CYBER ROAD

CyberROAD

DEVELOPMENT OF THE CYBERCRIME AND CYBER-TERRORISM RESEARCH ROADMAP

Grant Agreement N. **607642**

D 6.3 – Cyber Terrorism Best Practices Analysis

Date of deliverable: 30/09/2015
Actual submission date: 30/09/2015

Start date of the Project: 1st June 2014
Duration: 24 months
Coordinator: UNICA – University of Cagliari, PRA Lab - Pattern Recognition and Applications Lab
Version: 2.2

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)	Yes

Revision history

Version	Object	Date	Author(s)
0.1	Creation	05/03/2015	INOV, PJ
1.0	Revision 1	13/03/2015	INOV, PJ
1.1	Revision 2	18/03/2015	INOV, PJ, INDRA
2.0	Revision 3	17/09/2015	INOV, MELANI, FORTH, CYBERDEFCON
2.1	Revision 4	24/09/2015	INOV, HMoD
2.2	Final	30/09/2015	INOV

D6.3
Cyber Terrorism - Best Practices Analysis

Responsible
INOV

Contributors
PJ
INDRA
FORTH-ICS
CYBERDEFCON
HMoD
MELANI

Summary:

Focused on cyber terrorism, this deliverable was divided into two releases: a preliminary best practices analysis (D6.2) and a final best practices analysis document (D6.3).

The first release examined the state of collaboration between different sectors and stakeholders, with a focus on the initiatives, best practices, standards and frameworks that can be underlined to face the complex scenarios related to cyber terrorism.

This final D6.3 document, with the inclusion of the result and analysis of the surveys implemented within WP5 and WP6, gives us the opportunity to identify gaps in current knowledge, thus to draw conclusions towards a realistic set of best practices to combat cyber terrorism.

Keywords: best practices, cyber terrorism, counterterrorism, use of Internet

TABLE OF CONTENTS

1 INTRODUCTION

Starting in the 19th century, the rise of modern infrastructure systems has been increasing exponentially, assuming key roles for the economy and security of nations, particularly in the most developed ones. More recently, the increasing dependency on the Internet has brought heightened concerns about society's vulnerability to a relatively new form of risk - cyber terrorism.

Terrorists use cyberspace as a target, a weapon and also as a resource. As a target, terrorist activities are aimed at the Internet itself, its infrastructure and content (hardware and software), as well as anyone who uses the Internet in their daily lives. As a weapon, attacks are committed against physical targets (typically, critical infrastructures) using Internet resources, to produce real physical impact (i.e., damage to assets and/or death of humans). As a resource, it provides terrorists with a wide range of possibilities and applications, namely, propaganda, communication, command & control, and intelligence.

This document focuses on the best practices developed and used by different leading private and public entities to counter these terrorist cyber activities, in particular, Security & Defence organizations that work in counterterrorism.

Within the scope of this analysis we adopted the view of best practices presented by NATO:

“A best practice is a method or technique that has consistently shown results superior to those achieved with other means. It usually becomes a benchmark or standard way of doing things that multiple organizations can use. Effective practices exist at organizational, sector, national and international levels for many things, including interoperability, safety, and security. There are pockets of excellence that could be leveraged to minimize the duplication of effort and maximize security postures.” (NATO SfPS, 2014)

A more detailed discussion and definition of the concept of Best Practices is presented in the CyberROAD deliverable D5.2.

Since Cyber Terrorism is a specific domain within the more vast range of possibilities used by terrorists for centuries, it is important to mention that this D6.3 document will not refer to general counterterrorism best practices, except if they address the topic at hand.

A last note must be made on the existing limitation to directly refer to classified information, which includes most of the official documents of national and international security and intelligence agencies, discussing counterterrorism operational procedures and best practices (including in the cyber domain).

2 METHODOLOGY

The work of Task 6.2 was done in close coordination with the work of Task 6.1, to insure that the research and survey efforts were shared as much as possible. Care was also taken to avoid overlap with the work developed within Task 5.2.

This research was conducted using public open source documents complemented with inside classified information on the subject. All documents are unclassified and openly available for viewing (unless stated otherwise). References used for the analysis of the topics were found via the Internet. Examples of works cited are unclassified government documents found on government websites using the search terms related to the topics. Internationally distributed newspapers were also used to support the construction of this report. Other valid and reliable sources used in collecting data were government websites for agencies such as the Federal Bureau of Investigations, Europol, ENISA, NATO, etc. Additional research was pursued utilizing college and university websites that posted studies of similar matters. Furthermore, books written by experts were examined and relevant information was extracted to reinforce the views within this text.

