CyberROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

D3.1 - Social, Economic, Political and Legal Landscape Report

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

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

Project funded by the European Commission Directorate-General Home Affairs in the Prevention of and Fight against Crime Programme		
Restriction Level		
PU	Public	Yes
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)	No

Revision history

Version	Object	Date	Author(s)
0.1	Creation	01/08/2014	RHUL
0.2	Revision	01/03/ 2015	RHUL, CyberDefcon, NCSRD
0.3	Revision	06/05/2015	PJ, RHUL, NCSRD, CyberDefcon
0.4	Revision	07/05/2015	PJ, RHUL, NCSRD, CyberDefcon
0.5	Revision	12/05/2015	UNICA, CyberDefcon
0.6	Revision	13/05/2015	RHUL
0.7	Revision	15/05/2015	RHUL
0.8	Revision	21/05/2015	RHUL
0.9	Revision	22/05/2015	RHUL
0.10	Revision	26/05/2015	RHUL
0.11	Revision	26/05/2015	PJ, SBA, RHUL
0.12	Revision	27/05/2015	UNICA
1.0	Final draft	30/05/2015	RHUL

DT3.1
Social, Economic, Political and Legal Landscape Report

Responsible
RHUL

Contributor(s)
UNICA
CyberDefcon
PJ
NCSRD
SBA
RHUL

Summary: This document outlines the current social, economic and legal landscape that forms the backdrop to cybercrime and cyberterrorism analysis.

Keywords: cybercrime, cyber terrorism, security, privacy

TABLE OF CONTENTS

1 INTRODUCTION

1.1 *MANAGEMENT SUMMARY*

This deliverable provides a thumbnail sketch of the combined social, economic and legal landscape in order to frame the subsequent discussions of cybercrime and cyber-terrorism that lie at the heart of the remaining work packages.

This deliverable starts with a sociological framing of the concepts related to cybercrime and cyberterrorism and then develops this concept with an explanation of the motivations that drive cybercrime. This framing groups cybercrime into psychological cybercrime, economic cybercrime and geopolitical cybercrime with cyberterrorism specified as a form of geopolitical cybercrime. After setting the theoretical underpinnings of the conceptualisation of cybercrime, the deliverable takes a closer look at the dominant socio-economic, political and legal thinking towards cybercrime.

The deliverable contributes three main products: a) a summary of the dominant thinking across the social, economic, legal and political literatures of cybercrime 2) a taxonomy of cybercrime that synthesises the main perspectives on cybercrime found across the social sciences 3) a survey on cybercrime victimisation and attitudes towards cybercrime.

1.2 *BACKGROUND TO THE WORK PACKAGE*

Work package three is focused on the social, economic, political, and legal aspects of cybercrime. In particular, there are two main goals - firstly, to identify and characterise with a solid scientific methodology how the main cyber-threats can affect Social, Economic, Political, and Legal rights of citizens and stakeholders; secondly, to provide as a final output a list of research topics which are important for the protection of social, economic, political, and legal rights of citizens and stakeholders.

We begin with the premise that if cybercrime and cyberterrorism were problems that could have been solved putting in place the adequate technical solutions, probably we would have solved them several years ago. What we are actually lacking in the fight against cybercrime and cyberterrorism are not sophisticated cyber weapons but instead a social scientific analysis of legal, ethical, and political scenarios that lie behind cybercrime and cyberterrorism phenomena. Cyber attacks do not depend only on vulnerabilities or misconfigurations of the electronic building blocks of the cyber space but also on economic and political motivations. Enablers for cyber attacks are not exclusively the innovative electronic devices that are continuously put on the market, but also the wrong usage of them that we make within our modern societies.

This work package has a focus on the following objectives:

1. Identify the roots of cybercrime and cyber-terrorism, in terms of:

• social, economic and political motivations;

• common habits of the modern societies that enable cyber attacks;

- gaps in the existing international legislation, and ethics issues that do not allow possible effective combat of cybercrime and cyber-terrorism.

The roots of cybercrime and cyberterrorism are identified in this deliverable, 3.1, the concerns and needs of different stakeholder groups are defined in deliverable 3.2 and a presentation of the research gaps in the social, economic and legal aspects of cybercrime are fully described in the deliverable 3.3. This deliverable therefore focuses on the theoretical underpinnings of our conceptualisations of cybercrime and explores the empirical data and the legal instruments that shape our responses to cybercrime.

2 STATE OF THE ART IN CRIME, CYBERCRIME AND CYBERTERRORISM RESEARCH

This section examines the conceptual and analytical problem of cybercrime. It is important to understand the complexity of the problem before embarking on a description of the social, economic and legal landscape in which cybercrime is situated. The advent of the internet has transformed patterns of local and global communication and the ways in which individuals interact in online spaces. How such interaction can result in individuals and groups becoming the victims or perpetrators of harmful and criminal activity has become an important subject of study. As we learn more about what constitutes cyber criminal activity, and its social, psychological and economic costs, we discover greater legal and ethical challenges that need to be addressed in the of governance of the internet.

This section provides a framework through which to look at the psychological, organisational and geo-political aspects of cybercrime. In this section we explore the relevant literature into current conceptualisations of cybercrime, provide the reader with a summary of the main theories that examine cybercrime today, and put forward a proposal for a new taxonomy of cybercrime that brings together modes of thinking about cybercrime that are found in economics, psychology, sociology and law.

2.1 *WHAT IS CRIME?*

'an act is criminal when it offends the strong, well-defined states of the collective consciousness'

(Emile Durkheim, 1858-1917).

'The domain of criminal jurisprudence can only be ascertained by examining what acts at any particular period are declared by the state to be crimes, and the only common nature they will be found to possess is that they are prohibited by the state'.

(Lord Atkin in a 1931 case, cited in Reiner 1988:138)

The contextual and temporal nature of crime is widely discussed in the field of criminology. Power, ideology, social relationships, and the social, political, cultural and economic context play a dominant role in the conceptualisation of an act as a crime. Key elements in defining crime are generally understood to be a social consensus/collective consciousness about what constitutes a crime. Within such a framework, ideas of harm or the consequences of a criminal act for individuals, groups and the state are paramount. Such ideas are subject to change leading to a shift in the construction and concept of crime. Thus, we can see that some acts which were once criminal in most parts of the western world, such as homosexuality, are no longer conceptualised as such. Similarly, other acts which were deemed to be not issues of social or legal concern, such as intimate partner violence, or rape within marriage, are now deemed to be criminal acts which carry legal sanctions. Arguably, other acts of crime and deviance such as theft, and violence are also relative concepts when considered in the context of intentionality, context and historical time. Crime, therefore, is not a self-evident and a unitary concept. It is historically and culturally situated and encapsulated within a social and political ideological framework and this is equally true of cybercrime as it is of traditional crimes.

2.2 *CYBERCRIME AND CYBER SECURITY*

As the outputs of the deliverables across the CyberROAD work packages reflect, the notions of cybercrime and cyber security are closely related but nevertheless are conceptually distinct. Whilst cybercrime can be generalised as any type of intentional criminal scheme that is internet-mediated (Kshetri, 2006; Yazdanifard et al., 2011), cyber security can be defined as both cyberspace and physical space mechanisms that have the capacity to resist and respond to both intentional and unintentional cyberspace threats (Luiijf et al., 2013). Such threats may exist for individuals, groups, organisations, or nation-states. Similarly, the sources of these threats may emanate from individuals, groups, organisations or nation-states. The risks involved may be financial, or safety-driven. In almost all cases, data/personal information is at the centre of the potential or actual risk (Floridi 2005).

With the advancement in scientific and technical knowledge and development, theorists have argued that modern society generates its own new risks which become core to the maintenance of social order in society (Beck 1992). Cyber-space generates risks that require careful attention to ensuring security of individuals and groups. Such security can be conceptualised as multi-faced including the security that is embedded within our technical systems, within our ethical framework of privacy, trust and information sharing, and within our legal structures and processes. Crucially, technical systems do not operate in a vacuum. How we embed security in cyber-systems is contingent upon our value-framework surrounding core values around privacy, safety, trust, autonomy and agency. Such values are not and have never been absolute. For example, one of the core values/beliefs of a free democratic society is 'freedom of speech'. However, this is not an absolute right and a well-functioning democracy will weigh up the interests of diverse groups and the safety and security of its citizens in regulating such a right. Similarly, in the realm of cybercrime and cyber security, debates around the importance of privacy, for instance, are shaping how our societies are ordered now and in the future (Floridi 2005). The case studies presented as part of this deliverable provide examples of the ordering of these values differ across the EU.

2.2.1 CURRENT CONCEPTUALISATIONS OF CYBERCRIME

Whilst the definition of cybercrime continues to be perceived as a conceptual and an analytical problem, there is some emerging agreement about a general taxonomy of cybercrime. A synthesis of categorisation put forward by some scholars suggests that cybercrimes are understood as occurring in three principal ways (European Union 2007, Oates 2001, Anderson et al 2013). Namely, these constitute:

1. Traditional forms of crime including for example theft/fraud/forgery which are contingent upon the use of technology;
2. Publication of illegal content on the internet for example child pornography, hateful communication;
3. And crimes that occur within technological forums for example cyber attacks against communication/information networks including hacking, and denial of service.

In the UK, the Home Office has expressed a preference for opting for a two-fold categorisation:

1. ‘Cyber-dependent’
2. And ‘cyber-enabled’ crimes.

Here, ‘cyber-dependent’ encompasses crimes, such as hacking, viruses, and Denial of Service Attacks, which can only be committed using a computer; whilst ‘cyber-enabled’ includes traditional crimes such as theft and fraud, which are committed using computers. It is evident that both the three-fold and the two-fold dichotomies are useful in helping to promote better understanding of the nature of cybercrime. In any categorisation of cybercrime, it is important to understand the experiences of those at the receiving end of such crimes. For example, given that cybercrimes tend to be under-reported and under-recorded, it is essential to give recognition to different types of cybercrimes to assist individuals to come forward for appropriate help and assistance (Kshetri 2006, Fafinski 2010). Additionally, it is crucial to understand the nature and extent of cybercrime activity to help formulate appropriate measures to prevent and tackle this phenomenon.

It could be argued that cybercrimes are entities that are a consequence of transformations from traditional crime. These transformations arise from the creation and use of new operational methods to conduct crime and have inevitable consequence. Primarily, the separation of meaning of cybercrime in relation to traditional (or physical) crime is obscured and requires disentangling in order to provide meaningful categorisation of cybercrimes (Gordon and Ford, 2006). Currently, most efforts geared toward the conceptualisation of cybercrimes have come from legal perspectives and gaps exist to provide other perspectives. In this deliverable, we provide a categorisation that synthesises the cybercrime perspectives found in the different social sciences represented in this literature review. This synthesis enables a wider perspective on cybercrime and gives citizens, researchers, law enforcers and regulators a wider vocabulary with which to discuss cybcercrime.

Legal oriented research has argued that any significant attempt to define cybercrime must take into account the degree of dissimilarities and similarities between traditional crimes and cybercrimes (Jones and Choo, 2014; Rahman et at. 2009; Benner, 2001). These will help to ascertain if they indeed have viable and material differences and will also open possible avenues to draw a sharper contrast between them (Brenner, 2001; Jones and Choo, 2014). Specifically, Brenner (2001) examined how cybercrimes are different from traditional crimes in terms of four components: [1] conduct [2] mental state [3] attendant circumstances [4] a forbidden result or harm. Their research aimed to widen the criminal liability of cyber offences and concluded that it is too simplistic to assume that criminal conduct that exploits cyberspace represents an entirely new phenomenon. In a similar vein, Jones and Choo (2014) aimed to investigate possible avenues to modify international/national laws so as to cope with cybercrimes. They postulated that the existing international/national laws are almost impotent in the prosecution of cyber criminals (see also Sukenik, 2011; Pocar, 2004; Grabosky et al, 2004; Korns et al, 2008). Thus, technologies provide an affordance to create “new” crimes, i.e. those crimes that are not easily traceable and/or prosecutable.

Some critics have suggested that legal-oriented solutions are relatively limited in their effect (Zeller, 2005). Kshetri (2010) has argued that such solutions are fundamentally more beneficial in the geopolitical space in which they emerge, and that they may lack broader universality. Whilst acknowledging the vital importance of legal responses, Gordon and Ford (2006) have stressed the need to develop a more nuanced understanding of cybercrime. In particular, they suggest a two-fold dichotomy of cybercrime- 'techno-centric.' and 'people-centric'. Here, 'techno-centric' cybercrime is technologically oriented (such as e-commerce fraud, cyber-vandalism, data manipulations through hacking, phishing) whereas 'people-centric' cybercrime is inherently social in nature and will typically include perpetrator-victim interactions (such as cyber-stalking, cyber-bullying, cyber hate-speech etc).

It is evident that various efforts have been made by scholars to categorise cybercrime to help promote better understanding to help combat and prevent cybercrime activity (European Union 2007; Oates 2001; Anderson et al 2013; McGuire & Dowling, 2013; Gordon & Ford 2006). It would appear, however, that such classifications are limited in nature as they risk not only ambiguity and precision, but also the multi-dimensional aspects of cybercrime. Below, we discuss the levels at which cybercrime can occur, but also provide contemporary criminological and sociological theorising of cybercrime. Such explorations are employed to help develop a new taxonomy of cybercrime to offer a more nuanced picture.

2.2.2 Levels of cybercrime and their Actors

Cybercrime can occur at a number of different levels ranging from individual, group/organisation, and nation-state. Arguably, both targets and perpetrators of cybercrime can exist at these three levels. Whilst there is a growing literature into cybercrime, we lack a good understanding of the complexity of the vulnerability of targets, and the motivation and expertise of perpetrators. The relative newness, and the fluid and dynamic nature of the internet introduces new challenges in our quest to develop a sophisticated understanding of cybercrime.

As with all socially constructed concepts, cybercrime is multi-faceted and in reality contains families of related concepts. Using theoretical lenses to examine these different facets enables a better understanding of the nature of these different crimes and from there, a better understanding as to how to respond.

2.3 THEORY AND CYBERCRIME

In this subsection, we outline the main theories that examine cybercrime today. Theoretical frameworks rest on epistemic and ontological realities. In the conceptualisation of cybercrime, Wall (2007) postulates the existence of four major discourses. These include legislative/administrative (governance and legal structures and processes), academic (criminological/sociological/socio-legal/economic/computer science/information management), expert discourse (identification of trends/explanations/solutions), and popular (layperson's understanding of cybercrime). How knowledge is constructed, by whom, in what circumstances, and for what discourse rests on the positionality of the key actors. Moreover, the competing understandings are crucial in how societies move forward in forging change.

2.3.1 BACKGROUND TO THEORETICAL UNDERSTANDINGS

In nation-states, where there is a lack of 'reliable' official data into cybercrime, a 'culture of fear' can emerge about the perceived risk of such activity (Furedi 2006). For example, in contemporary British society, there is some effort on the part of police forces to record cybercrime. However, such data is currently unavailable for public consumption. It would seem, therefore, that if the main sources of the nature and extent of cybercrime remain the media, politicians/policy-makers, and security companies, this can lead to heightened public anxiety.

In the absence of relevant knowledge, it is challenging to advance theoretical frameworks that can help explain a particular phenomena. Given this context, the under-theorisation of cybercrime in the social sciences is perhaps understandable. Having said this, a few theories exist to help shine a light to promote better understanding of cybercrime. These theories are discussed in the following subsections:

2.3.2 ROUTINE ACTIVITY THEORY

This theory emerged from the work of Lawrence Cohen and Marcus Felson. In 1979, in their seminal paper in the American Sociological Review, Cohen and Felson identify 3 key components of criminal activity to help explain the paradox of rising crime rates in times of economic prosperity:

(a) Likely/motivated offenders
(b) Suitable targets
(c) Absence of capable guardians

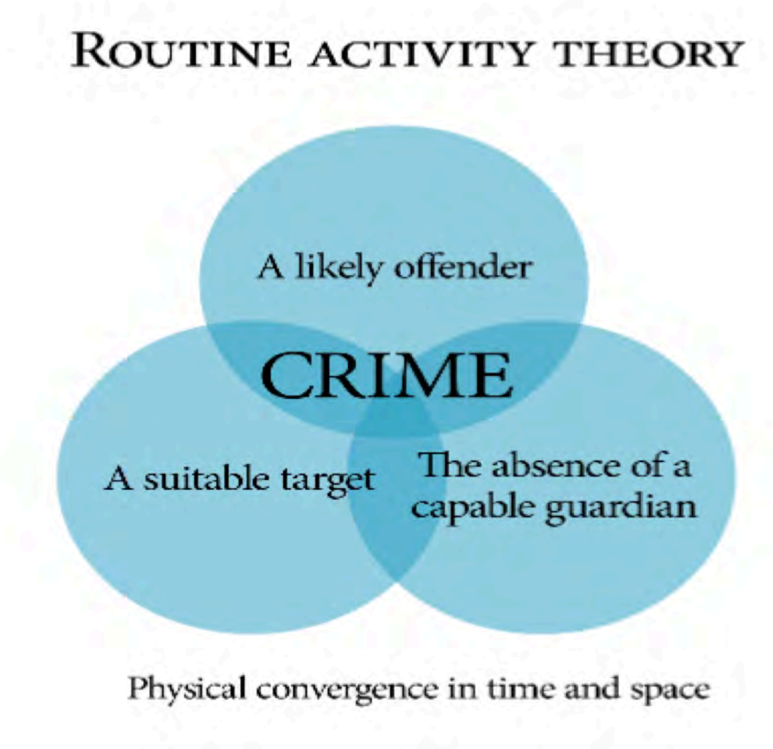

ROUTINE ACTIVITY THEORY
A likely offender
CRIME
A suitable target
The absence of a capable guardian
Physical convergence in time and space

Figure 1 – Description of Routine Activity Theory, Source: Cohen and Felson, 1979

Routine Activity Theory (RAT) holds that the spatio-temporal organisation of social activities helps people translate their criminal inclinations into action' (Cohen and Felson 1979: 592).

The applicability of RAT in promoting a better understanding of cybercrime is now being recognised, for example, in exploring how the online and routine activities of individuals can render them suitable targets for cybercrime (Pratt et al 2010). Thus, contemporary consumer practices via the internet, for example, online banking, social networking, email, and shopping can lead to risky online routines that can increase victimisation. In the absence of capable guardians (secure systems, legal protective measures, law enforcement personnel etc), individuals could become the targets of cybercrime including online identity theft, phishing, scamming, cyberbullying, cyberstalking, and trolling.

2.3.3 RATIONAL CHOICE THEORY – HACKERS – RATIONAL AGENTS

Rational choice theory is rooted in classical criminological thought. Social philosophers, notably Cesare Beccaria and Jeremy Bentham, adhered to the principles of rationality and choice. The key argument is that individuals are rational agents who will weigh up the costs and benefits of a given situation in their decision-making process. Thus, engagement in crime/cybercrime is perceived to be a rational choice (Ngo & Paternoster, 2011). This theory is closely related to the notion of deterrence in the realm of crime and punishment. The key belief revolves around proportionality in punishment. Policy making in the field of criminal justice is required to ensure that the punishment is in proportion to the crime. Here, the costs and benefits model is presented as the framework within which rational choices are made. Thus, it is argued that within the equation of cost (punishment), and benefit (economic/psychological/social gain), a would be perpetrator would exercise a rational choice in committing a crime.

