problématique nouvelle - Perspective française. *Investigação Criminal: Ensaios e Estudos* , pp. 95-99.

National Coordinator for Counterterrorism and Security (2013) .*'Reducing terrorist use of the Internet. Clean IT Project'.* The Hague, The Netherlands, Ministry for Security and Justice.

Nations, U. (2012). *The Use of Internet for Terrorist Purposes.* United Nations Office on Drugs and Crime. Vienna: United Nations.

NATO. (n.d.). Retrieved 02 26, 2015, from http://www.nato.int/nato-welcome/index.html

Olsen, G. (2010). *Understanding the risks mobile devices pose to enterprise security.* Retrieved 05 13, 2015, from TechTarget's: http://goo.gl/Knwycq

Online Etimology Dictionary. (25 de maio de 2015). Obtido de http://www.etymonline.com/index.php?term=terror

Oxford dictionaries. (s.d.).

Oxford.dictionaries.com. (25 de May de 2015). Obtido de http://www.oxforddictionaries.com/definition/english/terror

PGR. (n.d.). *Procuradoria Geral da República*. Retrieved 03 09, 2015, from http://cibercrime.pgr.pt/

Purser, S. (2014). *Standards for Cyber Security.* Retrieved 5 7, 2015, from https://goo.gl/nlxbRk

Reeb, C. (2010). Fight against Terrorism: French-Portuguese Cooperation. *Modus Operandi-Justiça e Segurança Interna* , pp. 56-58.

Roehrig, W. (2013). Cyber Threats and Countermeasures. *Atlantic Treaty Association Conference.* Rome: EDA PO Cyber Defence.

Rue, F. L. (2011,). *United Nations - Human Rights.* Retrieved 05 2015, 16, from Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

SysSec. (2013). The Red Book: A Roadmap for Systems Security Research. In D. B. Evangelos Markatos (Ed.).

Tendulkar, R. (2013, July). *Cyber-crime, securities markets and systemic risk*. Retrieved February 24, 2015, from IOSCO: http://goo.gl/fg50hE

Union, Council of European (20 May de 2015). *eu-council-internet-referral-unit.* Obtido de statewatch.org: http://www.statewatch.org/news/2015/may/eu-council-internet-referral-unit-7266-15.pdf

European Union, (13 June 2002). Combating terrorism. *EU Framework Decision, 2002/475/JHA* .

Swansea University (2013). *Cyberterrorism:A Survey of Researchers.* Retrieved from http://www.cyberterrorism-project.org/: http://www.cyberterrorism-project.org/wp-content/uploads/2013/03/Cyberterrorism-Report-2013.pdf.

UNODC - United Nations on Drugs and Crime. (2012). *The use of the Internet for terrorist purposes.* Retrieved 04 02, 2015, from http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

Ventura, J. P. (2010). A PJ e o Combate ao Terrorismo. A propósito da reunião da Interpol, sobre terrorismo na Europa, realizada em Portugal. *Justiça e Segurança Interna. Modus operandi, 3, pp 38-44.*

Weimann,G. (2005). *Cyberterrorism: The Sum of All Fears?* Retrieved 04 02, 2015, from Princeton: http://webcache.googleusercontent.com/search?q=cache:1VhpnHIEXyoJ:www.princeton.edu/~ppns/Docs/State%2520Security/Cyberterrorism%2520-%2520sum%2520of%2520all%2520fears.pdf+&cd=1&hl=pt-PT&ct=clnk&gl=pt

Weinberger, D. (2008). *Why open spectrum matters: the end of broadcast nation.* Retrieved 05 12, 2015, from Oss.net: http://goo.gl/rxzrEx

Wikipedia - The Free Encyclopedia. (n.d.). Retrieved 2 27, 2015, from http://en.wikipedia.org/wiki/Internet

Winters, R. (2013). *Mobile Devices and Web 2.0: The Growing Cyberterrorism Threat.* Retrieved 05 12, 2015, from Criminal Justice Focus: http://cjfocus.com/2013/07/02/mobiledevices/