Task 6.2 also used the results of the surveys of Tasks 5.1 and 6.1, related to Best Practices dealing with cyber terrorism, which were submitted to national stakeholders that partners considered appropriated in the respective Member States, as well as other relevant parties in Europe.

Ultimately, after gathering, collecting and analysing data from all the above-mentioned sources and finding the gaps between current knowledge and possible new phenomena, it was possible to draw conclusions related to best practices to combat cyber terrorism.

3 CURRENT BEST PRACTICES ANALYSIS

Terrorism, in all its manifestations, affects us all. The use of the Internet to further terrorist purposes disregards national borders, amplifying the potential impact on the victims. In this section, we elaborate on the state of the art for best practices to counter cyber terrorism at leading International Organizations, within the European Union, and also identified applicable international standards and frameworks that could be of use.

It is worth mentioning that several countries around the world created specific departments exclusively dedicated to combat cyber terrorism (ex: the Cyberterrorism Defense Analysis Center [CDAC] within the US Department of Defense Cyber Command [USCYBERCOM]). Almost all information related to these entities is classified and for this reason they are not mentioned in this report.

3.1 INTERNATIONAL ORGANIZATIONS

3.1.1 NATO – NORTH ATLANTIC TREATY ORGANIZATION

NATO's essential purpose is to safeguard the freedom and security of its members through political and military means. In November 2002, at the Prague Summit, NATO leaders initiated a new NATO Cyber Terrorism Program in order to strengthen its capabilities to defend against cyber-attacks.

On April 2008, in response to Estonia attacks in 2007, NATO defined a Policy on Cyber Defence, established at the Summit held in Bucharest, and created the NATO Cyber Defence Management Authority (CDMA). NATO leaders also agreed with the creation of the NATO Cooperative Cyber Defence Center of Excellence (CCD-CoE), based in Tallinn, who's mission and vision is "to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation" and to be "the main source of expertise in the field of cooperative cyber defence by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners"[i] (CCD-CoE).

On 4 May 2010, the Council agreed the Secretary General's proposal to establish an Emerging Security Challenges Division (ESCD) in order to address a growing range of non-traditional risks and challenges by consolidating in one entity the expertise spread-out across the Headquarters.

ESCD has been operational since 1st August 2010. The Division is structured around six sections and one directorate:

- Counter Terrorism Section (CT)
- Cyber Defence Section (CD)
- Energy Security Section (ES)
- WMD Non-Proliferation Centre (WMDC)
- Strategic Analysis Capability (SAC)
- Economics and Security Assessments (ESA)
- Nuclear Policy Directorate (NPD)

Cyber Defence section incorporates the Cyber Threat Assessment Cell to further enhance organization's cyber defence capabilities by providing timely and accurate cyber threat reports and warnings, including cyber terrorism.

On 1 July 2012, the NCI Agency was created through the merger of the NATO C3 Organisation, NATO Communication and Information Systems Services Agency (NCSA), NATO Consultation, Command and Control Agency (NC3A), NATO Air Command and Control System Management Agency (NACMA), and NATO Headquarters Information and Communication Technology Service (ICTM).

NCIA key objective is to deliver advanced Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) technology and communications capabilities in support of Alliance decision-makers and missions, including addressing new threats and challenges such as cyber and missile defence.

In this context, cyber security is responsible for providing the broad spectrum of services in the following special security areas: CIS Security, Cyber Defence, Information Assurance, Computer Security & Communications Security. Cyber Security incorporates the NATO Computer Incident Response Capability (NCIRC) Technical Centre, providing specialist services to prevent, detect, respond to and recover from cyber security incidents.

NATO has sponsored several studies and programs that have produced guidelines and listed best practices, that all entities are encouraged to follow. Two relevant examples are presented below, which are related to cyber security and cyber defence (and also relevant in the specific case of cyber terrorism):

National Cyber Security Framework Manual
NATO Cooperative Cyber Defence Centre of Excellence (CCD-CoE), 2012

"The 'National Cyber Security Framework Manual' does not strive to provide a single universally applicable checklist of things to consider when drafting a national cyber security strategy. Rather, it provides detailed background information and theoretical frameworks to help the reader understand the different facets of national cyber security, according to different levels of public policy formulation. The four levels of government – political, strategic, operational and tactical (technical) – each have their own perspectives on national cyber security, and each is addressed in individual sections." (CCD-CoE)

Best Practices in Computer Network Defense: Incident Detection and Response
NATO Science for Peace and Security Series - Information and Communication Security, 2014

"An Advanced Research Workshop (ARW) entitled 'Best Practices in Computer Network Defense (CND): Incident Detection and Response' was held from 11 to 13 September 2013 in Geneva, Switzerland, to exchange expert knowledge in cyber defense and discuss approaches and solutions to this emerging security challenge. Participants were selected from industry, academia, and public institutions, which have direct hands-on experience with and responsibilities for incident detection and response. In summary, twenty-one specific findings outlined how NATO member state and partners can improve their respective and collective cyber defense postures." (NATO SfPS)

3.1.2 UN – UNITED NATIONS

The United Nations (UN) has cybersecurity as one of its main themes in the traditional debates on the security policy. The International Telecommunication Union (ITU) of the UN also has potential responsibility in cybersecurity, by intending to develop confidence in the use of cyberspace by strengthening online security.