Such a theory may help to explain the intent of cyber criminals in some instances. However, there are limitations. For example, hacking and cracking refer to the practices of gaining unauthorised access to a computer system. Such practices may or may not include criminal intent and/or financial gain. Arguably, the term hacking has become rather ambivalent and contested (Steinmetz, 2015). Indeed, there is no uniform and cohesive hacker sub-culture. Hackers are conceptualised in a myriad of ways including as deviant, as political activists, and as geniuses. Regardless of the type of activity, engagement in hacking may be viewed as a rational choice. However, in a climate where the costs and benefits are unclear due to uncertainty about potential benefits of hacking, and the severity of punishment, hackers may act with impunity. Indeed, it would appear that the most sophisticated and skilled hackers may face prosecution for unauthorised access to a computer system for example, but they rarely face prison sentences. Instead, their cyber-security skills are so admired that they can be invited to work for technology companies, for government and others. Such practices may do little to deter hacking.

2.3.4 SUB-CULTURE THEORY

Sub-culture theory is rooted within a sociological paradigm that emphasises the existence and powerful influence of values and attitudes inherent in some groups and sub-cultures that are conducive to crime and violence. Such a theoretical framework emerged from an understanding of juvenile delinquency during mid 20th century USA during the process of rapid urbanisation and social and cultural change (Cohen 1955, Matza 1964). Theorists stressed psychosocial factors to argue that the failure of an individual to achieve success in society led to 'status frustration' leading to the need to belong to other like-minded people who shared similar values and beliefs and sub-cultures (Cloward and Ohlin 1960). These alterative sub-cultures were described as providing the individuals with a sense of belonging, respect, and acceptance.

Arguably, sub-culture theory is premised on three key assumptions. Firstly, it is believed that agencies, actions and values of a social group are different from the majority of the population. Secondly, those from subcultural groups unlike the majority have restricted avenues to achieve their goals and as a result, they follow alternative ways, which are necessary to succeed, considering their deprived social context and disadvantaged-social economic-positions. Thirdly, subcultural theories acknowledge the unequal power relationship between subcultures and the popular culture and that the subordinate-ordinate relationship is the main source of strain. This unequal power-relation also maintains the status quo that favours the elite in perpetuating their superior social positions (Blackman, 2005). Therefore, the efficacy of the sociological concept of subcultural model is its capacity to explain cultural variations of behaviours, values and the subjective meaning of actions as dictated by socio-economic realities.

In critiquing sociological models of subculture, Matza and Sykes (1969) argued that urban youth from deprived background are attracted to delinquency, not because of oppositional morality, but because of exaggerated adherence to widely held 'subterranean' values such as the pursuit of adventure, hedonic lifestyles, excitement and leisure activities unlike other parts of the dominant values such holding down highly paid jobs, which of cause they have restricted access to in the first place. According to Matza and Sykes (1961:717) "the delinquent may not stand as an alien in the body of society but may represent instead a disturbing reflection." This viewpoint explains that subcultural theories fail to appraise that rule breaking is commonplace in society and that rule breaking involves people from a diverse social background.

A three-fold typology put forward by Cloward and Ohlin (1960) may be helpful in understanding different types of cybercrime activity. Here, it is postulated that there are in effect 'criminal subcultures' (utilitarian crime), conflict subcultures (little utilitarian crime, but need for respect through other means for example, gang violence), and 'retreatist sub cultures (rejection from sub-cultures and solace in harmful behaviour for example, drugs and alcohol). Arguably, cybercriminals generally undermine authority and the conventional rule of law. This typology can be applied in an attempt to understand the contemporary social problem of cybercrime.

2.3.4.1 Criminal subcultures

If such rule-breaking is for financial gain through utilitarian crime, we can see that the 'criminal subcultures' category may well offer some understanding (Coleman, 2010). Interestingly, 419 cybercrime scams (principally email fraud and phishing) originating in Nigeria have been explained using such a theoretical framework. For example, in an ethnographic study, Tade (2013) argues that whilst Nigerian society encourages monetary success, it provides limited legitimate means for the majority of young people. Consequently, the youth innovate alternative ways in the context of the interplay between elevated capitalist-values and deprived economic realities (Ndjio, 2012; Tade and

Aliyu, 2011). Crucially, an understanding of the socio-economic, cultural and technological context is important here to understand the nature and extent of cybercrime activity. Gordon and Ford's (2006) two-fold typology of cybercrime, that is, 'technological' (Type 1), and 'human' (Type 2), may help explain global variations in the existence of types of cybercrime. For example, in Nigeria and other African countries, the cost of access to the internet is still relatively high. Consequently, access to the internet via cyber cafes remains the predominant method for many people. This coupled with the global and local socio-economic disparities and disadvantage helps explain the dominance of Type 1 utilitarian cybercrime as opposed to cyberstalking and cyberterrorism. Notably however, Type 1 crimes are still predicated on human weakness and gullibility and it may not be helpful to perceive 419 scams as fitting this category so perfectly.

2.3.4.2 *Conflict subcultures*

It is believed that there is little utilitarian crime in conflict subcultures. However, the need for respect through other means remains strong, for example, such respect may be earned through gang violence. If we adapt such a framework to understand the cybercrimes prevalent in contemporary society, perhaps we need to substitute the earning of respect through other means such as demonstration of bravado through trolling; or through the exhibition of one's hacking skills. Consistent with most subcultural theories, Steinmetz et al., (2014) offered a bottom-up view of cybercrime by asking and appraising criminals' perspective on authority and those that represent authority. This enquiry specifically deployed subcultural framework to consider hackers as entrepreneurs, who innovate alternative means of achieving their aims (socio-economic or person-centered) as they reject the legitimacy of the rule of law (Coleman, 2010). Given the complex heterogeneity of the hacker, the conflict subculture theory may only be relevant in instances where there is little utilitarian crime, but the primeval desire is to gain respect through other means including political positionality, and technological superiority.

2.3.4.3 *Retrealist subcultures*

Here, it is suggested that individuals experience rejection from sub-cultures and seek solace in harmful behaviour for example, drugs and alcohol. One could attempt to extend this theory to those who engage in harmful online behaviours such as child pornography. It could be argued that due to the rejection for their desired activity in society, such individuals turn to the internet which provides them with the social, individual and technological means to maintain their interest in child pornography (Taylor and Quayle 2003). Moreover, evidence of peer-to-peer networks in child pornography suggest the existence of a Retreatist Subculture. However, the nature and extent of harmful engagement remains an individualised activity. Indeed, in a recent paper in the Journal of Digital Forensics, Security and Law, Rogers, and Seigfried-Spellar (2014) outline the challenges for law enforcement agencies to argue that a behavioural analysis of digital evidence is necessary to assist investigators in profiling offenders.

2.3.4.4 *Motivation theory*

Drawing from Kshetri's (2006) insights on monetary and psychological benefits/costs of cybercrime and cyber-criminals based on motivational theory, it is resourceful to look at cybercrimes categories from a sociological-oriented standpoint. A person is motivated when such a person is moved or energised, inspired to do something (Ryan and Deci, 2000). Motivation differs in terms of the orientation (the underpinnings of the actions) and also varies in terms of the degree of occurrence, i.e., whether highly motivated or otherwise. Whilst the former is concerned with the reason for the action, the latter is concerned with the amount or size of impetus behind the action. Motivation therefore, can be seen as the bedrock of most crimes and can offer a clear social conceptualisation of cybercrime. According to Self-Determination Theory (Deci and Ryan, 1985), it is actually the type of motivation that defines the amount or level of motivation.

Arguably, motivation can be conceptualised as a binary phenomenon: intrinsic and extrinsic motivations. Whilst intrinsic motivation is the demonstration of actions inherently for mere satisfactions of doing it, extrinsic motivation is the doing of an activity solely to achieve a separate result (Ryan and Deci, 2000). Broadly speaking most human activities are more likely to be extrinsically motivated. People are most likely to be motivated to do something because of the expected consequence of their actions (Ryan and Deci, 2000).

In the conceptualisation of cybercrimes, based on the theoretical foundation, Kasheri (2006) emphasises intrinsic motivation as having a superior impact in relation to extrinsic motivation. However, in this deliverable, we conceptualise both extrinsic and intrinsic motivations of cybercrimes as being intertwined and relatively the same. Support for this position is found in (Layous et al. 2013: 5) that although people intrinsically motivated might appear to be more devoted to their behavioural-course than others extrinsically motivated. This is proposed by Wehmeyer and Little (2009) who comment that 'extrinsically motivated behaviours can parallel intrinsic motivated activities' if actors internalise their actions and have flow experience in such activities. Csikszentmihalyi's (1990 & 2000) flow theory posits that flow experience is a state of profound task-absorption and task-enjoyment, most conducive when the task is moderately challenging and most likely to condition a person to lose sense of time in doing the task which he/she is involved. This condition is most probable if actors' subjective moral scripts significantly support their intended activities. In an attempt to categorise cybercrime therefore, a loose grouping of crimes according to motivations that underpin them (see Figure 1) is necessary to enhance the understanding of the different facets, actors and their actions in terms of cybercrimes (Neufeld, 2010).

In conclusion, the different cybercrime theories serve two purposes: they help to explain the motivation behind cybercrime and they explain the thinking that underpins the response towards cybercrime. With a clearer conceptualisation of cybercrime, its motivation and responses, we shall now take a closer look at our operationalisation of cybercrime.

2.4 A Proposal for a Unified Taxonomy of cybercrime

The above theoretical and empirical literature allows us to present a novel synthesis of the various efforts to present classifications of cybercrime which forms one of the main outputs of this deliverable. The synthesis is encapsulated as a taxonomy with the following characteristics. Firstly, we define cybercrime as operating with three components – namely, *Impact, Target* and *Technology* Role. An *Impact* is conceptualised as an outcome that is either *psychological*, *economic* or *geo-*

political. A *Target* is the entity that is the victim of the cybercrime and is either an Individual, an organisation or a State. A *Technology Role* incorporates the dual definition of cybercrime proposed by the UK Home Office (McGuire & Dowling 2013). Here, a technology can either be *Enabled* – that is, the technology is simply a tool to enable the enactment of a traditional crime. Or it is *Dependent*, such that, the cybercrime is contingent on the availability of that technology and is a new form of crime with its own ontological reality.

This taxonomic structure allows the representation of a cybercrime from both the perspective of the victim and the perpetrator. For example, a perpetrator may have the intent to create a psychological impact and conversely, the victim will experience a psychological impact.

We envisage operationalisation of this taxonomy by a mechanism that allows any cybercrime to be encoded by references to the three defining characteristics described above. We provide two examples.

Cyberstalking is a transformation of a traditional crime that has been technology ***enabled***. The impact of that crime is one of a ***psychological*** nature and it operates at an ***individual*** level.

Cyberstalking => [(Psychological) AND (Individual) AND (Enabled)]

Malware is a type of cybercrime that is clearly technology ***dependent***. It impact is primarily ***economic*** and the target can be an ***Individual*** or an ***Organisation***.

Malware = > [(Economic)] AND (Individual OR Organisation) AND (Dependent)]

Figure 2: A Proposal for a Unified Taxonomy of CyberCrime

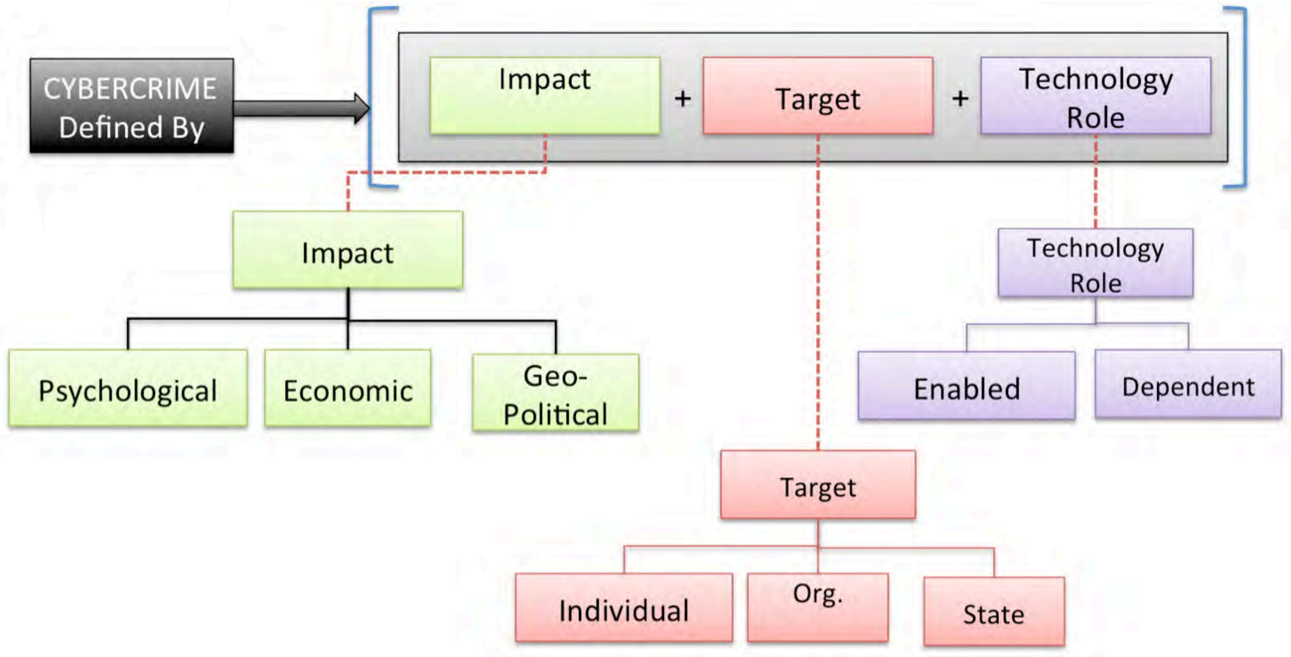


Table 1: Cybercrime category and associated typical examples of specific cybercrimes

	Impact			Target			Technology Role	
	Psychological	Economic	Geo-political	Individual	Organisation	State	Enabling	Dependent
Hackers and crackers (Newman and Clarke, 2013; Wall, 2013; Steinmetz, 2015)		x	x	x	x	x		x
Cyber fraud (Ebenezer and Elizabeth, 2014)		x	x	x	x	x	x	
Cyber embezzlement (Brinson et al., 2006)		x		x	x		x	
	Impact			Target			Technology Role	
	Psychological	Economic	Geo-political	Individual	Organisation	State	Enabling	Dependent
Cyber piracy (Wu et al., 2003)		x			x			x
Cyber blackmail (Hilley, 2006)	x	x		x	x		x	
Romance scam (Dorring, 2002; Couch, D., & Liamputtong, P. (2008)	x			x				x
Online drug trafficking (Castronova, 2006)		x		x	x		x	
Cyber prostitution (Ashford, 2008; Lee and Shin, 2004)	x	x		x			x	
Cyber extortion (Riem, 2001)	x	x		x	x		x	

Illegal online gambling (Chen et al., 2004)	x	x		x	x		x	
Cyber homicide (Gai & Shan, 2012)	x			x			x	
Hackers -‘Hacktivist’ (Hampson, 2012; Taylor, 2001; Steinmetz, 2015)		x		x	x			x
Cyber spies (Wall, 2013)		x	x	x	x	x	x	
Cyber espionage (Yar, 2006; Wall, 2013)		x	x		x	x	x	x
Cyber terrorism (Tripathi, 2015; Wall, 2013; Yar, 2006)		x	x		x	x	x	x
Cyber Vandalism (Brenner, 2001)		x	x	x	x	x		x
Cyber assault (Yar, 2006; Hinkle, 2011)	x			x			x	
Cyber hate speech (Weintraub-Reiter, 1998)	x		x	x	x	x	x	
Cyber riot (Axelrod, 2010)		x	x		x	x	x	
Cyber sabotage (Boni, 2001)		x	x		x	x	x	
Cyber-colonialism (Loo and Yeap, 1998)			x			x	x	
Cyber-nuisance (Kam, 2004)	x			x			x	
Cyber rebellion (Sangarasivam, 2013)			x	x	x	x	x	
Child pornography (Weaver et al., 2003; Wall, 2013)	x	x		x			x	

Cyber stalking (Brenner, 2001; Joseph, 2003; Yar, 2006)	**x**			**x**			**x**	
Cyber bullying (Bauman and Bellmore, 2015)	**x**			**x**			**x**	
Obscenity (Halder, 2013)	**x**			**x**	**x**	**x**	**x**	
Cyber rape (Brenner, 2001; Powers, 2003)	**x**			**x**			**x**	

In this categorisation we can see that cyberterrorism is part of this taxonomy and is a cybercrime that is intended to have economic and geopolitical impact, targets the state and organisation and is both technologically enabled and dependent. As von Behr et al. (2013) highlight the Internet provides a broader range of opportunities for individuals to be radicalised and to confirm existing beliefs. However, this report also highlights that the evidence that they have gathered and the analysis performed does not necessarily show that the Internet increases the likelihood of radicalisation.

3 SOCIO-ECONOMIC LENS OF CYBERCRIME

The socio-economic calculations of cybercrime are themselves situated in a political, social and historical context. This section presents a snapshot of the current thinking in the current work to calculate the cost of cybercrime.

There are a number of questions that we need to keep in mind when evaluating the cost of cybercrime. These questions include:

- How do we measure the 'extent' and 'cost' of cybercrime?
- What is the scale of the problem?
- How can such measurements help? What purpose do they serve?
- What do we mean by 'cost' in social, economic, moral and political terms?

The modern phenomenon of cybercrime raises questions on a scale which has few, if any, precedents. The global outreach and effect of criminal actions carried out via the internet tax the few international agreements that exist and, further, accentuate the absence of a truly global corresponding response. Concepts, such as values and norms, which help create national laws, can be difficult to reach agreement on at an international level. At the same time even palpable subjects, such as terminology, standards and practices are slow to evolve which can be an obstacle to early cross-border concord.

In the relatively short time in the evolution of cybercrime, immense progress has been made across a variety of domains. Cybercrime is now acknowledged as a global threat and a subject worthy of research in its own right. Nation states worldwide provide varying degrees of revenue towards their own protection and for further research into what has become an increasingly prominent topic. However, it remains the case that, despite large budgets spent on cyber defence and security, few straightforward numbers exist on the true extent of cybercrime and what is the cost politically, economically, socially and morally. Within the discipline of cybercrime research, costing remains an imprecise art. For example, in 2011, the information intelligence experts, Detica (Detica Ltd, 2011), reported that the cost of cybercrime to the UK economy was £27 billion per year (Detica, 2011). In this first joint Government and industry report into the extent and cost of cybercrime, Detica conceded that 'modeling cybercrime is a complex and difficult exercise' and that their assessments rest on 'assumptions and informed judgements rather than specific examples of cybercrime' (Detica 2011: 3). Not surprisingly, the £27 billion Detica figure has been questioned due its lack of rigour and transparency. Other studies that have attempted to examine the cost of cybercrime have used different methodologies. For example, Anderson et al (2012) produced a more nuanced picture detailing separate estimates for different cybercrimes. However, such work is also perceived to have limitations due to its reliability on scaled down global estimates and case studies (McGuire and Dowling 2013). The evidence-base about the true nature and extent of cybercrime presents an ongoing challenge and limits our understanding of the economic cost of this phenomenon to society at large. It is important to note that the problem of such cost estimates is not unique to cybercrime only, but exists in the realm of traditional crime too.