Several reports have been produced on this topic and one of the most relevant is the following:

The Use of the Internet for Terrorist Purposes
Report from the 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 propaganda, training and financing, planning and executing the acts of terrorism. It also presents the opportunities offered by the Internet to prevent, detect and deter such acts.

Considering counter-narratives and other strategic communications could be an effective means of disrupting the process of radicalization by adopting extremist ideals, which may in turn be manifested through acts of terrorism; understanding of the broader issues underpinning radicalization is also important in engaging in constructive dialogue with potential recruits to a terrorist cause, and in promoting alternative, lawful means to pursue legitimate political, social or religious aspirations. Respect for human rights and the rule of law is an integral part of the fight against terrorism. In particular, Member States reaffirmed those obligations in the United Nations Global Counter-Terrorism Strategy, recognizing that "effective counterterrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing". The effective implementation of a rule-of-law approach to combat the use of the Internet for terrorist purposes must be continually assessed during all stages of counter-terrorism initiatives, from preventive intelligence-gathering to ensuring due process in the prosecution of suspects (UN, 2012).

3.1.3 OECD – Organization for Economic Cooperation and Development

The Organization for Economic Cooperation and Development (OECD) guidelines for the Security of Information Systems and Networks, issued in 2002 by the Directorate for Science, Technology and Industry of OECD, have become a reference for national and international cyber security actions. These guidelines are based on nine principles of safety culture:

Organization for Economic Cooperation and Development (OECD)		
9 Principles of safety culture	Awareness	Security of information systems and networks
	Responsibility	Responsibility of all participants for the security of information systems
	Response	Capacity to act on security incidents on timely and co-operative manner
	Ethics	Respect the legitimate interests of other users and promotion of best practices

	Democracy	Security measures should follow the democratic values
	Risk Assessment	Broad assessment of threats and weaknesses
	Security Design and implementation	Software designed from the ground to be up to be secure
	Secure management	Involving all stakeholders at all levels, addressing threats as they appear
	Reassessment	Continuous review, revision and modification of security measures as risks evolve

Table 1: Nine Principles of Safety Culture

More recently, the OECD has also sponsored work on terrorism risk and insurance markets (2012), which is a topic of growing relevance in the cyber domain.

3.1.4 OSCE – Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe (OSCE) in the last decade has fomented the international cooperation and made a major effort to protect vital critical information infrastructures and networks from the cyber-attacks. Directions were given to participating countries in order to strengthen the monitoring of terrorist and extremist organizations webpages, and to exchange information with other governments in the OSCE, the monitoring of relevant forums, and suggested more involvement of the civil society institutions and the private sector in preventing and countering the use of internet for terrorist purposes.

3.1.5 CoE – Council of Europe

Council of Europe (CoE) signed the Convention on Cyber Crime, in November 2001 (only applied in July 2004), addressing cyber security threats and establishing common standards and procedures open to the Member States and others.

The CoE also introduced requirements for handling data and accessing it, due to the issues of privacy and civil liberties, that have became an important issue, that often conflicts with the actions to counter cyber terrorism.

3.1.6 G-8 – Group of Seven plus European Union

In line with the international cyber security policy, the G-8 created a Sub-group of High-Tech Crime to combat transnational organized crime, with the goal to "enhance the ability of the G-8 countries to protect, investigate and prosecute crimes committed using computers, network

communications, and other new technologies", including the use of internet by terrorists and the protection of critical information infrastructure. This G-8 sub-group has also been creating guidelines/best practice documents that could be implemented in other countries[ii].

3.2 EUROPEAN UNION INITIATIVES

Within the European Union many initiatives related to the topic of this report are under implementation. The European Commission has backed studies and programs (most of them being confidential), as well as several security projects. Of these, we highlight here "The Clean IT" project, on Reducing Terrorist Use of Internet, due to its relevance and impact.

Of relevance is also the work done by several think tanks and research teams. Without the possibility to analyse all the research in the EU in this domain, we highlight in the following sections a relevant example of the work done by the SDA – Security & Defence Agenda, as well as two examples of relevant publications by European research teams, studying cyber terrorism and its countermeasures.

3.2.1 EC – EUROPEAN COMMISSION

Study on Methodologies or Adapted Technological Tools to efficiently detect violent radical content on the Internet

This confidential EU study was commissioned by the European Commission (2012) 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 European Union for detecting online violent radical content. The best practices identified are intended to be disseminated among police forces in the EU.

The Clean IT – Reducing the Impact of the Terrorist Use of Internet

"The Clean IT" project (www.cleanitproject.eu) was started in June 2011 with the financial support of the European Commission and five government partners. It was the result of a structured public-private dialogue between government representatives, academics, Internet industry, Internet users and non-governmental organizations in the European Union. The project has the following objectives:

(1) To start a constructive public-private dialogue about terrorist use of the Internet;

(2) To draft a set of "general principles" that are supported by both public and private parties;

(3) To identify "best practices" which, after possible modification, could in the opinion of the Clean IT participants contribute to a successful reduction of the impact of terrorist use of the Internet.

The 'General Principles' mentioned above determine nine conditions for any action taken to reduce the terrorist use of the Internet.

In 2013, "The Clean IT" project has also put forward 13 best practices that could reduce the terrorist use of the Internet in the EU. For each best practice, it has also been presented, the challenge that best practice is meant to overcome, what the best practice consists of, as well as more detailed explanations and considerations on the best practice.

A full list of the proposed best practices can be found in:

http://cleanitproject.eu/files/95.211.138.23/wp-content/uploads/2013/01/Reducing-terrorist-use-of-the-internet.pdf

As this emerged from a public-private dialogue, any future implementation can only be voluntary and according to existing laws and regulations.

3.2.2 SPANISH CENTER FOR CYBERSECURITY IN INDUSTRIAL CONTROL SYSTEMS

The Spanish Center for Cybersecurity in Industrial Control Systems made a relevant effort targeted to assess good practices to diagnose cybersecurity in Industrial environments [CCI, 2014]. The report highlighted that there are no standard methods to assess the cybersecurity in ICS (Industrial Control Systems). Thus they propose a methodology with four main steps:

1) Preparation: this phase is oriented to elaborate a deep knowledge about the current environment.
2) Fieldwork: it implies to visit physically the facilities; the auditors will examine the target of evaluation. The objectives are: 1) Gathering information and 2) Verifying information.
3) Report development: after the previous phases the auditors will have tons of information that should be properly organized. At least the report should have an executive summary, current state and recommendations.
4) Presentation of results: In this phase the result will be presented avoiding technical terms to guarantee a good understanding of all the command echelons.

In addition to these guidelines to assess cybersecurity in ICS, the report recommended some best practices to improve the technical aspects in cyber security for ICS. Among these technical best practices are:

- Segmentation and filtering: the security areas should be identified and segmented by means of filtering devices able to control the traffic between two different zones.
- DMZ (Demilitarized Zone) for Operations: The communications between the corporative network (Email, ERP, etc.) and the industrial network will not be made directly, all the traffic will pass through the DMZ network.
- Routing policy: Multihomed servers will be avoided since they can serve as a bridge between different areas. All communications between networks should be made by

routing devices able of filtering communications according to security policies **as restrictive as possible.**

- Separation of engineering and operation: Engineering workstations and operation should be in separate security zones to prevent security incidents in one of the areas from spreading to others.
- Specialized security hardware: the firewalls to split critical areas of the network should be able to identify the context of industrial control communication protocols.
- Coherent network addressing: the network addressing used in facility should be coherent with that used in the rest of the organization, to avoid public addressing in internal systems and to allow their easy and secure expansion.

3.2.3 RESEARCH & THINK-TANKS

SDA – Security & Defence Agenda

Cybersecurity: The vexed question of global rules. An independent report on cyber preparedness around the world (SDA, February 2012)

The Security & Defence Agenda (SDA) is Brussels' only dedicated security and defence think-tank. Its activities include debates, international conferences and a range of publications.

The above mentioned report is made up of a survey of some 250 leading authorities worldwide and of interviews carried out in late 2011 and early 2012 with over 80 cyber-security experts in government, companies, international organizations and academia. It offers a global snapshot of thinking about the cyber threat and the measures that should be taken to defend against it, and assesses the way ahead.

CENTRIC – Centre of excellence in terrorism, resilience, intelligence & organised crime research, Sheffield Hallam University

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 also explores the technological and social aspects of managing information for contemporary national security imperatives."

One of the articles contains a list with a brief summary of the different categories of people involved and a brief analysis of their training needs. It also gives an extended list of countermeasures in order to promote a culture of cyber hygiene and vigilance, with people and

organizations following security policies, using strong passwords, regularly applying security patches, and so forth, would make a cyber terrorist's work more difficult.

The Cyberterrorism Project, Swansea University (UK)

Cyberterrorism: A Survey of researchers (March 2013)

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.