In thinking about the costs of traditional crime, the general focus has tended to be on crime reduction/prevention and criminal policy. Similarly, in the case of cybercrime we are beginning to think about not simply the outcome costs of the acts of cybercrime, but also the anticipated costs of preventive strategies as well as the costs of law enforcement.

To arrive at a valid methodology for costing is understandably complex. What currently exists is mainly the product of history and the result of an industry growing from infancy during a period of few accredited industry standards and practices. The rapid growth in the use of the internet since its inception leads to piecemeal advances in a security sector where data collection and analysis began on an ad-hoc basis by the community volunteers who were the first to observe the rise of the cybercriminal. The security sector evolved from the need to manage a new type of criminal with access to resources that challenged all but a small group of knowledgeable experts.

The perception that the security industry is in a constant state of 'catch-up' with the cybercriminal is still prevalent but laying aside the need for better technology is a crucial need to understand what is the problem being addressed. This entails the need for 'evidence-based' methods of measurement along with greater interaction with other disciplines and knowledge-based groups in order to arrive at a deeper understanding of cybercrime governance.

In order to evaluate the cost of cybercrime, we need to review a number of areas of research including cybercrime measurement research, general surveys of cyber threats and surveys of cybercrime threats.

In a response to the 2015 CyberROAD survey question to stakeholders (discussed in deliverable 5.1): *"Have you experienced a cybercriminal action in the last 5 years?"* **78%** of the respondents responded they had, either in a personal capacity (31%) or through work (47%). When asked *"To make the Internet a safer place and to fight cybercrime, what are the topics we should research into?"* most respondents rated "Better metrics and statistics on cybercrime" as their 2nd most importance choice (from a selection base of 6).

Cybercrime has climbed to the top tier in the National Security Strategy of many EU states e.g. France, the Netherlands and the UK, becoming the #1 threat above organised crime and fraud generally. However as indicated within a recent 2013 study for the European Parliament - Directorate General for Internal Policies "The Economic, Financial & Social Impacts of Organised Crime in the EU", *"estimates of cybercrime costs are highly contested"*. It concluded by saying *"So is cybercrime a threat, and to whom? It is a threat to all of us. The question is how much of a threat, and how can we better understand how much of a threat it is."* (Levi, 2013)

Using property crime, for example, as a comparison, in most countries the metrics are mostly readily available. For example in the US, the FBI's Uniform Crime Report will provide how many offenses were committed nationally in 2011 (9,063,173) and of what type (burglary 24%, larceny 68% and motor vehicle theft 7.9%). Overall property crime cost the US economy 2011 (€14bn) (FBI, 2011). *"However, when enquiring about the direct costs of cybercrime to any economy, individual industries, or companies and you get no straight answers."* (Roberts and Kielstra, The Economist 2013)

3.1 CURRENT OVERALL ESTIMATES

3.1.1 COSTS OF CYBERCRIME[1]

- The annual cost to the global economy from cybercrime is more than **€300 billion Euros** (McAfee, 2014)
- Cost of cybercrime for the **EU 0.4% of its GDP**[2] = **€13 billion / annum** (McAfee, 2014)
- Sample EU countries estimates for the cost of cybercrime[3]:
    - Poland = **€ 377 million /annum**
- Germany = **€ 2.6 billion /annum**
- UK = **€ 2 billion /annum**
- Cybercriminal revenues (estimate of the cybercrime market itself) **€15 billion / annum** (Group-IB (RU))
- Market for security products and services **€50 billion / annum** (IDC, 2014)

3.1.2 EXAMPLES OF OVERALL CYBER METRICS

- Billion users of the Internet (Mar 2015)(~39% world population) (World Wide Web Consortium, 2015)
- Over 200 billion emails processed / day (The Radcati Group, Inc, 2015)
- 917.9 million websites (variable) — 39 million / month added (4%) (World Wide Wed Consortium, 2015)(Accessed May 2015).
- IP addresses - IPv4 = 4,294,967,296 (232) - IPv6 = of (2128) (RIPE Network Co-ordination Centre, 2015)
- 2.3 billion mobile-cellular subscriptions worldwide (International Telecommunications Union, 2015)
- 1.4 million browser user agents - bots (Bots vs Browsers, 2015)

3.1.3 QUANTITATIVE METRICS OF CYBERCRIME ACTIVITY INDICATORS

- 85% of processed emails are spam (Barracuda, 2015)
- 7% of all urls malicious (Barracuda, 2015)
- Public Block List count: 1,018,203,532 IP addresses (Spamhaus, 2014)
- 350 million in total identifiable malware (AV-TEST, 2015)
- 1 million+ measurable cyber-attacks every day (Akaimai, 2014)

[1] The sources for these figures are listed in website format at the end of the references section.

[2] Estimate of average - range is up to 0.9% of GDP - high-income countries incur higher losses.

[3] Based on share to EU GDP. Figures on GDP are available on the IMF website https://www.imf.org/external/data.htm

- 330 active Real-time Blackhole Lists (RBL & DNSBL) (Squid Blacklist, 2014)
- € 7.9 million is the average annualized cost of data breaches (Ponemon Institute, 2014)
- 10.4% net increase cost of data breaches over the past year (Ponemon Institute, 2014)
- 250,000 – 500,000 malicious binaries / day (Shadowserver, 2014)
- ~280 million malicious binaries collected (Shadowserver, 2014)
- 6 / 10 million unique IP's sinkholed / day (Shadowserver, 2014)
- 900,000 malicious domains / day (Shadowserver, 2014)
- 500 of 52,000 ASNs worldwide (4%) account for hosting 85% of malicious activity (HostExploit, 2014)

3.1.4 OVERVIEW OF CURRENT ESTIMATES

In conclusion, the above examples demonstrate that a variety of data types on cybercrime metrics are available. This is a good starting point. The next step is to evaluate which statistics have value and how they can be used. More research is needed in the area.

A significant amount of groundwork is needed before a functional framework is achieved but will effect greater value in trust alone. For example, it may be simpler to compute a single "cost" figure for a whole sector at any one time, which is how cybercrime figures are often portrayed, but unless this stands up to scrutiny the result is a waste of good resources. An effective way of working out how, for example, loss of reputation is "costed" is important as these sums may vary enormously. A blanket approach may not be accurate enough, for instance, for budgetary and insurance purposes. The development of a working model is an essential research area if the impact of cybercrime is to be fully understood and appreciated.

3.2 REVIEW OF THE STATE OF THE ART OF METRICS

A review of the state-of-the-art of the metrics and economics of cybercrime requires an evaluation of current studies and reports. Within the last 5 years (2011 to Jan 2015) there are 3,920 web searchable scholarly articles, papers and books relating to the 'economics or costs of cybercrime'[4]. Added to this is the wide spectrum of commercial sources collecting, collating and disseminating related information and data, some of which is not publically accessible.

An in-depth comparative study of all relevant reports is outside the remit of the CyberROAD project and instead a sample of typical studies and reports were reviewed. Four major studies on the theme of the "cost of cybercrime" were selected as representative of their genre, together with one quantitative study with a focus on a specific attack type, and one study that specifically tackles the issue of the cost of privacy, the related cost of identity theft and data breaches relating to personal data. The studies either present a breakdown on the "cost of cybercrime", offer recommendations and advice on how costing and metrics can be improved or convey specific quantitative data. The

[4] Result from Google browser search (13 Feb 2015)

studies selected come from academia, consumer groups, technology providers and policy advisors and align to the criteria of the CyberROAD Triad approach.

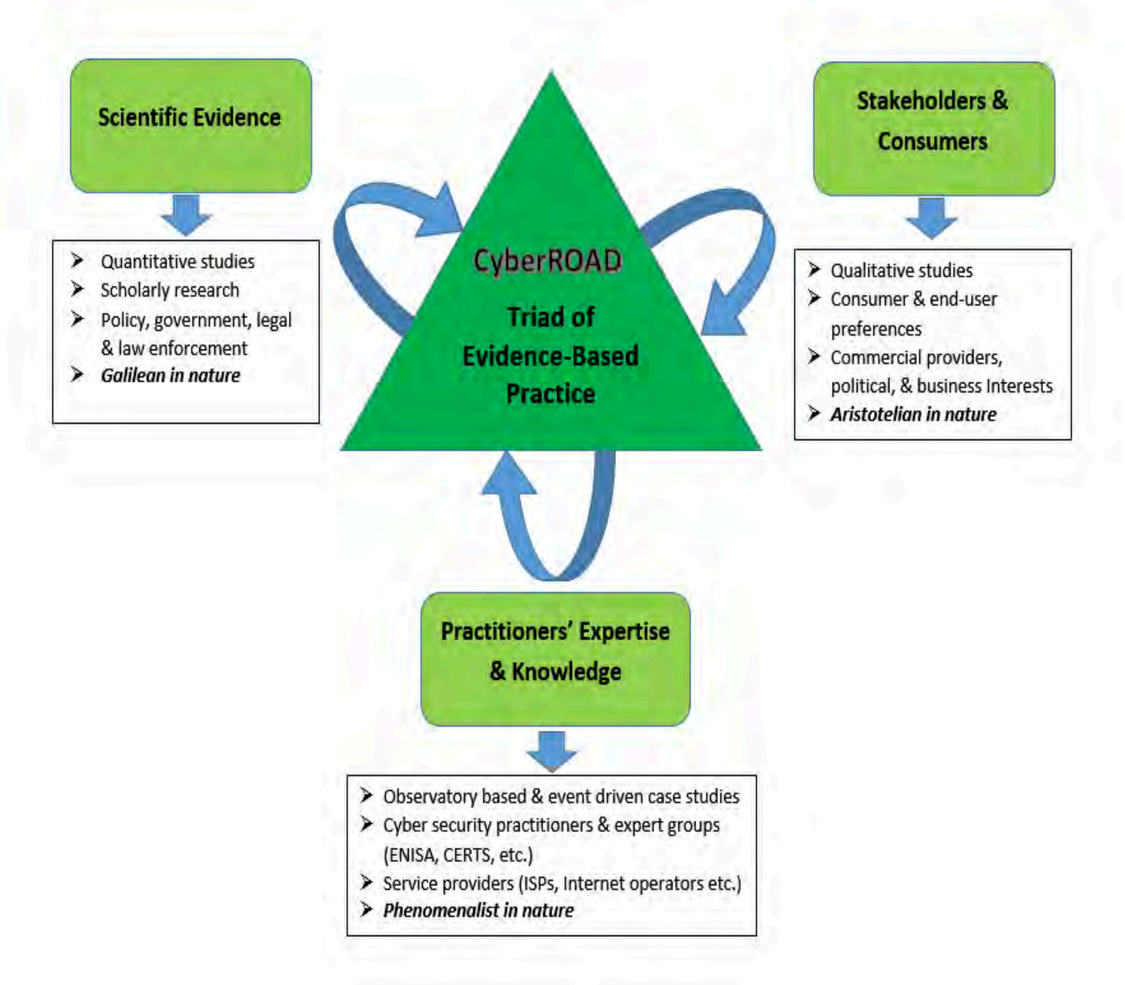

Scientific Evidence
Quantitative studies
Scholarly research
Policy, government, legal & law enforcement
Galilean in nature
CyberROAD
Triad of Evidence-Based Practice
Stakeholders & Consumers
Qualitative studies
Consumer & end-user preferences
Commercial providers, political, & business Interests
Aristotelian in nature
Practitioners' Expertise & Knowledge
Observatory based & event driven case studies
Cyber security practitioners & expert groups (ENISA, CERTS, etc.)
Service providers (ISPs, Internet operators etc.)
Phenomenalist in nature

Figure 3 CyberROAD Triad of evidence-based practice - to validate all the choices made in cybercrime metrics and threat data.

This short overview revealed commonalities among the studies, if not their methodologies, which point the way to a number of identifiable research gaps. Firstly, the degree to which data is considered as open and publically accessible depends on the viewpoint. The intended motive and aims of the data provider, which may altruistic in nature or commercially interested, is difficult to quantify. It follows that any related data is regarded with suspicion and its validity questioned; whose data can be trusted, how can a "trusted" environment be measured? Methodologies used to collect and collate information can be unique to the entity, unclear or not fully disclosed. Data may be incomplete in the wake of a lack of standard modus operandi, guidelines on best practices or benchmarks for the measurement of data.

3.2.1 (A) Anderson et al study

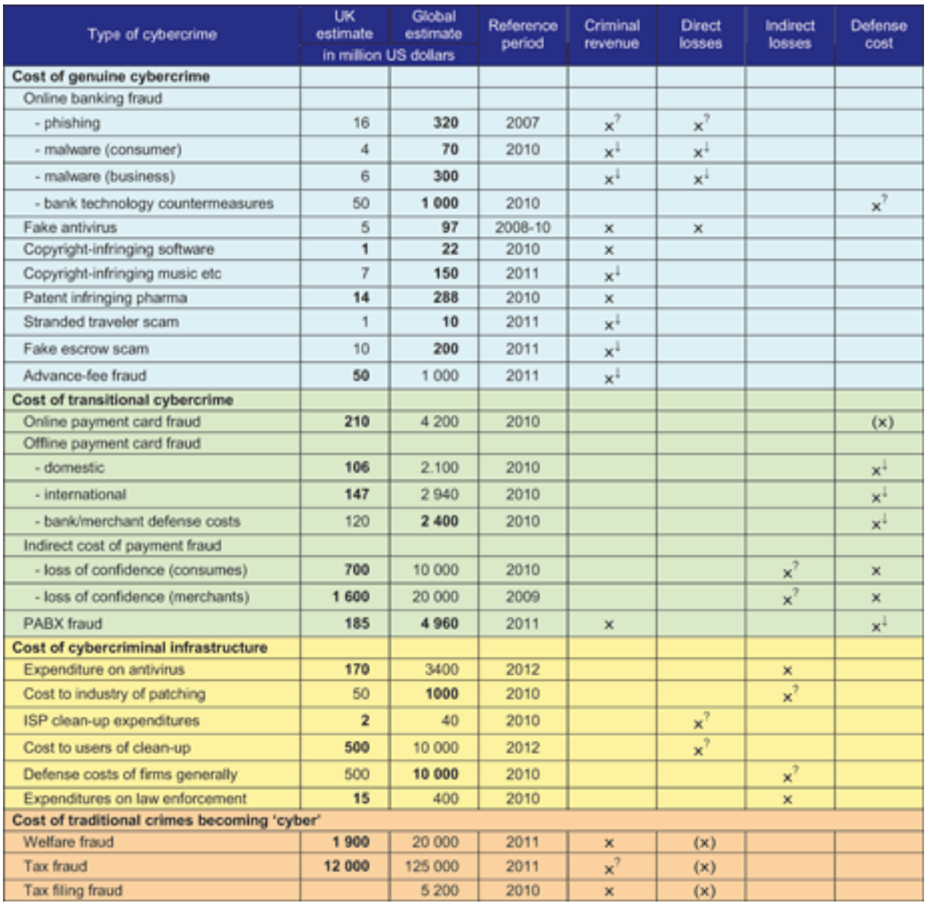
Although more than 100 different sources of data on cybercrime were counted in early 2012, the 'first systematic study of the costs of cybercrime' (Anderson, et al., 2012) concludes that available statistics are 'insufficient and fragmented'. The unequivocal message is that a lack of cohesion between different sources clouds the issue, leads to inconsistency of data and engenders mistrust of the numbers. As a consequence policy makers, who depend upon reliable figures, are left with little to go on, while the problem's true extent is obscured by the absence of easy-to-understand metrics. This report supports the widely held opinion that despite eye-catching headlines suggesting otherwise, it remains the case that few straightforward numbers exist on cybercrime and its true cost politically, economically, socially and morally.

This 'Cost of Cybercrime' study details a simplified framework for standardising measurements, arrived at by decomposing an earlier, and much criticised (Anderson, 2012), report from Detica (Detica Ltd, 2011), where 'difficult to assess' categories were used. Anderson et al suggest that 'cost to society' can be calculated through the application of 'sum of direct losses, indirect losses, and defence costs', to 'known data' on cybercrime and supporting infrastructures. The definition of cybercrime is an integral baseline, from which the criteria for measurement is determined, and it is necessary for boundaries between traditional, transitional and modern crimes to remain flexible as society's dependence on cyberspace continues to increase. Using this method, the report claims that 'new computer crimes' actually cost only 'tens of pence/cents' per person and not the vast sums as reported elsewhere.

Within this study 'known data' consists of main types of cybercrime; online payment card fraud, online banking fraud, industrial cyber-espionage and extortion, fake antivirus, etc. Within the 'Infrastructure Supporting Cybercrime' grouping 'known data' is used on Botnets, Botnet mitigation by consumers, Botnet mitigation by industry, other botnet mitigation costs, and Pay-per-install. These are applied to one of four sections: Cost of genuine cybercrime, Cost of transitional cybercrime, Cost of cybercriminal infrastructure and Cost of traditional crimes becoming `cyber', and the category 'Criminal revenue' to direct/indirect/defence costs, is added to complete the framework. (See Fig 3)

Anderson et al conclude 'Previous studies of cybercrime have tended to study quite different things and were often written by organisations (such as vendors, police agencies or music industry lawyers) with an obvious `agenda'.

Questions raised within this report provide several areas for further research, for example, what data can be trusted and from where should it be sourced, what are the determining metrics to be used, the need for benchmarks, why does cybercrime have high indirect costs and low indirect costs, (Anderson et al, p26). Additionally, Anderson et al conclude that less should be spent on '…anticipation of computer crime (on antivirus, firewalls etc.)', and more on '… catching and punishing the perpetrators.'



Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defense cost
	in million US dollars						
Cost of genuine cybercrime							
Online banking fraud							
- phishing	16	**320**	2007	$x^?$	$x^?$		
- malware (consumer)	4	**70**	2010	$x^{\downarrow}$	$x^{\downarrow}$		
- malware (business)	6	**300**		$x^{\downarrow}$	$x^{\downarrow}$		
- bank technology countermeasures	50	**1 000**	2010				$x^?$
Fake antivirus	5	**97**	2008-10	x	x		
Copyright-infringing software	**1**	**22**	2010	x			
Copyright-infringing music etc	7	**150**	2011	$x^{\downarrow}$			
Patent infringing pharma	**14**	**288**	2010	x			
Stranded traveler scam	1	**10**	2011	$x^{\downarrow}$			
Fake escrow scam	10	**200**	2011	$x^{\downarrow}$			
Advance-fee fraud	**50**	1 000	2011	$x^{\downarrow}$			
Cost of transitional cybercrime							
Online payment card fraud	**210**	4 200	2010				(x)
Offline payment card fraud							
- domestic	**106**	2.100	2010				$x^{\downarrow}$
- international	**147**	2 940	2010				$x^{\downarrow}$
- bank/merchant defense costs	120	**2 400**	2010				$x^{\downarrow}$
Indirect cost of payment fraud							
- loss of confidence (consumes)	**700**	10 000	2010			$x^?$	x
- loss of confidence (merchants)	**1 600**	20 000	2009			$x^?$	x
PABX fraud	**185**	**4 960**	2011	x			$x^{\downarrow}$
Cost of cybercriminal infrastructure							
Expenditure on antivirus	**170**	3400	2012			x	
Cost to industry of patching	50	**1000**	2010			$x^?$	
ISP clean-up expenditures	**2**	40	2010		$x^?$		
Cost to users of clean-up	**500**	10 000	2012		$x^?$		
Defense costs of firms generally	500	**10 000**	2010			$x^?$	
Expenditures on law enforcement	**15**	400	2010			x	
Cost of traditional crimes becoming 'cyber'							
Welfare fraud	**1 900**	20 000	2011	x	(x)		
Tax fraud	**12 000**	125 000	2011	$x^?$	(x)		
Tax filing fraud		5 200	2010	x	(x)		

Figure 4: Judgement on coverage of cost categories by known estimates (Anderson et al, 2012)

3.2.2 (B) Ponemon Institute Study

Since 2009, The Ponemon Institute has been conducting 'The Cost of CyberCrime Study' (Ponemon Institute, 2014). The Ponemon Institute is an independent U.S.-based research group with the aim of informing the private and public sector on how to '…improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise…' Ponemon Institute research is used by major corporations, U.S. federal and state departments, consumer groups and is widely publicised by a variety of media outlets. This report was sponsored by HP Enterprise Security.

The 2014 Ponemon Institute report is based on the findings from surveys conducted with 257 organisations using a cross-section of industry sectors in 7 countries – U.S.A, U.K., Germany, Australia, Japan, France and the Russian Federation. The research is field-based via interviews with senior-level personnel '…about their organizations' actual cybercrime incidents…' from large sized entities with more than 1,000 direct connections to the network or its systems (enterprise seats).

The total cost incurred by an organisation is analysed using criteria such as the 'costs to detect, recover, investigate and manage the incident response' along with costs that 'result in after-the-fact activities and efforts to contain additional costs from business disruption and the loss of customers' but excluding the cost of 'expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations'. The research gap here points to the use of 'difficult to assess' categories, a criticism Anderson et al's report levelled against the Detica study. Is it reasonable to publish figures that are hard to substantiate?

An initial comparison of the Anderson et al study to the Ponemon Institute report (2014) reveals an immediate and common problem within this field of inquiry. For example, both reports use valid research techniques but comparison is untenable as different criteria and methodologies are employed in gathering and collating the material. Here are two studies with the same title but with a diverse approach to the research matter. It is, therefore, unsurprising that the results are disparate.

The research gap uncovered here points to the use of 'difficult to assess' categories, a criticism levelled against the Detica study in Anderson et al's report (2012), but could equally apply to a number of recent studies. Further research is needed to ascertain how much trust can be placed in figures that are hard to substantiate.

3.2.3 (C) MCAFEE ANNUAL CYBERCRIME REPORTS

The McAfee report of June 2014 'Net Losses: Estimating the Global Cost of Cybercrime' (McAfee 2014) reviews the accuracy of its own evaluation early on under the section header 'Estimating global loss from incomplete data' (McAfee 2014: 4), 'International agreement on a standard definition of cybercrime would improve the ability to collect consistent data.' Despite this data accuracy warning, McAfee appraises that the inclusion of certain additional indirect costs, such as reputational damage, show the '…full effect of cybercrime on the global economy.'

Sources for this report range from the German Office for the Protection of the Constitution, the Netherlands Organisation for Applied Scientific Research (TNO), China's Peoples Public Security University, the European Commission, the Australian Institute of Criminology Research, Malaysia's Chief Technical Officer, and estimates by government agencies in other countries and consulting and cybersecurity companies around the world.

McAfee aggregates data from sources within 51 countries '…who account for 80% of global income,' and uses what is 'publically available' from resources on IP theft, fraud, or recovery costs with additional field-based data from public servants and subject specialists. Adjustments are applied to account for regional differences and to arrive at an estimated global cost. The results for individual countries are available as separate reports.

The lack of effort made by most countries in collecting data on cybercrime losses, as along with widespread inconsistencies and poor quality of the data that is gathered, is a re-occurring theme in this report. The three examples methods used to 'extrapolate a global loss figure' highlight this very problem. Method 1 uses the loss by high-income countries to deduce a global total, method 2 totals the amount for all countries where open source data is available, and method 3 'aggregate costs as a share of regional incomes.' The report goes on to acknowledge the inadequacies of these methods which, due to the lack of reliable data, could either be an 'overestimate' or 'underestimate' of the true cost of cybercrime worldwide.

The research gaps presented by the McAfee report point directly to the lack of reliable data. Despite being a multi-national company with a global outreach, McAfee is unsure of its own results and deemed it necessary to express its doubts about the ability to collect and collate accurate and reliable data.

A further research gap relates to the role of the corporate entity in this field. Is it possible to assess whether information delivered from the private sector is always biased towards its own agenda? Many different types of organisations currently provide critical services and share data to help protect against cyber-attacks. How can these be more effectively used, and trusted, to provide the types of figures that are missing. What can be done to improve the availability of data in countries around the world? Who can be trusted to provide this service in other countries? Should this be a role for a new, independent entity?

3.2.4 (D) East West Institute study

One of the few global studies into the need for improved methods of measurement was undertaken in 2013 by the East West Institute (EWI) (East West Institute, 2015[5]), an international, non-partisan, not-for-profit policy organisation that focusses on confronting critical challenges. 'Measuring the Cybercrime Problem' (Rauscher & Cox, 2013) examines how trusted metrics and performance benchmarks can be established, and a trusted centralised data collection entity created, research gaps previously identified in this review. The EWI study 'presents a bold solution to this problem that involves private sector leadership aimed at promoting trust and cooperation'. The report concludes with three recommendations and calls for '…volunteers from all sectors—ICT, energy, financial services, transportation, retail, medical and others…' to carry these out.

Existing information sharing entities are benchmarked against 'Target Criteria' (Figure 5) based on three key areas: Governance-Related, Breadth-Related and Information-Related. Results of the 'Gap Analysis' are reported in table format (Figure 6).

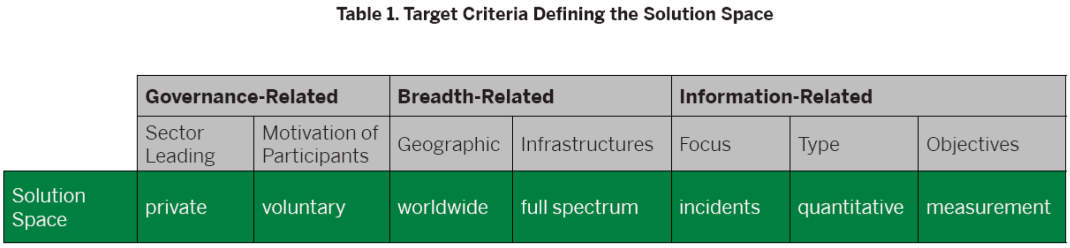


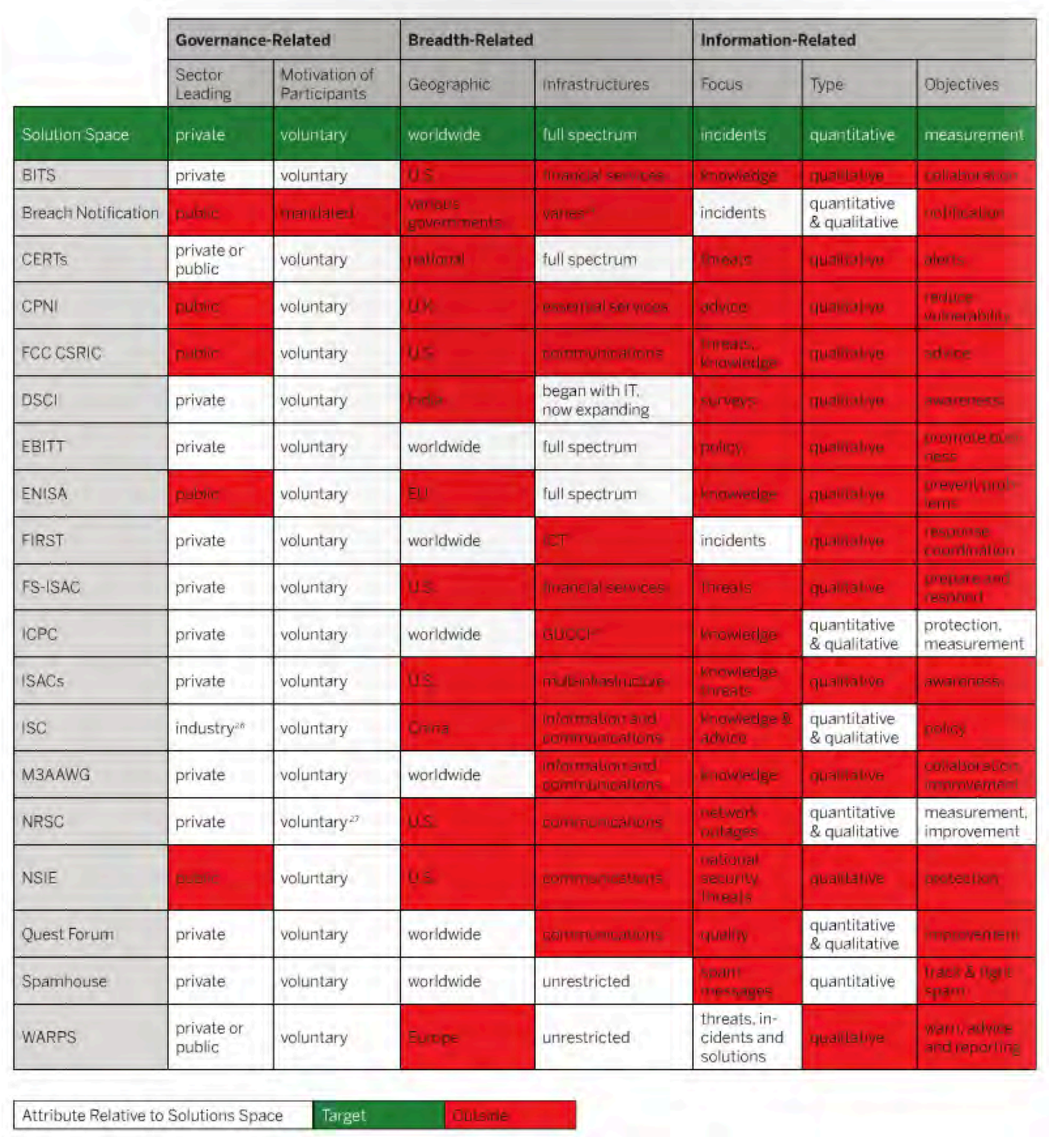
Table 1. Target Criteria Defining the Solution Space

	Governance-Related		Breadth-Related		Information-Related		
	Sector Leading	Motivation of Participants	Geographic	Infrastructures	Focus	Type	Objectives
Solution Space	private	voluntary	worldwide	full spectrum	incidents	quantitative	measurement

Figure 5: ***EWI Scope of Target Criteria*** **(Rauscher & Cox 2013)**

Commercial entities are excluded on the grounds that, '… they are seen as likely to try to influence market conditions, whether or not this perception is justified.' The resulting 'Gap Analysis' reveals that not a single entity reached all the Target Criteria, one achieved 5 out of 7, and 5 scored 4 out of 7, giving justification to EWI's call for the creation of a trusted entity for data measurement, as one could not 'be found'.

[5] http://www.ewi.info/



	Governance-Related		Breadth-Related		Information-Related		
	Sector Leading	Motivation of Participants	Geographic	Infrastructures	Focus	Type	Objectives
Solution Space	private	voluntary	worldwide	full spectrum	incidents	quantitative	measurement
BITS	private	voluntary	U.S.	financial services	knowledge	qualitative	collaboration
Breach Notification	public	mandated	various governments	varies	incidents	quantitative & qualitative	notification
CERTs	private or public	voluntary	national	full spectrum	threats	qualitative	alerts
CPNI	public	voluntary	U.K.	essential services	advice	qualitative	reduce vulnerability
FCC CSRIC	public	voluntary	U.S.	communications	threats, knowledge	qualitative	advice
DSCI	private	voluntary	India	began with IT, now expanding	surveys	qualitative	awareness
EBITT	private	voluntary	worldwide	full spectrum	policy	qualitative	promote business
ENISA	public	voluntary	EU	full spectrum	knowledge	qualitative	prevent problems
FIRST	private	voluntary	worldwide	ICT	incidents	qualitative	response coordination
FS-ISAC	private	voluntary	U.S.	financial services	threats	qualitative	prepare and respond
ICPC	private	voluntary	worldwide	GUCCI	knowledge	quantitative & qualitative	protection, measurement
ISACs	private	voluntary	U.S.	multi-infrastructure	knowledge threats	qualitative	awareness
ISC	industry[26]	voluntary	China	information and communications	knowledge & advice	quantitative & qualitative	policy
M3AAWG	private	voluntary	worldwide	information and communications	knowledge	qualitative	collaboration, improvement
NRSC	private	voluntary[27]	U.S.	communications	network outages	quantitative & qualitative	measurement, improvement
NSIE	public	voluntary	U.S.	communications	national security threats	qualitative	protection
Quest Forum	private	voluntary	worldwide	communications	quality	quantitative & qualitative	improvement
Spamhouse	private	voluntary	worldwide	unrestricted	spam messages	quantitative	track & fight spam
WARPS	private or public	voluntary	Europe	unrestricted	threats, incidents and solutions	qualitative	warn, advice and reporting

Attribute Relative to Solutions Space	Target	Outside

Figure 6: *EWI Gap Analysis* (Rauscher & Cox 2013)

Applying the EWI Gap Analysis in CyberROAD

In Deliverable 2.1 Section 4.4.2 we outlined how CyberROAD would define its roadmap goals, using normative and explorative means, supported by available data such as partner CyberDefcon's observatory *http://globalsecuritymap.com*.The EastWest Institute study shows the critical nature of quantitative data in the measurement of cybercrime costing. To test out the suitability of the observatory tool it was measured against the 'EWI Scope of Target Criteria'.

The 'Global Security Map' surpasses the scores of every other entity used in the EWI sample but misses the target on 'Focus' when matched to the criteria determined by the Institute. In the context of CyberROAD the target criteria for 'Focus' would more appropriately be 'knowledge', as opposed to 'incidents', which returns a good match according to the needs of the project.. So according to the criteria required in the CyberROAD project, applied to the EWI methodology in assessing the suitability of selected candidates, the 'Global Security Map' passes the 'trust' test. This exercise demonstrates two points: 1) The value of this type of methodology in matching a sample set against specific criteria, 2) Modifying the criteria in 'Focus' enables the EWI assessment tool to be applied according to individual requirements.

Further research is needed into how similar tools can be used to assess the suitability of data providers according to need. There may be value in widening the sample set to include corporate entities who are willing to provide verifiable and quantitative data that passes set standards and benchmarked criteria.

3.2.5 (E) Neustar UK annual DDoS report

In May 2014 Neustar published its second annual 'UK DDoS Attacks and Impact Report' (Neustar, 2014[6]). Neustar began as an operating unit managing large datasets under Lockheed Martin, a global aerospace, defence, security and advanced technology company. Today Neustar handles billions of DNS queries and millions of text messages and phone calls. The findings for the report are based on Neustar's survey of 331 UK companies across a variety of industries including financial services, technology, retail, government/public sector, health care, energy/utility, telecommunications, e-commerce, Internet services and media.

The scope of the inaugural 2012 survey was further developed with additional questions for 2013. Each is a targeted question to find out very specific information and to gather data that builds into a year-on-year profile of DDoS patterns and related changes. Example questions include: What are the sizes and velocities of DDoS attacks?, How long are DDoS attacks lasting?, Are DDoS attacks a bigger or smaller threat to your business versus a year ago?, and How often were you attacked?

This seems a simple yet effective way of gathering quantifiable information and a good example of how the data can be displayed in an easy-to-understand format.

Even though this report appears to provide a model template for measurement and metrics there are still a number of issues related to the findings from our earlier gap analysis. Under the EWI method of analysis, Neustar would not qualify as a 'trusted' data provider as it is not a non-profit organisation. So, to what extent can this data be trusted? In the absence of benchmarks or standards, this is an unknown entity. Further research is required in this area to establish the criteria for cross-industry best practices and benchmarks. Private, public and non-profits may each have a role to play that can contribute to measurement and metrics improvements. Metrics used in this way can point to security vulnerabilities and provide a valuable source for gap analysis research. The results of the Neustar report specifically highlight the vulnerability of the DNS/NTP servers to amplification attacks, when there are server misconfigurations. Such reports are, therefore, a valuable additional source in the identification of problem areas. This is not the case when data is not quantifiable.

3.3 Conclusions From the socio-economic snapshot

This introduction and overview of the metrics and economics of cybercrime with analysis of the four example studies on how to cost cybercrime reveals the difficulties of comparative research on this

[6] Available from https://www.neustar.biz/ddos-attacks-report.

subject. For those producing a ‘cost of cybercrime’ the lack of quantifiable data leaves the final sum questionable. Without standardisation and benchmarking, there is little that is comparable between one study and another especially when the definition of cybercrime is still open to debate.

This does, however, expose several research gaps which can be summarised as follows:

1) A comparison of all available data sources is a worthy research topic in its own right. This area has been partly covered in both the Anderson study and the EastWest Institute Study but requires further in-depth analysis.
2) How can cybercrime be defined and agreed upon on an international level?
3) How can the measurement of cybercrime be quantified?
4) International standards and benchmarks in cybercrime metrics
5) i) What is ‘trusted’ data?
   ii) Who can be ‘trusted’ with data?
   iii) The role of public sector/private sector/government/governance, in information sharing
6) Can anti-cybercrime budgets be better spent?

4 PEOPLE-CENTERED LEVEL OF CYBERCRIME

4.1 INTRODUCTION

In this section we present the key research themes relevant to the study of the main actors in cybercrime. We look at three broad areas of literature: technology practices of end-users, technology practices of hackers/attackers and technology practices of cyber criminals. In this section we identify the current state of the art in terms of research understanding of the connection between the social habits of end-users, the social habits of attackers and the social habits of cyber criminals.

4.2 SOCIAL HABITS OF END-USERS

The technology practices of people have been the focus of human-computer interaction and of user experience research. Of particular relevance to CyberROAD is the study of information sharing practices and the study of practices related to the use of security technologies. Information sharing practices are key because of the potential of information to be used in so-called social engineering attacks that combine an understanding of the social practices of an individual with technology vulnerabilities in order to complete an attack. Practices related to security technologies such as access control mechanisms (passwords, file persmissions), data protection (cryptographic tools) and data provenance (digital signatures and validation techniques) have the potential to impact an attacker's ability to conduct a criminal activity.

4.2.1 INFORMATION CONTROL PRACTICES

Perhaps the richest area of research into general information sharing and protection practices stem from informational privacy studies. Studies show that the information sharing and protection practices people use are influenced by social factors (Barnard-Wills and Ashenden 2010, Dowd 2011, Dourish et al 2004, Livingstone and Helsper 2007]. A number of quantitative measurement scales have been developed to measure the use and perceptions of such practices. For example, Buchanan et. al. in 2007 developed and validated Internet-administered scales measuring privacy-related attitudes and behaviours. Buchanan et al identified two broad groups of practices that people may carry out to protect the flow of their personal information. The first group is termed "General Caution" practices and contains social practices that users may deploy to protect their personal information such as anonymising their disclosures, fabricating part of the disclosure, taking social measures to limit the extent of the dissemination of their personal information, etc. The second group, known as 'Technical Protection' practices, is a set of practices that use hardware and software as tools for protecting their personal information. This may include the use of cryptographic techniques and access control technologies. These two categories can be applied to other areas of information control, for example the protection of organisational data.