"This report provides an overview of findings from a project designed to capture current understandings of cyber terrorism 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."

Concerning the most effective countermeasures against cyber terrorism, most respondents indicated: **target-hardening, greater international cooperation, refusing to exaggerate the threat, utilizing the same responses as for cybercrime, preventing radicalization**.

As to the question concerning the differences to more traditional forms of counter terrorism, the most common answers were: same strategies with different methods, greater technical expertise required, greater role of private sector, greater role for individual citizens.

3.3 STANDARDS AND FRAMEWORKS

The European Union, with the support of ENISA, has started to include standards in its strategies and policies, but much remains to be done. The development and use of standards is necessary, timely, and requires the involvement of public and private sector actors working in tandem. (PURSER, 2014)

According to Cyber Security Strategy of the European Union (EU CSS) of 04/02/2013, to ensure a high level of security at the EU level, Members States were asked to support standardization in the area of Network and Information Security (NIS). The EU CSS contains the following:

> *"The importance of 'commercial and non-governmental entities, involved in the day-to-day management of Internet standards";*
>
> *'A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establishing voluntary EU-wide certification schemes building on existing schemes in the EU and internationally";*
>
> *The Commission will support the development of 'security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing".*

Apart from the EU, there are also several relevant entities that regularly publish security standards and guidelines.

The NIST (USA) is a prime example: "The Computer Security Division's (CSD) Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia." (NIST)

Other examples include: the Australian Government, that published Strategies to Mitigate Targeted Cyber Intrusions; the British Standards Institute that published Cyber Security Risk – Governance and Management Specifications, and the European Energy Regulator (ENTSO-E European Network of Transmission System Operators for Electricity), that in its Network Code on Operational Security recommends that operators define comprehensive organizational, logistical, and technical plans, with a particular attention to alert, detection, and restoration procedures.

4 CYBERROAD SURVEYS

The use of surveys to receive up-to-date input, directly from stakeholder in the counter cyber terrorism domain, was considered of high relevance. To avoid duplication of efforts, Task 6.2 made use of the surveys developed within tasks 5.1 and 6.1 of WP5 and WP6.

4.1 WP5 SURVEY

4.1.1 WP5 SURVEY RESULTS

Within Task T5.1, three surveys were developed, full details of which are presented in D5.1. In brief, the surveys were designed using a Delphi approach beginning with an initial poll, from which it is possible to drawdown and to generate other polls out of the analysis, and which enables deeper probe in the later stages. In Survey #1 Cybercrime, participants were asked if they would be interested in contributing to the next stage where more specific questions, based on previous responses, would be available to answer. Participants voluntarily responded across a broad range of occupation types including, for example, policy makers, technologists, users, etc.

Analysis of the surveys contributed to the deliverables of other work packages, mainly to WP3, Social, Economic, Political, and Legal Scenario, and WP5, Cybercrime, as well as towards the formulation of the CyberROAD roadmap. Although not directly relating to WP6, Cyber terrorism, for which a specific survey was carried out, some questions asked in the WP5 surveys help to provide valuable insights into a number of issues that could equally be applied to attacks coming from cyber terrorists or from cybercriminals, and which could potentially impact on stakeholders in a variety of ways. It should be noted that, by definition, cyber

terrorism is an act using cyber means to create fear and terror in citizens with attribution to unknown actors, non-aligned groups or individuals. Attribution is the key element here, for example, if such act can be determined as being carried out by a nation or state, it is an act of war, namely, of cyber war. However, in the early stages of an attack it may not be possible to determine who the attackers are: the attack methods can be utilized rather universally.

Survey #1 explores general themes within the topic of Cybercrime while Survey #2 concentrates on issues relating to Technology & Organization, and Survey #3 on Social, Economic and Political themes. Whilst none of these areas directly explore cyber terrorism and best practices, answers to the questions on technology, for example, provide evidences on the gaps in practices that either cyber terrorists or cybercriminals could exploit. Stakeholder views on these issues help to provide valuable insights on some of the common practices and mal-practices, from the ground up, as well as pointing towards areas where gaps in research may exist.

4.1.2 WP5 Survey Results Analysis

In Survey #3 - Social, Economic and Political Issues, participants were asked, "How real a problem do you think cyber espionage is?"

Cyber espionage is topically related to cyber terrorism especially when the act is from hitherto unknown actors. Such acts are typified with the deployment of APT (advanced persistent threats) to attack infrastructure and disrupt cyber communications or, for example, data breaches, where the main targets are data, plans, designs, cyber materials, etc. This is regardless of whether the victims are the state or commercial entities.