The majority of the research in general caution practices is related to the use of privacy policies (e.g. McDonald and Cranor 2009, Bonneau and Preibusch 2010). In a broader sense, the general consensus of usability and security research is that a) security technology is too onerous (Adams and Sasse 1999, Inglessant and Sasse 2010, Crawford and Renaud 2014) and b) increased security does not always give more protection (e.g. Florencio et al. 2007 Herley 2014, Schechter et al, 2008). As a result, it is perhaps unsurprising that people develop general caution practices.

However, it is often difficult to generalise the findings of such studies because at times they suffer from a lack of clear definition as to what information security actually is. Is it the protection of data or the protection of individuals through the protection of data? This lack of clear referent object results in a lack of clear measurement of security in particular scenarios and lack of clear understanding as to what it is in a particular scenario that protects the individual. Research into these areas is vital if our understanding of protection against person-centered cybercrime is to increase.

4.2.2 YOUNG ADULTS, CYBER PRIVACY, CYBER THREATS, AND CYBERCRIME

The terms youth, young people and young adults remain ambiguous and are invariably used in a range of ways in theoretical and empirical writings. The chronological age ascribed to these states can vary from 16-35. The dynamic nature of society, social relationships and social identities leads to such fluidity in meaning. In the digital age of technology, there is much concern about how children and young adults may be pre-disposed to online risky behaviours and practices. Whilst there is a growing research base on the vulnerability of children in cyber space, we lack a clear understanding of how young adults may also be at risk (Benson et al 2014).

The notion of privacy is considered to be socially constructed. It is temporal and contextual. Societal social norms govern the value and meaning of privacy to the individual, group, and society as a whole. And social norms are subject to change over time and space. In our contemporary modern 21st century world, where technology has become pervasive, there is a real and perceived threat to individual privacy. Yet, the ways in which users, perhaps freely, share information on the internet is also unprecedented (Kornblum 2007, Bennett 2013). Sociologists have theorised such information sharing in a myriad of ways from Goffmanian perspectives about presentation of self, to Butlerian views about identity performance (Zhao et al 2008, Pearson 2009).

In this modern age of the internet, personal information is an invaluable commodity. This is witnessed in a number of fora including the ways in which social networking sites, and other websites seek, accumulate and monetise information through a process of monitoring individual online behaviour and practices. Moreover, the ubiquity of technology via the internet of things is leading to a situation where any notion of privacy is said to become obsolete (Cas 2005).

Research on cybercrime reveals that the younger demographic (16-24) are prone to cybercrime (Tynes 2007, Oksanen & Keipi 2013, Benson et al 2014). Greater online participation where, technology-mediated information sharing takes place, is considered to be a key risk factor. It would seem that young people's offline relationships and networks are also deemed to be crucial psychosocial risk factors. For example, it is argued that problematic offline relationships predispose young people to share greater amounts of personal information online that consequently result in them sharing personal information online, and risk their privacy and security and safety leading to adverse situations such as cybercrime victimisation (Oksanen & Keipi 2013).

A popular view is that young people have become an 'online open-book', and their perception of privacy is radically different from that of the older generation. Other scholars have argued that young people value their privacy, however they may be faced with 'limited choices and limited information about how to participate in the processing of their data' (Richard 2014:1).

To advance understanding about young people's habits as end users, and thereby their perceptions of cyber privacy, cyber threats, and cybercrime, we carried out an empirical study involving young adult participants. Through a quantitative survey and qualitative data collection in focus group discussions and interviews, we explored young people's conceptions and practices of the value and meaning of privacy, and fears and apprehensions of cyber threats that can lead to cybercrime.

The survey comprised a mixed sample of 132 participants. Male and female respondents were represented in equal number (66 male, 66 female). The sample included a racially/culturally diverse population with 46% of the sample describing their ethnic background as White British/White European/White Other; and 25% recorded their ethnicity as Asian/Asian British. There were lower numbers of other ethnic groups, for example, 10% of the sample described their ethnicity as Black/Black British, and 8% reported a mixed-heritage background. A total of 10% of the sample were described as belonging to "other" ethnic backgrounds.

Almost two-thirds of the respondents were Home/EU students. About half of the sample were postgraduate Masters students (51%). Undergraduate students comprised just over two-fifths of the sample (44%).

Characteristic	n	% (1dp)
Gender		
Male	66	50.0
Female	66	50.0
Age		
18-20	46	34.8
21-24	40	30.3
25-29	21	15.9
30-34	8	6.1
25-39	8	6.1
>40	9	6.8
Ethnicity		

White British	38	28.8
White European	15	11.4
White Other	8	6.1
Asian/ Asian British	33	25.0
Black/ Black British	14	10.6
Mixed Ethnicity	11	8.3
Other Ethnicity	13	9.8
Citizenship Status		
Home/ European Union	81	61.4
Overseas	51	38.6
Current Degree		
Bachelors	59	44.8
Masters	67	50.8
PhD	3	2.3
Other	3	2.3

Table 2: Breakdown of results

Note

Before collapsing age into categories the mean age of the sample was 25.02. The age of the oldest respondent was 54 and the youngest respondent was 18.

Key findings

(a) Victimology

In a direct question about having falling prey to cybercrime, slightly over a tenth (14%) of the sample reported that they had been a victim of cybercrime in the last 12 months. However, other questions which asked specfically about the general frequency of cybercrime experiences, higher numbers of respondents reported victimisation experiences involving malware (30%), cyberbullying (22%), online scam (20%), and IPR theft (14%).

(b) Perceptions about the seriousness of cybercrime

Our findings reveal that with the exception of 'sexting' between consenting adults, our respondents were generally equally concerned about other types of cybercrimes. Thus, a third of our sample did not perceive sexting to be a serious crime, but were agreed on other forms of cybercrime to be of a worrisome activity. From the list of cybercrimes listed in our survey (see Appendix A for the full survey), pornography was reported to be of most concern (68%). Interestingly, whilst there has been a spate of recent cases in the news where young people between the ages of 16-18 have been prosecuted for online-sharing of nude photographs of themselves on ground of obscenity/pornography, our respondents express less concern about this. There appears to be a marked difference between the views of our respondents on the issues of sexting and pornography, and those of the Criminal Justice System in society which conflates sexting with pornography.

When looking at the demographic characteristic of those who perceived that engaging in posting or viewing offensive content online warranted extremely serious action which would involve prison the most likely group that would favour this were respondents age 35-39 (87.5%), closely followed by respondents aged over 40 (87.5%). Respondents who were under the age of 24 perceived more liberal views of this offence, as some respondents reported this to be not serious at all, or somewhat serious. This finding was not emulated in any other age categories.

Women (71.2%) were more in favour of this act resulting in prison than males (63.6%). Students engaged in a Bachelors degree (72.9%) favoured prison for engaging in posting or viewing offensive content online more often than Masters (62.7%) or PhD (33.3%) students. Students who were of mixed ethnic origin (90.9%) were most in favour of prison for this offense than compared with students from the other ethnic origins. Additionally, when comparing the seriousness of engaging in posting or viewing offensive content online perceived by Home/EU students and Overseas Students, it was found that Home/EU students saw this as far more serious than Overseas students. Specifically 75.3% students from Home/EU deemed this as extremely serious, whereas only 54.9% of Overseas students identified the offence to be extremely serious.

(c) Reporting of Cybercrime

Our study confirms the broader picture about the under-reporting of cybercrime to the criminal justice authorities. Only a fifth of our sample reported that they would refer an online scam experience to the police. The vast majority expressed a preference for reporting such an experience to their bank (75%). Arguably, it could be argued that reporting such an incident to one's bank would be the first concern of the majority of people, particularly in the context of preventing further financial loss. A study of actual reporting experiences would help shed further light on this situation. Indeed, there are important implications for policing practices of recording and investigating cybercrime here.

(d) Fear of Cybercrime

Interestingly, over half of our sample (53%) reported that they were not afraid of cyberbullying or cyberstalking. A quarter expressed no fear about online scams (26%). However, 9 out of 10 respondents were fearful about malware (computer virus, Trojan horse, spyware).

Our survey reveals some gender and ethnic differences. For example, women expressed more fear of all types of cybercrime - online scam, malware, use of intellectual property without giving permission, cyber bullying and cyber stalking. In particular, 27.3% reported being quite or extremely afraid of cyber bullying compared with 22.8% of males. However, these findings were not statistically significant.

In comparison to Home/EU students, overseas students were more fearful of being a target of cybercrime. Our survey shows that overseas students are more fearful than Home/EU students in a range of areas including online scams, cyber-bullying, cyber-stalking and use of their intellectual property without their persmission. Independent t-tests showed these differences were statistically significant.

(e) Perception of security of services on the internet

Of all the services we asked to be rated in terms of security, our respondents reported 'use of public wifi hotspots', and free files downloading as the least secure (37% and 25% respectively). On-line home banking was perceived to be the most secure (49%), followed by on-line travel booking (40%).

The following are some of the key findings in this section:

- Females have a higher perception of online security than males
- Respondents aged 30-34 have the highest perception of online security. Above the age of 35 the perception of online security decreases to the lowest observed of any age group.
- Perception of security of online services is particularly high among respondents who identified themselves as 'other' ethnicity, closely followed by respondents from Asian/ Asian British backgrounds.
- The perception of security between Home/ European Union and Overseas students is rather similar.
- Respondents who were engaged in a PhD had the highest perception of security of services on the internet.

(f) Privacy

Here, we presented our respondents with a number of statements which we asked them to rate on a Likert scale of strongly agree to strongly disagree. Over two-thirds of our sample (67%) agreed/strongly agreed that 'consumers had lost all control over how personal information is collected and used by companies'. Only 2 out of 10 respondents agreed/strongly agreed that 'most businesses handle the personal information they collect about consumers in a proper and confidential way'. On questions which were specifically about social networking sites, our respondents were equally concerned about their privacy. Significant number of respondents were concerned about 'selling of personal information without prior consent (83%), 'changes to SNS privacy settings without prior notice' (71%), and web applications accessing personal information (61%).

These findings are worrying and demonstrate the anxiety of young adults in contemporary society.

(f) Cybercriminals vs Traditional criminals

Interestingly, over two-fifths of our sample believed cybercriminals to be more dangerous than traditional criminals. A question on dangerousness of cyber criminals compared with traditional criminals revealed that male respondents believed the former to be more dangerous. Just fewer than 25% of males 'strongly agreed' that cyber criminals were more dangerous than traditional criminals, compared with just over 5% of females.

4.2.3 SURVEY CONCLUSIONS

In a context where much of the existing research evidence points to the risky online experiences of children and young people (Böhme & Moore 2012, Eurostat 2011), our survey of young adults, particularly those in university settings, makes a useful contribution to the literature. Young adults living away from home are said to be particularly in need of establishing new relationships and social connections. Moreover, the need to use social networking sites (SNS) not only for social but academic purposes may be greater (Benson et al, 2014). Such a situation may demonstrate the potential for increased vulnerability. Our findings suggest, however, that whilst the fear of cybercrime may be palpable, the actual lived experiences of cybercrime are generally minimal. For example, only 14% of our sample reported having been a victim of cybercrime in the previous 12 months. This figure is somewhat higher in relation to particular types of cybercrimes. What is interesting but not wholly surprising is that the 'fear' of cybercrime is considerably high. In particular, our findings identify women and overseas groups to be more fearful of cybercrime victimisation. Future research would benefit from drawing a larger sample and disaggregating ethnicity/nationality from within the overseas group. It is possible that those living away from home and who use make greater use of SNS, and are reliant on public wifi at times will fear greater cybercrime victimisation. Certainly, our findings related to privacy and SNS are worrying and demonstrate the anxiety of young adults in contemporary society. Moreover, the anonymity of cyberspace adds to a heightened fear of cybercrime. Interestingly, although female respondents express greater fear of online victimisation, it is male respondents who believe cyber criminals to be more dangerous than traditional criminals. Here, it is possible that there is a male perception of being able to better protect oneself from a visible aggressor as opposed to one who is faceless, and possibly 'traceless'.

5.1 THE REGULATION AND GOVERNANCE OF CYBERCRIME

The regulation and governance of cybercrime and cyberterrorism faces general and issue-specific problems of cooperation. Discussing cybercrime, cyberterrorism and its impact on politics also adds to a long-term debate in political science whether technology is to be understood as a determining variable, so that politics follows advances of technology ('technological determinism'), whether it is a conditioning variable, so that it affects politics which needed to react to technological progress and its implications, or whether politics and technology interact, in the sense that politics influences technological progress in specific directions and the reverse (e.g. (Ferkiss 1973).

5.1.1 RELATIONSHIP BETWEEN CYBER TERRORISM AND CYBERCRIME

Adding more difficulties to these varying understandings of how politics, society and technology interacts is also an unclear definition of cybercrime, cyberterrorism or the more comprehensive term 'cybersecurity'. Cybercrime includes 'traditional' crimes like fraud that are now committed online, in which the computer is a tool, but also crimes in which the computer is the target, e.g. when malware is spread or used (e.g. (Jakobi 2013). Cyberterrorism is mainly focussed on the public impact cybercrime could have when targeting critical infrastructures. Cybersecurity refers to the security and safety of computers that are used for critical infrastructure, for individuals or organizations. The focus of cybersecurity can range from national security concerns to the protection of users or of technical systems. All these different aspects of cybercrime are taking place in a digital infrastructure that has weaknesses (ranging from defunct program codes with security weaknesses to risky behaviour of users), and in which even a market exist where criminals (but also security agencies) trade and buy data that enable exploitation of users and attacks on systems (Hunton 2012) (Holt 2013). There seems to be a growing number of cyberattacks that are targeted to achieve financial or political aims, and the geographical spread of attacks grows (Kim et al. 2012). Only some research exits on what ultimately influences the number of cyberattacks in a given country (Kigerl, 2012). Cyberterrorism statistics are hardly available and fully depend on where the borders of 'crime' and terrorism' is drawn: The Council of Europe Database on Cyberterrorism, for instance, shows that statistics are rarely available to countries (http://www.coe.int/t/dlapil/codexter/cyberterrorism_db.asp). It is also debated whether cyberattacks of any form are ultimately and effectively a threat comparable to other national security threats is debatable, and highly dependent on the targets, the impact and consequences of future attacks (Geers, 2009). Despite this lack of knowledge, there is a high political attention related to scenarios of possible cyberattacks and cyberterrorism even if such events might be highly unlikely. This is a general tendency in the 'politics of risk', and is explained by the fact that individuals – and policy makers – tend to pay more attention to high risk scenarios with low probability than to low risks with high probability (Daase, 2002). While therefore differences remain in the understanding, definition and impact of these crimes, this subsection refers to the general term 'cybercrime' when denoting any illegal or illegitimate activity in cyberspace.

5.1.2 Multidimensional Aspects of Cybercrime Regulation and Governance

While most research on regulation has focussed on the global nature of cybercrime and on identifying what exactly is the threat potential, less has been done on how to regulate, what to regulate and whom to involve in regulation and governance. To outline these lines of inquiry, the first part of this section elaborates on the multilevel dimension of regulating and governing cybercrime. It outlines the major challenges in this area and why cooperation is difficult to achieve. As governments are only one among many possible governance partners in this regulatory field, the section includes also a focus on non-state actors. Moreover, policy-making with regard to cybercrime is analysed, pointing out a general restriction in knowledge about causes, consequences and processes related to cybercrime and its regulation. Based on this overview, four fields for future research needs are identified: First, the definition, extent and the economic impact of cybercrime still needs consideration, including the question of political priorities in this diverse field. Second, reasons for policy convergence and divergence need to be more closely analysed, to ultimately bridge across the persistent and continuing differences in national approaches to cybercrime. Third, cooperation with non-state actors needs to be more closely analysed as their input to policy making is underdeveloped in some areas. Finally, there is a notable shift to discussions of human rights in cyberspace, a debate that so far had been absent from the mainly technical and economic debates about regulating cybercrime.

All in all, research on cybercrime ultimately needs to go beyond a technical perspective of analysing attacks to a more interactive perspective in which more emphasis is placed on how technology impacts on individuals' security and the reverse. Political consequences of such a perspective range from discussing responsibility of individuals and organizations (including companies that provide infrastructure and their software) to normative debates of what is legitimate activity in cyberspace.

5.2 *General Problems in the Regulation and Governance of Cybercrime*

International cooperation against cybercrime is difficult for four, partly related reasons: a) due to sovereignty protection of states, b) national security concerns, c) differences of the societal, cultural and legal background of countries and d) general weaknesses in implementation. Sovereignty protection relates to the fact that states are unlikely to enter cooperation if there is no immediate or long-term gain that can be expected from a treaty. While the regulation of cybercrime, as many other crime, at first sights seems to have cooperation benefits, related disincentives are substantial: For instance, states can profit from an unregulated cyberspace, in which the technical most advanced countries can actually play out their advantage in cybersecurity at the expense of others. One example of these mixed interests is the black market of security flaws in software, where both criminals and intelligence agencies can buy knowledge how to enter or intercept critical infrastructure (Hunton 2012). A treaty that, inter alia, limits such activities in cyberspace is not necessarily in the interest of all states. Furthermore, not all states investigate and prosecute cybercrime in a comparable way (Kshetri 2013): Some countries might shield offenders actively from law enforcement, while others do not have adequate policing capabilities or different priorities when fighting crime. Given the technical specificities of cybercrime and the difficulties in finding the source of cyberattacks, a treaty would suffer from limited possibilities to verify that states actually fulfil their obligations. The diversity of national legal, economic and social backgrounds further adds to the variety of state interests, cooperation targets and approaches against cybercrime. The implementation of regulations is particularly difficult related cybercrime, as cyberspace can accessed easily from anywhere in the world, and monitoring needs to stretch beyond territorial boundaries to be effective. Moreover, the technology used is advancing, and regulations that might be effective at one point in a time can be useless only a short time after. Finally, given the huge discrepancy in knowledge among users of cyberspace also means that the regulatory efforts and monitoring targets very different groups of users. The way cyberspace is used differs among individuals, as does the perception of associated risks that can range from naïve use to an assessments of risks and benefits (Ruginis and Rughinis, 2014). Moreover, there is only limited oversight to how far critical infrastructure is protected, as it includes private and public organizations. Finally, given that access and data exchange in cyberspace is usually organized through private companies, these need to be included in implementation efforts. All in all, the amount of non-state actors that are part of the regulation and governance of cybercrime is extremely high compared to other policy fields (Jakobi 2013).

Given the huge variance of cybercrime is, international counteractivities vary depending on what exactly they aim to fight: Choucri et al. used the concept of an 'ecosystem' of cybercrime governance, including treaties as well as international efforts of individual agencies like the FBI to come up with a list of institutions (Choucri et al. 2014). While this list sheds light on the variety of existent exchange and provides a useful overview, it does not say much about the difficulties of cooperation related to these institutions, how they are linked to each other or the impact they have.