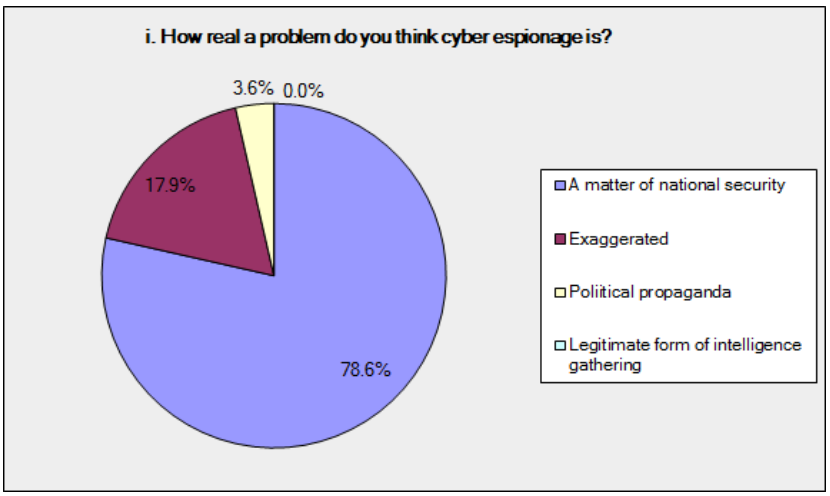

Figure 1: Survey #3 Respondents Views on Cyber Espionage as a Problem

Respondents to Survey #3 consider cyber espionage to be one of the leading cyber security matters for EU citizens and view it as a real problem for national security.

Adopting best practices within a managed security policy can help improve the cyber security posture of organizations whether the potential for attack originates from cyber terrorists or cybercriminals. Building in cyber resilience is a key component of the International Standard ISO27001. In Survey #1 participants were asked: How often staff is given training on cyber security risks? The responses are outlined below:

Weekly	5.6%
Monthly	8.8%
Yearly	22.7%
Never	16.4%
Only if there is a problem	25.4%
Don't know	21.1%

Participants were further asked: Does your organization allow the use of Bring Your Own Devices (BYOD)? The results are as follows:

Yes	65.5%
No	34.5%

The next question then asked:

Does your organization have a Best Practices Policy for BYOD? The responses are detailed here:

Yes	28.2%
No	41.5%
Don't know	30.3%

The results indicate that there is wide adoption of Bring Your Own Devices (BYOD), but with a lack of corresponding Best Practice Policies in place. This indicates that, in the majority of cases, there is a potential gap in the cyber resilience of respondents' organizations. This together with results that indicate a lack of regular staff training, reveal key areas where research and improved cyber resilience are needed.

4.2 WP6 SURVEY

4.2.1 WP6 SURVEY RESULTS

Within Task T6.1, one survey was developed and processed, which has specific interest for T6.2. The details of this survey are presented in document D6.1.

The main purpose of the questionnaire was to gain further insight on the issues of cyber terrorism and the potential threats and needs involved. Furthermore, there was a need to identify gaps and derive best practices based on the answers provided to a well-structured set of questions addressed to diverse group of stakeholders and to identify differences with the existing literature in the dynamically changing landscape of cyber terrorism.

The questionnaire was presented to a large and diverse group of stakeholders from different countries and organizations. Mainly, the countries with which the partners had ties were considered. Stakeholders from the following countries were contacted: 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. The type of organizations that received the questionnaire included: LEA, Justice Infrastructures, Universities, Health service providers, Rail infrastructures, Road transport companies, ISPs, CERTs, SMEs and Large Enterprises. A total of 90 organizations, partially (56 entities) or fully (34 entities) participated in the survey.

The survey was structured in five different sections in order to help to achieve a spherical perception of the situation and to unveil the major facets of the problem and how it is perceived in various countries and organizations. These sections were: Concept of Cyber terrorism, Legal System, Guidelines, Best Practices, and Plan of Incident Response. Most of the questions were of multiple choices while some allowed open answers. Although, this may have presented some extra difficulty in answering the questions, the results signify that it worth including the extra sections. Finally, the respondents were given the option to reply to the questionnaire anonymously, not identifying their organizations.

4.2.2 WP6 Survey Results Analysis

A total of 90 questionnaires were filled in (56 partially and 34 fully). From the organizations participating in the survey, the majority (41%) was from the legal and law enforcement sector, while 33% were governmental. For the rest, 7% were military and defence organizations and another 7% were academic institutions. A definition of Cyber terrorism was presented in the questionnaire, with which 70% of the respondents agreed, while the ones that did not fully agree did not suggest or give any guidelines for an alternative definition.