5.2.1 International/Interregional Governance Approaches

Despite a large variance of cybersecurity initiatives, only one major multilateral treaty related to cybercrime exists, the Convention of the Council of Europe whose start dates back to 1996 (Council of Europe, 2001). It is the only instrument that was ever agreed against a background of different national aims and means in cyberspace. The draft treaty was developed with major input from the American Department of Justice and aligned to American laws (Wales 2001). It received criticism of stakeholders with regard to business and privacy concerns. Minor revisions to the draft preceded the adoption in 2001, and today has 49 signatories and 44 ratifications (Kierkegaard 2007:22) (Council of Europe, 2015). The Cybercrime Convention of the Council has also been signed by non-member countries, among them the United States. An additional protocol to the convention was adopted in 2004, criminalizing hate speech and other content-related offenses in cyberspace. (Council of Europe 2004, Council of Europe 2011). The convention contains a criminalization requirement of fraud, child pornography, illicit access to networks and other offenses. It aims to strengthen cross-national cooperation by regulating data availability to law enforcement and enable arrests across countries (Kierkegaard 2007:23, Calderoni 2010:343-344, Archick 2006:2). Given the limited convergence of national legal systems with regard to cybercrime, the status of instruments like the international search warrants in national law are debated (Keyser 2003:315-316, Calderoni, 2010:346). Moreover, the convention paved a way to increase data surveillance, as it requests providers to store traffic data (Keyser 2003:324-325). As the number of ratifications is restricted, the CoE convention is a global instrument that can still not prevent the existence of safe havens for cybercriminals, given a lack of countries covered, a restriction in scope and a lack of implementation in member countries (Calderoni 2010).

5.2.2 Regional Governance Approaches

Regional efforts against cybercrime are mainly confined to the European Union. With the growing area of justice and home affairs, cybercrime (listed as computer crime) has been part of a harmonization process related to criminal law. While Commission activities had been uncontroversial in some content-related areas like child pornography, others were met with resistance from the member states, for instance criminalization of copyright infringements (Mendez 2005:519-20). While cybercrime has been established successfully as an issue of European concern and Commission activity is therefore legitimised, important frameworks are sometimes resisted by member states or being cut back for legal reasons. The most recent example is a data storage directive of 2006 (European Commission, 2006). The directive was partly rejected resisted by member countries, in particular Germany, and later found to violate human rights principles by the European Court of Justice in 2014 (BBC 2014). Up until today, the commission thus faces difficulties in unifying the different members' interests and forming a coherent cyberspace policy (Barrinha and Carrapico 2014).

Besides from European regional activities, international cooperation related to cybercrime takes place in the framework of police and intelligence cooperation, for instance coordinated via Interpol or in the framework of other international organizations (e.g. (Choucri et al. 2014). Also bilateral cooperation is frequent, in particular among police and intelligence agencies.

5.2.3 Fragmentation in Cybercrime Regulation

With regard to political exchange and agreements, international cooperation is fragmented represents rather a minimum consent of what can be achieved in countering cybercrime in different areas. The reason for this is the huge cross-national variance in what is considered to be a crime, what legal and legitimate ways to counter it are, and how privacy and state surveillance is balanced. The failure of the European directive is a prime example for this tension. National laws and their enforcement therefore remain the cornerstone of governing cyberspace, and impact stronger on the actual prevention and prosecution than international arrangements. Aligned to national governmental regulation, the role of private internet providers is pronounced, as they usually store or access traffic data, and governmental agencies rely on this information. At the same time, given different interests and legal systems, there is considerable divergence in the interaction of public and private actors.

5.3 *Research Needs*

There is currently a range of emerging research issues related to the governance of cybercrime, mainly relating to a) the definition, focus and costs related to cybercrime, b) the reasons for convergence and divergence in regulating and governing cybercrime, c) increasing exchange with non-state actors and d) the development of legal and other normative perspectives on cybercrime.

5.3.1 THE FOCUS OF CYBERCRIME RESEARCH

Given the breath of cybercrime definitions, a focus is difficult to establish for politics as well as research. There are a range of cyberspace-related societal concerns that range from stalking to pornography, from malware to espionage, from loss of individual data to threats to critical infrastructure. While the term 'cybercrime' is ill-defined and can for these reasons be exploited politically, it can be doubted that there is the possibility for a coherent political action on cybercrime. Instead, it could be useful to clearly distinguish the dangers, the impact, the offenders and the victims of different cybercrimes. Future research could invest more in classification of threats, e.g. cybercrime with a high-risk or low-risk, or those with a high impact or low impact. Such classification can also help setting governmental priorities.

Partly due to the unclear definitions, the extent of damage due to cybercrime is highly debatable, and given a strong emphasis of company-related research in this field, political actors have expressed the concern that the extent of damage might be inflated (Anderson et al. 2013:267). Reliable crime statistics are difficult to establish, and often used for political aims (e.g. (Andreas and Greenhill, 2010), so that cybercrime would not be an exception in this regard. There has been some work to assess the damage of cybercrime independently of business analyses, to guarantee independent review of the economic costs, but this is rarely done (but see (Anderson et al. 2013:267). Even in such assessments, a clearer distinction could be made in the calculation between the direct costs of cybercrime as costs directly caused by criminal activity, and cost that occur to avoid impact of criminal activities, questioning whether the latter are necessarily cybercrime-related costs. Other areas of crime governance would usually not include these costs either, when assessing costs of crime (e.g. costs for an average door lock are usually not conceived as costs related to crime, but as standard security necessity of houses independent of the local crime rate). Distinguishing between the direct costs of cybercrime, and the value/costs of the related security industry could enrich the debate of what the main damage of cybercrime is. It could also shift a focus the most effective safeguards relating to cybercrime, as these might include a requirement to deliver better software (e.g. software-producing companies) to a more comprehensive computer-education of users.

5.3.2 DIVERGENCE AND CONVERGENCE OF CYBERCRIME REGULATION

Problem pressure related to cybercrime is a potential source of harmonization or some degree of convergence in the legal and political realm. Reasons for divergence, however, are strong and concern, inter alia, the societal importance of cybercrime, different political understandings of how a legitimate fight against cybercrime can look like or legal cultures and principles. For instance, a comparison of Estonia, the United Kingdom and Germany shows the high degree of variance that exist even in EU countries. Estonia has been affected by early and prominent cyberattacks and is an important example of how small, technological advanced states can react to cybercrime (e.g. Geers 2009:5-6). While the case had a high impact on NATO policy development, its influence on EU affairs is nonetheless limited. In contrast, the UK and Germany represent powerful EU members and large, advanced economies and have tried multiple times to set cybercrime agendas. Yet, their approach to cybercrime regulation is different for cultural, legal and historical reasons. Cybercrime is discussed for years as a threat to the UK economy (e.g. (Hunton 2012:202) The UK has initially been affected strongly by the ECJ decision, as it has a comprehensive regime of monitoring and storage of traffic data. As a consequence, national emergency legislation was introduced that covers similar areas as the directive, and gives law enforcement comprehensive access to communication data (Jakobi 2015). Regulations typically follow the principle of enabling state agencies vis-à-vis criminals, while privacy concerns are limited. In stark contrast, Germany resisted the implementation of the 2006 EU directive, risked a fine for non-compliance and welcomed the ECJ rejection of the directive (Die Zeit 2014). The degree to which companies should store traffic data and how much information could be available to law enforcement agencies is typically discussed controversially. Constitutional limits in how far the state can monitor citizen activities are high in Germany, given a repeated history of state surveillance and violation of human rights in the 20th century. In contrast to the UK, German discussions on surveillance and monitoring are less pragmatic, but oriented on avoiding a strong state position that might harm citizen rights and privacy.

The regulation of cybercrime is thus, like any other regulation, intrinsically linked to the national political system, its history and culture. However, research on policy diffusion, policy learning and policy convergence has frequently shown that even diverse political systems tend to become more similar over time in some areas (e.g. (Heichel et al. 2005). This strand research has not yet been applied to the study of cybercrime regulation, and future research could benefit from analysing which areas of cybercrime regulation are more likely to converge than others. This could contribute to the existent research literature as well as it would enable political pathways to international consensus on cybercrime regulation.

5.3.3 STATE AND NON-STATE COOPERATION IN REGULATION AND GOVERNANCE

Non-state actors like companies, non-governmental organisations etc. have become important part of many issue areas of crime governance (e.g. (Liss and Sharman 2015). Non-state actors rise awareness regarding crime, but they also implement regulations that governments decide. The governance of cybercrime is particularly dependent on non-state actors, for instance with regard to the storage of traffic data, but also with regard to the surveillance of computer systems, the prevention of attacks or the education of potential threats and vulnerabilities. Future research could analyse how the public-private interplay can be facilitated and which problem of implementation are likely to be expected. There is an ongoing debate on the role of private actors in regulation and governance, analysing the transnational processes involved in standard setting (e.g. Djelic and Sahlin Anderson 2006). The results show that non-state actors often disseminate standards that are not necessarily related to governmental intervention, including self-regulation. While being acknowledged in the literature for a while, this important role of non-state actors has not yet been explored sufficiently in the area of cybercrime, Industry self regulation, e.g related to security standards, could deliver important contributions to prevent cybercrime, but no research on potential benefits and shortcomings exist.

So far, non-state actors are mostly involved in the implementation of cybercrime regulations, less non-state activism is visible with regard to policy-development and public debate in the prevention and prosecution of cybercrime (Jakobi 2015). Future research could analyse the extent to which politics regarding cyberspace can be based on a more public input of civil society, and how society can become engaged in the discussion among cybercrime. A stronger participation of civil society could benefit not only the policy-making process, but could contribute to awareness on how users can protect themselves in cyberspace.

5.3.4 LEGAL VERSUS OTHER NORMATIVE PRINCIPLES IN CYBERSPACE

Cyberspace is not only a legally widely unregulated space, but is also mainly discussed under a technical frame. Only recently, debates about human rights and cyberspace have started, leading to the declaration of human rights and principles in the internet (Internet Rights and Principles Coalition 2014). The declaration, the outcome of several NGOs aims to set new standards in how human rights can be protected and strengthened in the internet. Research has not yet analysed the implications of such perspective, despite the centrality of human rights in international and national politics. While criminalization is only one way of including normative standards, cyberspace is also affected by other developments, e.g. bullying, spread of misleading information or other activities that are not clearly criminal. Proponents of an unregulated cyberspace emphasize that rules often restrict political freedoms and are usually (in particular important in authoritarian countries). Research on cybercrime has not yet turned to these areas that are not illegal, but nonetheless considered partly illegitimate, and whether there are other ways of changing user behaviour than criminalizing, or how regulations can be set in place without supporting authoritarianism and political censorship.

Changing normative expectations has also implications for democratic decision-making: Cyberspace has enabled e-government and e-democracy for more than a decade (e.g. (Chadwick and May, 2003, Chadwick 2003), but only little research has been done so far on how cybercrime might affect these services and which priorities for security should be set. The limits of defining cybercrime have some effects here, too: For instance, misinformation in cyberspace might have a huge effect on public opinion, and countries like Russia and China have been suspected to employ PR agencies to set opinionated or false information into public discussion forums (Freedom House 2013:6). As it is difficult to consider this to be a formal crime, more research on legitimate and illegitimate activity in cyberspace would be beneficiary to gain a normative framework on cyberactivism, cybercrime and e-democracy.

5.4 *CONTRIBUTION OF LEGAL FRAMEWORKS*

Perhaps one of the most well-known pieces of cyber space regulation within the EU is the EU data protection directive. As discussed in the previous section, such a directive is open to interpretation and we see here the effects of the cultural and historical context on the different interpretations of the directive across the Union. We take a closer look at this directive in the following sub sections.

5.4.1 EUROPEAN REGULATORY FRAMEWORK FOR PRIVACY AND DATA PROTECTION

The *Charter of Fundamental Human Rights of the European Union* (European Commission,2000) lays down the basic ethical principles that represent the shared values upon which the EU is founded. As published in the Official Journal of the European Communities, it highlights:

- Respect for human dignity,
- Respect for autonomy (based on the people's decisional capacity),
- The right to the physical and mental integrity of the person, and
- The protection of individuals' privacy and protection of personal data.

Specifically within the context of preserving the individual's right to privacy, the European Union has put into effect the appropriate legal framework comprising of a multitude of directives, regulations and amendments. The current framework is put into place in order to protect the individual from infringement of their right to privacy, which could be a direct result of a cyber offense or any illegitimate processing of data.

This legal framework addresses issues of privacy and data protection including, to a certain extent, security. It also provides a basis for the validation of compliance of information and communications systems in terms of ethical, privacy and data protection requirements. Within this document, we provide a concise summary of the current state of EU regulation.

5.4.1.1 EU Data Protection Directive (1995/46/EC)

The Data Protection Directive (1995/46/EC) (European Commission, 1995) of 1995 applies to data processed by automated means (i.e. ICT systems) and data contained in non-automated filing systems (i.e. conventional archives). It does not apply to the processing of data during personal activities or within operations concerning public or State security. It sets guidelines to protect the rights and freedoms of the individual with respect to the processing of their personal data, relating to:

- the **collection of dat**a for explicit and legitimate purposes,
- the **quality and accuracy** of the data,
- the **legitimacy of the data processing** with the individual's unambiguous consent,
- **the definition of special categories of data** that require certain provisions to be made (i.e. data revealing racial/ethnic origin, political opinions, religious or philosophical convictions, trade-union membership, health data, etc.)
- the **subject's right to data access** by the data controller (i.e. the individual must be able to access the data collected from them)
- the **subject's right to information** by the data controller (i.e. the subject must be informed on the purpose of data collection and data processing methodology etc)
- the **confidentiality and security** of processing,
- the subject's **right to object** to the processing of data relating to them,
- the **notification of processing** by the data controller to a competent supervisory authority (which the EU Member States are required to provide),
- the **transfer of data** between EU Member States and Third Countries, and
- **various exemptions and restrictions** leading to a clear definition of the Directive's scope.

In case of violation leading to a breach of rights, the individual reserves the right to seek judicial remedy. Moreover, the person who suffered damage as a result of unlawful processing of their personal data is entitled to seek compensation.

Most EU Member States, however, have implemented the 1995 Directive in different ways thus leading to significant fragmentation. Therefore, the EC has proposed (Jan.2012) a recent comprehensive reform of the Data Protection rules, including the proposal for a *"Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing* *of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.”* The proposed reform aims to lead to a single law, namely the “General Data Protection Regulation”. It is estimated that this law will be adopted in late 2014 and will be followed by a two-year transition period. This new law will extend the scope of the current directive to all foreign companies processing data of EU residents and greatly help harmonise the legislation that is currently in effect across Europe.

5.4.1.2 EU Directive on Privacy and Electronic Communications

The 2002/58/EC Directive on Privacy and Electronic Communications (European Commission, 2002), is designed to regulate the electronic communication sector and amend other existing regulations, as part of the “Telecoms Package”. This Directive principally concerns the processing of personal data relating to the delivery of communications services, stating that the relevant service providers need to ensure:

- that personal data are accessed by authorised persons only,
- that the integrity of personal data is protected (i.e. from being destroyed, lost or accidentally altered),
- that an appropriate security policy on the processing of personal data is implemented
- that there is no unauthorised data retention (i.e. traffic data and location data must be erased or made anonymous when they are no longer required for the conveyance of a communication or for billing, except if the subscriber has given their consent for another use.)

In the case of an infringement of personal data, the service provider must inform the person concerned, as well as the respective National Regulatory Authority (NRA). The users also retain the right to:

- Opt-in to unsolicited electronic communications for commercial reasons (spamming),
- Give their consent for information to be stored on their terminal (including cookies and any kind of software, malicious or otherwise)
- Give their consent for their telephone numbers (landline or mobile), e-mail addresses and postal addresses to appear in public directories.

The Directive also reiterates the basic principle that Member States must, through national legislation, ensure the confidentiality of communications made over a public electronic communications network. Each Member State must: “*prohibit the listening into, tapping and storage of communications by persons other than users without the consent of the users concerned. The subscriber or user who stores their information must first be informed of the purposes of the processing of their data. They have the option to withdraw their consent on the processing of traffic data*.” Member States are also required to put in place a system of penalties and legal sanctions to be enforced in the case of infringements to the provisions of this Directive. National competent authorities need to be allocated the necessary powers and resources to ensure compliance with the national provisions.

The “Telecoms Package” was further amended in December 2009 by the two Directives on “Better law-making” and “Citizens’ rights”, and the establishment of a body of European regulators for electronic communications (BEREC).

5.4.1.3 EU Regulation on Data Protection by Community institutions and bodies

The 45/2001 Regulation on data protection (European Commission, 2001) amends the EU Data Protection Directive and contains provision relating the processing of personal data by institutions and bodies of the European Union, aiming to ensure a high level of protection. It pertains to:

- fair, lawful, non-excessive processing of data,
- collection of data only for single-use and for specified, explicit and legitimate purposes,
- accurate storage of data which also permits identification of data subjects for no longer than necessary

This regulation also foresaw the establishment a “**European Data Protection Authority**”, an independent Community authority responsible for monitoring the application of the data protection rules by the EU institutions and bodies. The European Data Protection Authority allows citizens to directly file complaints if they consider their data protection rights have been compromised. Each Community institution and body is also required to appoint at least one person as a **Data Protection Officer** with the task of cooperating with the national Data Protection Supervisor and ensuring that the rights and freedoms of the data subjects are respected. This regulation also reinforces the EU Data Protection directive, so that citizens retain the right to access, rectify, block or delete personal data relating to them in files held by the Community institutions and bodies.

5.4.1.4 Support for Privacy Practices

According to the Data Protection EC Directive 2002/46/EC, Personal Data are defined as:

> *“any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (art. 2 a)”*

A similar definition of Identity Data including data protection methodologies have been adopted in other documents as well. For example, Special Publication 800-122 (“Guide to protecting the Confidentiality of Personally Identifiable Information”) (NIST, 2010) was issued by the United States National Institute of Standards (NIST) and the US Department of Commerce, defining Personally Identifiable Data (PID) as:

> *“any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information”.*

Based upon the existing legislation and guidelines, a number of international standards and paradigms have evolved to provide the guidelines for the development of ICT systems that process personal data while safeguarding the citizens' right to privacy. Within the next subsections, we will provide a concise review of the ISO and OASIS families of standards on privacy and the management of personal data as well as provide some best practices on the proper design of ICT systems that manage personal data.

5.4.1.4.1 Privacy By Design

Embedding privacy in the design of an ICT system that is expected to handle personal data is not an easy task. It requires a systematic approach to the design and development of ICT systems, aiming not only to ensure compliance to current legislation but also to increase user trust, which may significantly affect the rate of adoption. The principle of Privacy By Design (PbD) highlights the need to adopt best practices as early and consistently as possible. This concept may be applied to information technology, organizational practices, physical devices etc. and implies:

- A clear and demonstrable commitment to uphold high standards of privacy,
- The establishment of specific methods to recognize poor and failing designs and ways to repair them,
- A continuous iterative process for risk assessment and management.

The need to include data protection controls in a system's design gave rise to a number of tools and standards (Finn et al 2013) for:

- **Privacy self-assessments** help users and organizations (an example can be found in the footnote[7]) to document data flows and processes in a systematic way, in a preliminary phase. Usually implemented as comprehensive checklists and benchmarks against which an organization's privacy "readiness" may be quantized, privacy self-assessment tools provide useful insight during initial organizational planning.
- **Privacy impact assessments** aim to identify and mitigate the risks associated with personal data processing. Multiple documents, methodologies and guidelines are available[8], covering different aspects of application, timing, transparency, levels of prescription etc.
- **Risk management**[9] involves the identification of areas of highest risk, so as to apply the appropriate proactive measures and integrate them into operational policies.
- **Privacy management frameworks (examples can be found in the footnotes**[10,11,12]) are systematic and verifiable methods for instilling privacy and security principles and injecting

[7] Example: Office of the Information and Privacy Commissioner of Ontario, Canada, Guardent and PricewaterhouseCoopers, (2001). Privacy diagnostic tool workbook and FAQ, Office of the Information and Privacy Commissioner of Ontario, Canada. (Accessed November 2014): http://bit.ly/gAhbsN and http://bit. ly/eaHrMv.