Concerning the legal system, answers were received only from countries that have cyber terrorism integrated into their legal system, namely, Portugal, Belgium, Spain, Italy, Greece, Hungary and the UK. Major challenges and gaps in relation to the legal system were identified by stakeholders in these countries, the most important of which are the following: competence of police personnel, cooperation and harmonization of national legislation at European level, raising public awareness, difficulty to follow innovation and lack of specialized units and personnel to cope with the problem.

With regard to the issue of guidelines and best practices, only 23% responded that their organizations have guidelines for security threats enumerating some of them. Concerning guidelines and best practice availability for cyber terrorism, only 9% responded positively, raising a major issue for large European organizations lacking a concrete set of policies and procedures for their personnel on how to deal with security threats and certainly cyber terrorism.

Subsequently, the stakeholders were requested to identify the three best practices to cope with cyber terrorism. This question raised the issue of international cooperation, the coordination among security forces as well as the exchange of information. Other issues revealed related to risk management and enhancement of police forces. Only 18% of the stakeholders replied positively to the question "Does you organization provide a plan incidence response?", thus identifying a major gap in this domain.

The stakeholders were then provided with a list of eight different domains of cyber security and were asked to rate them in relation to their importance for cyber terrorism. The answers identified three major issues, which are the following: System protections of servers/PCs (74%), Critical infrastructures protection/prevention (67%) and Education/Awareness (58%). Secondary issues included Ethical domains research (32%) and Political/social interventions (26%). Training and Staff were identified as the main resource required to achieve the aforementioned goals.

The next section of the survey asked the stakeholders to elaborate on the required Needs in order to deal with cyber terrorism. In this question Portugal, Belgium, Spain, Italy, Greece, and the UK responded. The answers can be summarized using the following keywords/key phrases: awareness, tools, police training, and the existence of a specialized unit.

The final part of the survey helped to understand the level of cooperation of stakeholders with the cyber security sector. A small number of organizations answered positively and only two briefly elaborated on the type of cooperation. A follow-up to this question concerned the level of PP (Public-Private) cooperation, to which only a small percentage answered positively, identifying another major issues in relation to cyber terrorism. Concerning prevention, only 3% of the organizations answered that there is a prevention policy in place by their organization. Finally, the domains identified as the most important to fight cyber terrorism were Cooperation between business sector and government (26%), Legal Framework (26%) and Technological Security Techniques (16%).

The survey helped identify major gaps in the fight against cyber terrorism in Europe, to raise important issues and to help identify tools and instruments that major stakeholders in the area consider to be the most important. A summary of these is given below:

- There is a need for specialized units equipped with highly qualified staff that will be competent enough to follow the innovation capacities of terrorists and respond proactively to the emerging threats.
- The creation of specialized police units to monitor the cyber environment, identifying contents of a violent extremist or terrorist nature and working closely with the industry is imperative. Specialized police units should be equipped with appropriately trained personnel. Police cooperation among individual countries should be improved.
- There is a need for fast and agile harmonization of national and European legal frameworks. Furthermore the legal frameworks must be dynamically adapted to the various threats and needs identified.

- Increase the development of training programs for judges, public prosecutors and criminal investigators.
- There is a need for a set of best practices (program, policies, and procedures) in major organizations on how to deal with security threats and cyber terrorism.
- A common strategy at European level to increase the level of public awareness should be set in place.
- The cooperation between public and private sectors is a major issue.
- Specialized training programs designed for social media should be devised.

5 CONCLUSIONS

Investigating best practices in combating cyber terrorism, we first defined the methodology, which is based on using public open source documents (complemented with knowhow from classified information on the subject) and by results of the surveys carried out within the framework of Tasks 5.1 and 6.1, related to best practices dealing with cyber terrorism.

This definition was followed by the comprehensive analysis of the issue carried out in Section 3 with respect to international organizations, the EU supported initiatives, and implementation of the pertinent international standards and frameworks. This analysis identified a wide range of best practices already specified and some being at different stages of implementation. In particular, "The Clean IT" EU-funded project has put forward some best practices that could reduce the terrorist use of the Internet in the EU, whose complete list can be found in the online document:

http://cleanitproject.eu/files/95.211.138.23/wp-content/uploads/2013/01/Reducing-terrorist-use-of-the-internet.pdf

Most of the countermeasures and practices developed for cyber terrorism, as well as the revealed gaps, are akin to those identified for cybercrime. It should be noted that they are not exhausted by the open access lists and publicly discussed issues: due to the specificity of the subject, many efficient practical measures and discovered weaknesses are strictly classified and thus are not discussed in this document.

The CyberROAD surveys, from both WP5 and WP6, highlight very similar findings and gaps related to cyber security best practices against both cybercrime and cyber terrorism. Those practices can be divided in three major categories: legislation, technology, information sharing.