[8] Example: RFID PIA framework adopted by the EU: (Accessed November 2014): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

[9] Example: The ISO/IEC 27005 standard Guidelines for Information Security Risk Management.

privacy objectives into information and communication technologies. Privacy management frameworks usually include privacy, security and accountability controls and aim to maximize user trust in the system or process in question.

Concepts such as privacy are socially-constructed and have different cultural and historical significance from country to country. As a result, privacy and the protection of it is a highly contested area. The response to this contestation has been to define standards in the area. Privacy related standards are outlined below.

5.4.1.4.2 Privacy-Related Standards

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are the main bodies that form a specialized consortium for worldwide standardization. Various national bodies, governmental and non-governmental organizations etc. participate in the creation of international standards as members of ISO or IEC, through the establishment of special technical committees that apply their work in specified areas of technical activity. In the field of information technology, ISO and IEC have established a Joint Technical Committee, ISO/IEC JTC 1, whose main task is to prepare International Standards on Information technology in strict accordance with rules and guidelines already defined within the ISO/IEC Directives.

Draft International Standards that are prepared by the JTC may then be circulated to national bodies for voting. In order for a draft to be accepted and published as a Standard, an approval rate of at least 75 % of the national bodies casting a vote is required. The Subcommittee SC 27 is created within JTC 1 and is devoted to IT Security Techniques. Within SC 27, a dedicated Working Group (WG5) has been set up, focusing on Identity Management and Privacy Technologies. The privacy-oriented standards that WG5 is responsible for drafting include the:

- ISO/IEC 24760 Framework for Identity Management,
- ISO/IEC 29100 Privacy Framework, and
- ISO/IEC 29101 Privacy Reference Architecture.

ISO/IEC 24760 defines a framework for identity management, focusing on defining what constitutes Identity information and their attributes, how to manage the data lifecycle, Identity Management requirements and implementation, control objectives and information access management (policies, privileges, authorization, authentication etc.). Identity is defined as a set of characteristics or attributes representing an acting entity, while a partial identity is defined as a subset of those characteristics. Furthermore, in ISO/IEC 24760, unified and differentiated identities are defined. ***Unified identities*** (user accounts, authentication methods etc.) are used to ease administration

[10] Example: The PACT project Privacy Reference Framework for Security Technologies (PRFST) and Decision Support System (Accessed November 2014): http://www.projectpact.eu

[11] Example: The PRISMS project decision support system (Accessed November 2014): http://prismsproject.eu/?page_id=13

[12] Example: The SURPRISE project theoretical framework (Accessed Novemebr 2014): http://surprise-project.eu/research/

within an organization, while individuals might prefer ***differentiated identities*** to protect their privacy and anonymity, especially in the World Wide Web. The identity data lifecycle and flow are also defined within this standard, supporting the design of the architecture of an Identity Management system (IdM). Currently, ISO/IEC 24760-1 ("Part 1: Terminology and Concepts") has been completed, while the remaining two parts ("Part 2: Reference Framework and Requirements" and "Part 3: Practice") are still under development. The terminology and basic concepts of data lifecycle serve as a basis for the 29XXX family of ISO standards.

The ISO/IEC 29100 Privacy Framework defines the requirements for safeguarding Personally Identifiable Information (PII) processed by any ICT system, across any jurisdiction. It is internationally applicable and general in nature, in the sense that it takes into account organizational, technical, procedural and regulatory matters. Specifically, it sets common privacy terminology and principles. It also lists privacy features to be upheld in conjunction with security guidelines. It also serves as a base for other relevant documents and standards (e.g. privacy reference framework architecture, assurance of privacy compliance etc.). Within this framework, the PII Providers and PII Receivers are defined as the Actors. The PII providers may be the users of an ICT system, subscribers to a service, the data owners etc., while the service/application providers, administrators of a system etc. are perceived as the PII receivers. The PII providers set their privacy preferences. Privacy requirements and safeguarding controls are applied during the PII lifecycle including the collection, storage, use, transfer and deletion of information. The PII receiver is required to define a Privacy Policy based on existing requirements and internal rules.

This standard also aligns with the 2002/58/EC E-Privacy Directive by the European Commission and the NIST Special Publication 800-53 Revision 4 titled "Security and Privacy Controls for Federal Information Systems and Organizations" (NIST, 2013) which concerns the creation of a security and privacy framework to be applied in Federal Government Information Systems.

The ISO/IEC 29101 Privacy Reference Architecture aims to provide guidelines in order to maintain the effectiveness and consistency of any technical implementation of privacy safeguarding mechanisms within ICT systems. It resolves to suggest a privacy-enhanced system architecture that enables the creation of cohesive privacy protection mechanisms within and across ICT platforms.

The ISO/IEC 27000 family of standards focuses on Information Security Risk Management. ISO/IEC 27001 provides the Requirements, while ISO/IEC 27002 includes the Code of practice for information security management. The ISO/IEC 27005 standard provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements listed in ISO/IEC 27001. However, this International Standard does not provide any specific methodology for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. In this standard, the risk management process comprises of:

- Context Establishment,
- Risk Assessment,
- Risk Treatment,
- Risk Acceptance,
- Risk Communication, and
- Risk Monitoring and Review.

The Organization for the Advancement of Structured Information Standards (OASIS) is an international consortium that works on the development, convergence and adoption on e-business and web service standards. OASIS set up in 2010 the Privacy Management Reference Model (PMRM) Technical Committee (TC), in order to further refine the already existing International Security, Trust, and Privacy Alliance (ISTPA) framework. PMRM aims:

> *"to provide a standards-based framework that will help business process engineers, IT analysts, architects, and developers implement privacy and security policies in their operations"*[13].

The PMRM provides pragmatic guidelines on how to map those privacy requirements into a well-defined set of privacy-supporting services. Specifically, the main goal behind the PMRM is to help decision makers map clearly defined sets of privacy into the operational services that specify *how* privacy will be managed, while helping avoid semantic debates. The PMRM provides a complete and ever evolving set of privacy services that can be implemented, flexibly combined into functionalities, and invoked on command. It thus supports moving privacy management from the policy domain to operations. PMRM approaches are also useful for the policy makers as it can help them identify too current weaknesses or shortcomings in existing policies and to establish best practice guidelines.

5.5 *GEOPOLITICAL CASE STUDY – PORTUGAL*

In the following section, we can see how the use of legislation to protect the individual's privacy in cyber space and the imperative to protect the state against cyber terrorism interoperate.

5.5.1 INTRODUCTION TO THE PORTUGESE SCENARIO

Technology is one of the strategic factors driving the increasing use of Internet. While many benefits of the Internet are self-evident, as the facility the communications between people and within organizations, it moved societies into an ubiquitous computing environment; their daily activities have become automated and are relying on remote computer networks thanks to ubiquitous computing environment with the increase in using the Internet and Internet protocols for their operations; more and more industrial and infrastructure applications move from relying on dedicated, proprietary networks to using the Internet and Internet protocols for their operations (Lewis 2002).

In this sense, as we embraced the convenience and effectiveness of the Internet into our lives, homes, retirement plans, and even wallets, we also opened the door to a new breed of attackers determined to gain profit from this wonderful new cyber world. Motivated by fun profit, and even political motives, cyber attackers have now impacted, or threaten to impact, most realms of our lives (ONS 2014).

This raised new questions about vulnerability, threats, security and privacy since cyberspace became a new device for criminal purposes. The more we use the cyber technology the more it is likely to be

[13] OASIS Privacy Management Reference Model (PMRM) TC, (Accessed November 2014), http://www.oasis-open.org/committees/pmrm

used against us. The greater dependence of our societies on information technology makes us more vulnerable, exposing targets that would otherwise not be accessible (McGuire and Dowling 2014).

In this regard the fight against cybercrime and cyberterrorism is now a great European and International priority and also a challenge, since it is not only the need to protect Western democracy model, that is threatened by insecurity, panic and pain, but the reaction of the states. These may be tempted to threaten the very model of democracy they represent, jeopardizing what is its very foundation - the rights, freedoms and guarantees of citizens such as we understand them in our societies.

5.5.2 PORTUGAL LEGAL LANDSCAPE

According to several international studies and indicators Portugal is among the safest countries in the world, and the overall crime, including violent and serious crime, has dropped uninterrupted and consistently since 2008. In 2013 it was the best year of the last 10, and the findings relating to 2014 "are very encouraging and seem to confirm this trend of remarkable and sustained drop in crime" (LUSA, 2015). The focus on security conditions as a strategic vector of economic recovery and ensure the full right and fundamental freedoms of citizens proved to be of the utmost importance and contributed to the remarkable growth of tourism, a crucial area for the Portuguese economy.

Given the increasing development and use of new technologies, particularly those that provide access to the Internet, whether in the context of infrastructures or in the individuals daily life, Portugal is equally vulnerable and exposed to cybercrime and cyber terrorism.

Portugal adopted the Convention on Cybercrime (Budapest) in 2009, through the Parliament Resolution No. 88/2009 from 15 September. Since that date there were no changes to the Convention in Portugal.

The current criminal investigation often resorts to measures of evidence collection in digital form assuming the collaboration from private entities (eg Internet service providers). Such entities - generally private companies - are the only holders of important information, often decisive for the discovery of truth. In addition, some of the specific procedural steps, the specificity of the environment in which they develop, contradict some of the procedural tradition by requiring effective collaboration from communications operators with prosecutors and criminal police in a way that was not allowed, in previous legislative frameworks, (secrecy of telecommunications).

In 2009, a national unit was established in Polícia Judiciária (PJ), aiming at centralizing the knowledge and action towards prevention and investigation of computer and technology crime. Nowadays, this action is descentralised in regional departments of this criminal force as it becomes more and more difficult to separate cybercrime from other criminal behaviours.

According to PJ, the major crimes currently investigated are computer fraud, fishing, child pornography, unlawful access (violation of business networks and violation of e-mail and social networks such as Messenger or Facebook), and computer sabotage. These crimes have registered a proportional increase with the increased use of Internet, especially in metropolitan areas with has easier access to knowledge, computers and the Internet. To combat these type of crime, PJ works much in cyberspace, operating 24 hours a day and seven days a week. (LUSA, DN Ciências, 2009). The highly complexity of these crimes, and the increasing number of processes and huge volumes of data to analyse have led to high delays in conclusion of criminal cases and high economic losses. Investigations to crimes such as internet child pornography, require important human and technical resources for extensive analysis, screening, decoding of data, including photos and videos that are encrypted or concealed and the identification and location of both criminals and victims.

5.5.2.1 *Data*

It is difficult to have a global overview, because there is a lack of data from private sector, namely companies, banks, insurance companies and financial institutions, when they are victim of any kind of cybercrime. In general, these entities prefer not to complain to the authorities and solve the problem internally absorbing losses. They fear that such attacks being public, could lead to their disrepute and loss of trust from their customers. Most of the time, they consider that the consequences of communication any cybercrime may be greater that the criminal occurrence, namely there may be legal liability due to the protective duty of confidential data. Another common reason is the poor level of awareness or the belief of the ineffectiveness of the criminal inquiry and the feeling of impunity of these crimes. This makes it difficult to measure the reality and to perform, quantitative and qualitative assessments about the reality and the consequences to economy and politics.

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

Table 3 - Statistical data gathered by PJ[14]

5.5.3 PORTUGESE LEGAL FRAMEWORK RELATING TO CYBERCRIME AND CYBERTERRORISM

[14] This table shows us the evolution of numbers of PJ investigations and complaints directly communicated to PJ. These data relate only to computer crimes and that the crimes perpetrated with a computerized system resource.

5.5.3.1 *Legislation*

Although in the Portuguese national legal system, cyber attack and cyber terrorism are not typified as crimes, they are pointed in several internal legislation[15]:

> Constitution of the Portuguese Republic recognizes data protection as a sui generis right. This is contained in Article 35 which specifically highlights the Constitutional importance of Data Protection in Portugal. Accordingly, data protection has a particular constitutional setting in Portugal that is similar to Article 8 of the Charter of Fundamental Rights of the European Union;
>
> Resolution of the Council of Ministers No. 7-A/2015 of February 20 - National Counter-Terrorism Strategy;
>
> Decree Law 69/2014, of May 9, 2014 established the National Centre of Cyber Security. The Centre's mission is to contribute to the use of cyberspace in a free and secure way, as well as to monitor anticipation, detection, and incident response regarding cyber attacks. The mission of the Portuguese Criminal Police - Polícia Judiciária (PJ) - is to assist the judicial and prosecuting authorities in investigations, to develop and foster preventive, detection and investigative actions, falling within their jurisdiction or the actions which Polícia Judiciária is entrusted in association with the competent judicial and prosecuting authorities. Within the scope of cybercrime and cyber terrorism, PJ must be immediately informed of any crimes that are being prepared or executed. The CyberCrime Office, set up by order of the Attorney General, is the key authority in the internal coordination of the Public Prosecution Service as far as this crime area is concerned. The Office is also involved in the development of scientific training and the in creation of communication channels, in particular between criminal police bodies and communication network access service providers, thus enabling criminal investigation cooperation.
>
> The Cybercrime Law (Law 109/09 of August 17). This piece of legislation approves the CyberCrime Act and transposes to the national legislation the Council Framework Decision no. 2005/222/JHA16 thus adapting national legislation to the Council of Europe Convention on CyberCrime. The National Security Office is a central service under the administration of the State endowed with administrative autonomy, subordinated to the Prime Minister, whose mission is to guarantee the security of classified information, both at national level and within the scope of international organizations to which Portugal is party. Furthermore, the Office acts as a clearing authority for people and companies in relation to the accessing and handling of classified information;
>
> Assembly of the Republic Resolution No. 91/2009, of September 22 - Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of Nature Racist and Xenophobic Committed through Computer Systems, adopted in Strasbourg on 28 January 2003;

[15] Qualification common types of crime through computer: Computer fraud (art.221 C.P. and 5 L.C.I.) and Computer damage (Article 5. LCI should relate to 212 and 55 CP)

[16] Council Framework Decision no. 2005/222/JHA, of February 24, 2005, on attacks against information systems

The Parliament Resolution No. 88/2009, of September 15 - Convention on Cybercrime, adopted in Budapest in November 23, 2001;

Law No. 32/2008, of July 17 - Transposing into national law the Directive 2006/24 / EC of the European Parliament and of the Council of 15 March on the retention of data generated or processed in connection with the provision of public electronic communication services available or of public communications networks;

Decree-Law No. 176/2007, of May 8 - Makes the first amendment to Law 5/2004 of 10 February (Electronic Communications Law), establishing the penalties of the acquisition, ownership and use of illicit devices to private purposes in the field of electronic communications;

Law No. 5/2004 of February 10 - This law establishes the legal regime applicable to networks and electronic communications services and associated facilities and services and defines the powers of the national regulatory authority in this field, as part of the implementation process of directives of the European Parliament and of the Council.

Decree-Law No. 7/2004 of January 7 - Directive on electronic commerce - This law aims mainly at transposing Directive 2000/31 / EC of the European Parliament and of the Council of 8 June 2000.[17]

Law No. 41/2004 of August 18 - Transposing into national law Directive 2002/58 / EC of the European Parliament and of the Council of 12 July, concerning the processing of personal data and the protection of privacy in the electronic communications sector;

Law 5/2004 of February 10 - Electronic Communications Law

Law No. 67/98 of October 26 - Personal Data Protection Act (transposing into the Portuguese legal system Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data);

PENAL CODE, Decree No. 48/95, of March 15 (already has an updated version);

Law 109/91 of August 17, on Cybercrime;

Decree-Law No. 63/85 of March 14 – Official Journal No 61, Series I, of 03.14.1985 - Adopting the Copyright Code and Related Rights.

[17] The Directive on **electronic commerce**, despite the name, does not regulate the entire e-commerce: leaves large areas open. On the other hand, it deals with issues such as e-procurement, which only has regular sense as a matter of common law and not just commercial.

5.5.4 ADDITIONAL PORTUGESE LEGAL INSTRUMENTS

There are a number of additional instruments that support the legal instruments. These include the Portuguese strategy on cybersecurity and the Computer Emergency Response Team; in order to promote cyber security at the national level, particularly in in the context of critical infrastructure protection, the Foundation for National Scientific Computing established the Portuguese Computer Emergency Response Teams (CERT.pt). This has been encouraging a national network of Computer Security incident Response Team (CSIRT), in specifically related critical infrastructure sectors namely: Communications, infrastructures, Energy, Transport, Banking and Public Administration.

Protocol between the Attorney General's Office and communications operators in order to increase mutual cooperation and to achieve greater effectiveness in fighting cybercrime and obtaining digital evidence;

Cybercrime Office - The prosecution of the Activity Coordination Office in the area of Cybercrime is headquartered in Attorney General of the Republic, under his dependency. Its general scope is the coordination, the specialized training and the establishment of communication channels with Internet service providers, to facilitate the criminal investigation[18].

5.5.5 SUMMARY OF THE PORTUGUESE CASE STUDY

Portugal, like all other EU countries, is involved in a reality shaped by informatics technology and, ever more, by internet and social networks. These are the mirror of natural conflicts between people, therefore, there has been an increased number of complaints to the police, and with regard to reality of police work, there has been a considerable effort to have the work done, considering the legal constraints, the increasing volume of information and lack of police officers and other police professionals.

The Portuguese law, relating to computer crime, in general, is in line with the guidelines enshrined in Budapest Convention (2001), but there are still **gaps**, especially those concerning to achieve a more effective criminal investigation, namely:

- some definitions specific from internet environment are still not set out in Portuguese law. For instance “computer data”, “service provider” or “traffic data” etc.;
- the 9º article of Budapest Convention establishes the 18-year-old age as a reference when it comes to underage; in Portugal, the Penal Code, in article 172º establish 14 years old;
- the Convention criminalizes the **mere** possession of child pornography (nº1 art.9ª) , Portugal also criminalizes that possession only if is for the **purpose of display or assign** (nº3 art.172 Penal Code);
- number 2, article 19º of Convention establish the possibility of the authorities investigating computer crime, access other computer systems such as banks, but if the Portuguese law reference the possibility to access to electronic communication by providers

[18] http://cibercrime.pgr.pt/gabinete/gabinete.html

of electronic communications, still leaves out other entities, such as banks, which place constraints to fighting against economic crime (both tax evasion, money laundering).

6 IMPLICATIONS FOR RESEARCH

In the previous sections, we have identified that there are research gaps that need to be addressed if we are to move forward with our social, political, legal and economic understanding of cybercrime. However such research must conform to ethical and legal standards. This is yet another area of contestation that requires consideration. In this section we outline some of the issues and the current thinking in this area/.

6.1 ETHICAL AND LEGAL IMPLICATIONS OF SECURITY RESEARCH

During the last years, research has started regarding the ethical background, as well as obligations, when conducting research in the area of IT-Security. While in earlier times research mostly took place on sealed environments in the possession of the researcher, security research on commonly used protocols or common infrastructure started blurring the line between research and actual manipulation of systems. Furthermore, the ethical implications of publishing unsolved security issues in commonly used products can open up a wide variety of ethical considerations.