Substantial differences between national legislations and weakness of international law to implement common and wide accepted legal measures or procedures, leads to the conclusion that further analysis is required along with deeper cooperation between different entities in order to provide a solid methodology and solution of how to tackle cyber terrorism activities. With attribution being a significant drawback, more effort has to be done towards the

releasable information exchange between involved entities, in a way to offer a trusted and safe environment for efficient response.

Current cyber security technology reflects what most organizations have in place regarding protection and prevention from cyber-attacks. It has been highlighted that existing solutions comprised of firewalls, early warning systems, intrusion detection systems, data encryption and security and event management systems are the key components that will provide improvement on security posture of every organization. However it has been identified that technical expertise and highly skilled personnel is missing and therefore those technologies cannot solve the problem alone. More education and training is needed also in the area of user security awareness, which remains the weakest link. Although most of the organizations include in their strategies security awareness programs, there aren't any metrics or standards of how to measure the efficiency of such programs.

Last but not least, there is the need for information exchange best practices. It is common that among counter terrorism entities there is an established communication channel that is classified. Therefore it wasn't feasible in our surveys to include any relevant sensitive information. However, since cyber terrorism has common areas for investigation with traditional one, it could be a good approach to use existing methodologies for information exchange. At this point we should also highlight that along with current security solutions, cyber threat intelligence should be also integrated in a multi layered security infrastructure. In a similar way national intelligence authorities have developed their information exchange channel in order to share confidential information. Cyber intelligence should also use similar practices in order to better define and determine the right cyber security measures tailored to each organization's specific threat environment.

Summarizing the results, best practices analysis revealed the need for technology improvement as well as expertise development. While user security awareness remains one of the key factors for improving security, it is always not enough. Best practices should also focus on information exchange and cyber threat intelligence solutions, in order to provide more proactive options in security operations.

Additionally, a prompt response capability with respect to a cyber terrorism incident is identified as a key requirement for improving the overall security posture. Further analysis on existing, but classified best practices, should also be done in order to pave a way for wide implementation of successful and tested methodologies in the cyber domain.

Awan, I. (2014). *Debating The Term Cyber-Terrorism: Issues And Problems.* Retrieved 12/05/2015, from Internet Journal of criminology: www.internetjournalofcriminology.com

Axelos. (n.d.). *AXELOS - Global Best Practices*. Retrieved 13/05/2015, from ISIL

Bravo, R. (2010). *Do espectro de conflitualidade nas redes de informação: por uma reconstrução conceptual.* Polícia Judiciária.

[CCI, 2014] Centro de Ciberseguridad Industrial (2014). Buenas prácticas para el diagnóstico de ciberseguridad en entornos industriales.

European Comission. (2013, January). *Reducing terrorist use.* Retrieved 13/05/2015, 13, from Clean IT project: http://www.cleanitproject.eu/files/wp-content/uploads/2013/01/Reducing-terrorist-use-of-the-internet.pdf

Detica. (2011). *The cost of cyber crime*. Retrieved 29/04/2015, from http://goo.gl/C6RD3X

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

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

Lipovetsky, G., & Hervé, J. (2010). *L`Occident Mondializé - Controverse sur la culture planétaire.* Éditions Grasset & Fasquelle

NATO, CCD-CoE. (2012). *National Cyber Security Framework Manual.*

NATO, Science for Peace and Security Series. *(2014). Best Practices in Computer Network Defense: Incident Detection and Response.* Available at:

http://www.nato.int/cps/en/natolive/news_109346.htm

NIST. (n.d.). *Computer Security Resource Center (CSRC)*. Retrieved 13/05/2015, from National Institute of Standards and Technology: http://csrc.nist.gov/

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

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

SDA. (2012). *Cyber-security: The vexed question of global rules. An independent report on cyber-preparedness around the world*

University, S. (2013). *Cyberterrorism: A Survey of Researchers.* Retrieved 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.* Retreived 02/04/2015, 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.* From Justiça e Segurança Interna.

WEIMANN, G. (2005). *Cyberterrorism: The Sum of All Fears?* Retrieved 02/04/2015, from Princeton: http://webcache.googleusercontent.com/search?q=cache:1VhpnHIEXyoJ:www.princeton.edu/~ppns/Docs/State%2520Security/Cyberterrorism%2520-%2520sum%25200f%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://www.oss.net/dynamaster/file_archive/080219/951848ff4f05d48a630d5f1d385e8742/II-07-03%20Weinberger%20Open%20Spectrum%20445-454%20(18%20Feb%2008)%20SP%20FINAL.doc.

Winters, R. (2013, 07 02). *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/

---

[i] https://ccdcoe.org/about-us.html

[ii] G-8 Principles for Protecting Critical Information Infrastructures: adopted by the G-8 Justice & Interior Ministers, May 2003 (http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf) (G-8)