In (Schrittwieser et al. 2013) the authors analyse and discuss a selection of well-known publications in the area of IT-Security that can be considered as borderline papers with respect to the ethical aspects of the underlying research, focussing on the justification of the research as given by the respective authors. A special focus is put on the fact that nowadays (a) many researchers either need to verify their theoretical research in the wild on real networks in order to justify their theories, (b) for studying existing infrastructures in order to generate realistic results, no models of said systems can be built and (c) many ethical implications of data driven research are brought to security research through the use of big data approaches and the analysis of real data instead of pure theoretical reasoning. In [1] the authors propose four fundamental criteria for evaluating the ethics behind research, derived from related aspects in medical research:

1. Do not harm humans actively.
2. Do not watch bad things happening.
3. Do not perform illegal activities to harm illegal activities.
4. Do not conduct undercover research.

While the authors do not claim that research not following these rules must be considered unethical, they state that at least better arguments for violating these principles are needed and must be demanded by editors of scientific conferences and journals. Furthermore it must be noted that in several legislations all these aspects can lead to criminal charges against a researcher, who would then maybe have conducted a case of cybercrime him/herself. Some related aspects, but seen from the view of general psychological research on the Internet, have been put forward in (Nosek et al. 2002), especially focussing on the protection of individual privacy and the ethical implications of psychological research through the Internet at large, more precisely:

1. The absence of a researcher and the resulting distance from the research subject.
2. Uncertainty regarding adequate informed consent and debriefing.
3. Potential loss of participant anonymity or confidentiality (Privacy).

In (Matwyshyn et al. 2010) the authors focus on the question of ethical implications regarding vulnerability research and argue that searching for and publishing of vulnerabilities in software (as well as hardware) products cannot be considered unethical or even illegal under most western legislations. Still, they discuss several aspects that should be taken into account in order to not cross the border towards conducting cybercrime.

Since many research facilities nowadays have IRBs/ERBs (internal/ethical review boards) in order to thwart attempts of illegal or unethical research conducted by their employees, the authors of (Buchanan et al. 2011) discuss borderline examples of research and how IRBs should approach such proposals. Based on this analysis, they propose a set of best practices for judging and dealing with these problems, including implications on education and training.

6.2 DISCLOSURE AND RESPONSIBLE DISCLOSURE

The discussion on whether and how to disclose security bugs has quite a long history until now, as has the notion on various ethical arguments that are very closely related.

In their work (Cencini et al. 2005) the author discuss different kinds of disclosure models, covering the whole range from full disclosure over responsible disclosure to no disclosure at all. While this work gives some valuable insights and arguments, it is, possibly due to the time of writing, not including any form of online service or system, but solely focussed on the offline world. Furthermore, the authors restrict themselves to Software only, which is too restricted in the current world of cheap and ubiquitous hardware. Furthermore, while this work covers also a taxonomy for the Software lifecycle including a timeline, this cannot be generalized to the modern world of online services and, even for products solely for local installations, ability to patch systems on a very frequent and performant basis. Paraphrasing previous work conducted in (Shepherd 2003) “responsible disclosure is a policy in which software vulnerabilities are disclosed in a manner that puts users at the least risk without stifling the security research community”. Based on this definition, the authors put forth arguments for and against each of these strategies, giving several strong points for the concept of responsible disclosure. Still, due to the age of the publication, the results must be seen with some care with respect to generalizations into nowadays online world.

In (Ransbotham and Mitra 2013) the authors discuss the impact of immediate disclosure on several key aspects of attack spread. Here the process of an attack is seen as a race between the attacker(s) and the defenders. According to their study, the immediate disclosure of a vulnerability reduces the delay in the attack diffusion process, but also results in an increased penetration of the attack with respect to the set of potential targets, as well as the volume of attacks carried out, all compared to responsible disclosure policies. While these results do point out some interesting dynamics, especially claiming that the danger of full disclosure makes vendors more aware of potential security threats, while responsible disclosure on the other hand allows vendors to stall fixes for a longer period of time, it is unclear on how this can be translated to real world environments, where not every attack will be fixed by the vendor, who is possible not even a commercial, but rather an academic or private institution. Based on this definition and rather strict definitions for full and non-disclosure strategies, they bring up models for simulation of attack spreads and expected damages.

In (McQueen et al. 2007) the authors discuss improvements to the patch process due to various timespans allowed as grace periods with respect to several established responsible disclosure mechanisms. More precisely, they study the effect of different grace periods for ZDI (Zero Day Initiative) and related projects like Rapid7 and the Google Security Team.

The authors of (Cavusoglu and Raghunathan 2007) discussed several different disclosure strategies proposed by different stakeholders in order to identify the optimal policy, utilizing social loss as metric for optimization. They state that they identified that responsible disclosure mechanisms actually ensured the release of patches for vulnerabilities best in their sample, still they claim that putting a timespan as grace period, after which the vulnerability will be disclosed even in case no patch no is available, gives no incentive to the vendor for developing patches and may even hinder the release. Still, this result needs further investigation. The authors also give a good overview on issues and research gaps regarding responsible disclosure with respect to the time of writing in (Cavusoglu and Raghunathan 2005). Some focus has also been put on the economics of various types of disclosure, e.g. (Bollinger2004) or (Böhme 2006).

6.3 LAWFUL INTERCEPTION

The term "Lawful Interception" usually describes means and methods demanded by governments to be able to monitor telecommunication networks and other means of (digital) communication. The fundamental principles and regulations differ from country to country due to different laws and legal frameworks. This especially includes the question like

- How long can the data be stored?
- Is the data stored in advance for everybody, or just in special cases?
- Is only metadata intercepted, or also content of the communication?

While being a rather political and controversial topic, interfaces for lawful interception have been known for being misuse by forces (criminal or from other states) that there were not intended for, e.g. during the Athens affair (Prevelakis and Spinellis, 2007) where an interface was modified in order to sniff on cellphones of high officials, without any legal background. While the affair was never cleared, the attackers possessed very detailed knowledge on the underlying technology, actually performing life hacking of MSCs in a working network. Attacks like these have been reported to be encountered again, without any traces of the actual attacker.

Also the fact itself that governments want to enforce backdoors into private communication is under heavy discussion, especially considering the recent affairs regarding secret services. One of the first debates in this respect took place in the nineties when the US government wanted to introduce Clipper (see Froomkin, 1995 and Froomkin, 1996).

7 DISCUSSION AND CONCLUSION

Our key work package objectives for this deliverable have been to examine the social, economic and legal landscape of cybercrime and cybersecurity. In doing this, we have sought to identify the roots of cybercrime and cyberterrorism, in terms of their economic and political motivations and we have aimed to contribute to the literature on the common habits of the modern societies that enable cyber attacks. Moreover, by adopting a robust and scientific approach, we have examined how the main cyber-threats can affect social, economic, political, and legal rights of citizens and stakeholders. A final output of a list of research topics which are important for the protection of social, economic, political, and legal rights of citizens and stakeholders is put forward.

Our thinking about cybercrime is embedded within a framework which holds that crime is not a self-evident and a unitary concept. It is historically and culturally situated and encapsulated within a social and political ideological framework. Importantly, it is subject to re-conceptualisation with social and technological changes in society and the status of individuals and groups. Although the theoretical and empirical literature into the criminology of cybercrime is still at an embryonic stage, it is evident that the domain of cybercrime is historically and culturally specific and subject to social, cultural, political and legal construction.

In our new digital society, cyber-space generates risks that require careful attention to ensuring security of individuals and groups and our social order (Beck 1992). Such security is multi-faced including the security that is embedded within our technical systems, within our ethical frameworks of privacy, trust and information sharing, and within our legal structures and processes. To help build such security, there is an important need to understand the problem of cybercrime. Here, an examination of cybrecrimes helps construct a better understanding of its nature and extent including potential targets and offenders.

Whilst the definition of cybercrime continues to be perceived as a conceptual and an analytical problem, there is some emerging agreement about a general taxonomy of cybercrime. A synthesis of categorisation put forward by some scholars suggests that cybercrimes are understood as occurring in three principal ways - namely, traditional crimes (for example, theft/fraud/forgery) that are contingent upon the use of technology; publication of illegal content on the internet (for example child pornography, hateful communication); and crimes that occur within technological forums (for example cyber attacks against communication/information networks including hacking, and denial of service). In any categorisation of cybercrime, it is important to understand the experiences of those at the receiving end of such crimes. Crucially, given that cybercrimes tend to be under-reported and under-recorded, it is essential to give recognition to different types of cybercrimes to assist individuals to come forward for appropriate help and assistance (Kshetri 2006, Fafinski 2010). Additionally, it is vital to understand the nature and extent of cybercrime activity to help formulate appropriate measures to prevent and tackle this phenomenon.

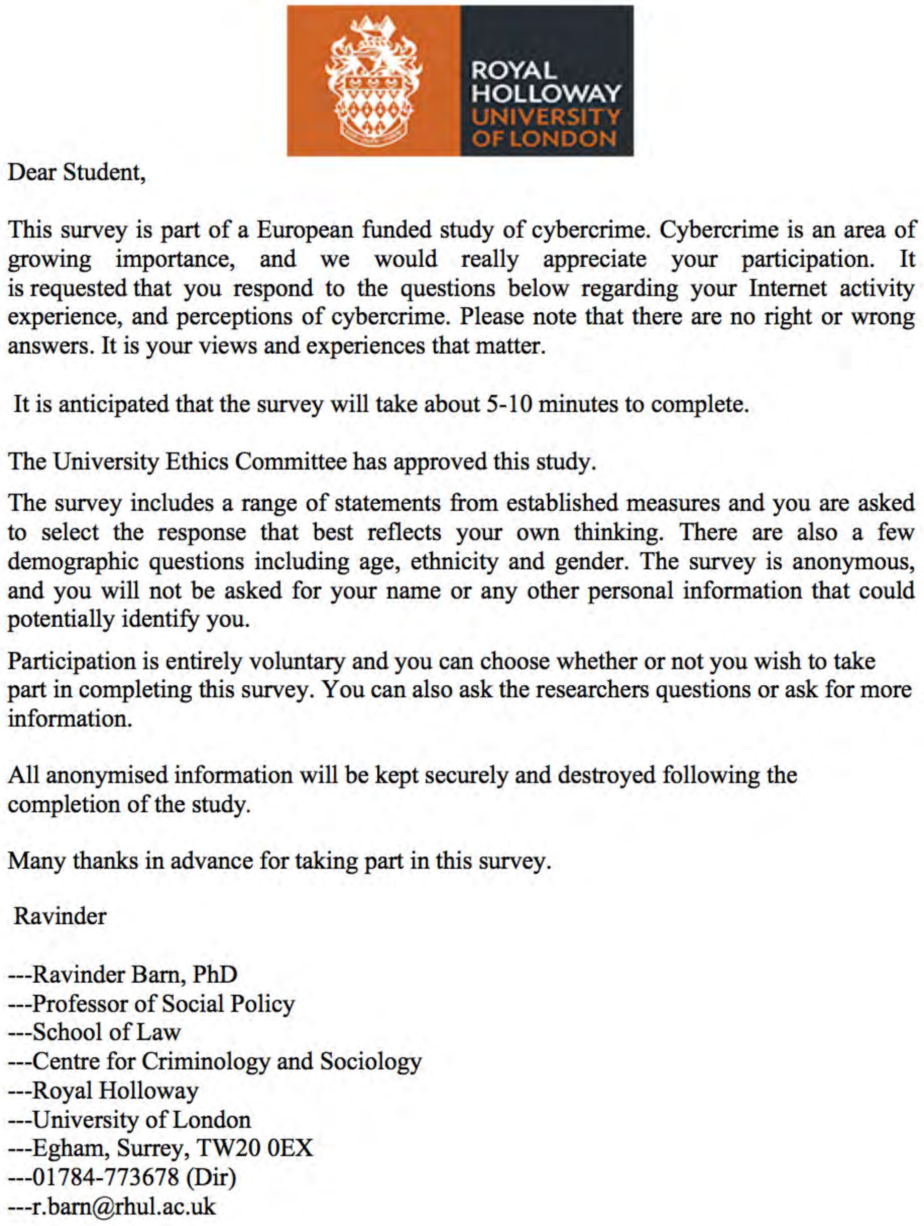
In a climate where there is a lack of 'reliable' official data into cybercrime, a 'culture of fear' can emerge about the perceived risk of such activity (Furedi 2006). Arguably, if the main sources of the nature and extent of cybercrime remain the media, politicians/policy-makers, and security companies, this can lead to heightened public anxiety. Our survey findings show that whilst reported victimisation experiences were relatively low, some groups of respondents (namely women, and some ethnic groups) expressed greater fear of cybercrime. Whilst further research is needed to explore this situation, it is important to point out that alongside improved technical cyber security, clear public information is vital to help dispel fear and/or complacency.

An engagement with criminological theory can also help promote understanding and guide policy, practice and provision to ameliorate cybercrime activity and its negative impact on users. Here, both sociological and psychological literature may serve to enhance criminological insights. An identification of key factors that may lead to offending behavior as well as interventions that may raise education and awareness among users at risk of victimization is of paramount importance. Competing theoretical approaches that point to socio-economic disparities (for example 419 and other online financial scams), individual 'rational' motivations (for example, political, social, sexual), and absence of suitable technological/legal enforcement are all important in developing a composite picture of the nature and prevalence of cybercrime. Indeed, a range of strategies and interventions would be needed to tackle the complexity of cybercrime.

In this deliverable we have brought together the different conceptualisations that we have found in the social science literatures reviewed and abstracted the different elements found in each conceptualisation. We have operationalised these elements and characteristics into a taxonomy that can be utilised to derive a social science explanation of cybercrime. This taxonomic structure allows the representation of a cybercrime from both the perspective of the victim and the perpetrator. Within this taxonomy, we can see that cyberterrorism is a form of cybercrime. At the geopolitical level, our literature review indicates that there is a range of emerging research issues related to the governance of cybercrime, mainly relating to a) the definition, focus and costs related to cybercrime, b) the reasons for convergence and divergence in regulating and governing cybercrime, c) increasing exchange with non-state actors and d) the development of legal and other normative perspectives on cybercrime.

In this deliverable we have also considered the socio-economic aspects of cybercrime and our analysis shows that there are gaps both in the availability of data upon which to make a socio-economic calculation and in the understanding of how derive socio-economic measures. In areas that are contested such as this, standards and baselines are often used as an initial means to provide a common start point for implementing a generally start point for an evaluation or calculation. This is reflected in the manner in which legal instruments use standards to operationalise the legal principles. When considering the ethical aspects of increased research in the area of cybercrime and the ability to obtain more accurate data, perhaps standards and baselines are needed in this aspect too.

ANNEX A: VICTIMISATION SURVEY



ROYAL HOLLOWAY UNIVERSITY OF LONDON

Dear Student,

This survey is part of a European funded study of cybercrime. Cybercrime is an area of growing importance, and we would really appreciate your participation. It is requested that you respond to the questions below regarding your Internet activity experience, and perceptions of cybercrime. Please note that there are no right or wrong answers. It is your views and experiences that matter.

It is anticipated that the survey will take about 5-10 minutes to complete.

The University Ethics Committee has approved this study.

The survey includes a range of statements from established measures and you are asked to select the response that best reflects your own thinking. There are also a few demographic questions including age, ethnicity and gender. The survey is anonymous, and you will not be asked for your name or any other personal information that could potentially identify you.

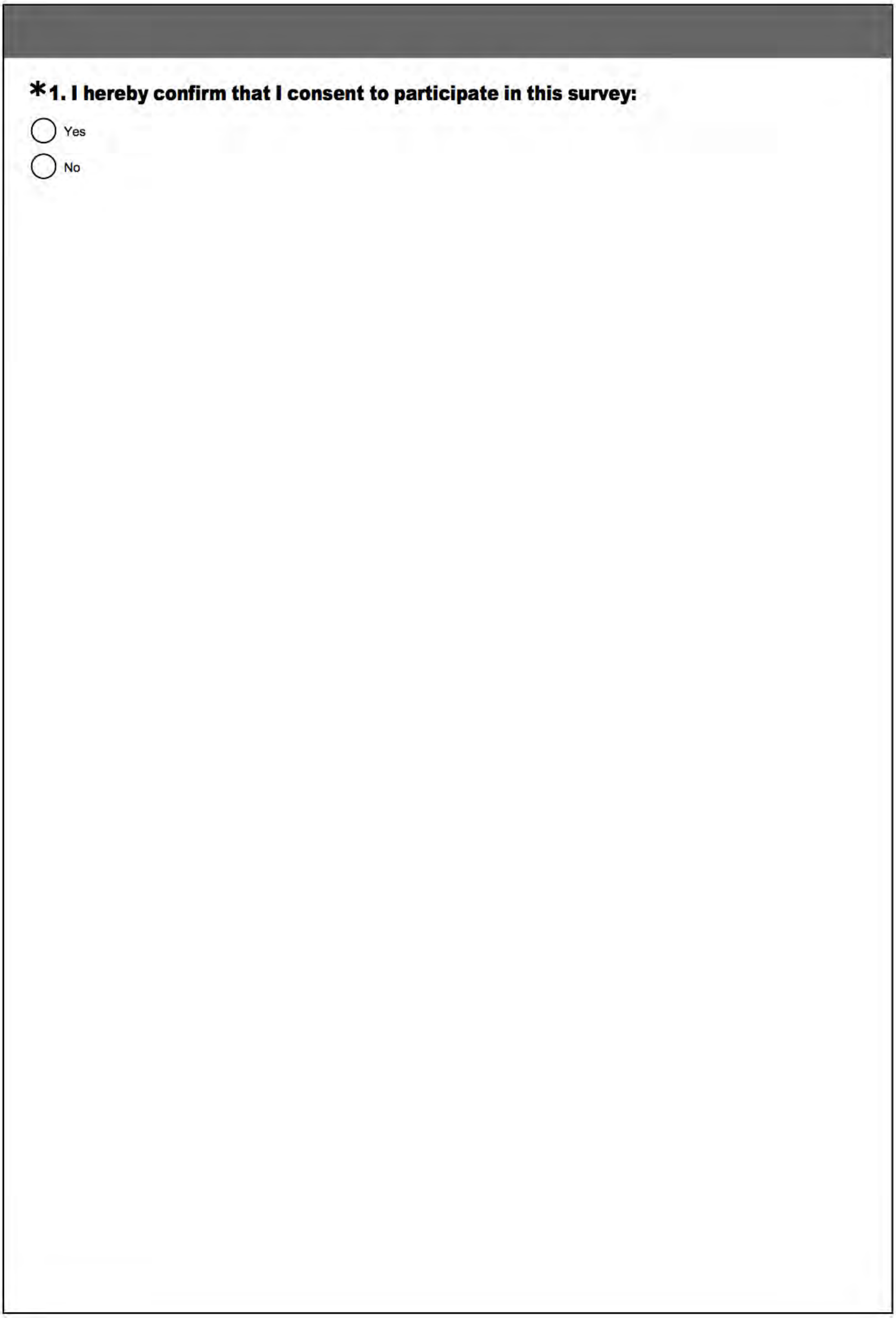
Participation is entirely voluntary and you can choose whether or not you wish to take part in completing this survey. You can also ask the researchers questions or ask for more information.

All anonymised information will be kept securely and destroyed following the completion of the study.

Many thanks in advance for taking part in this survey.

Ravinder

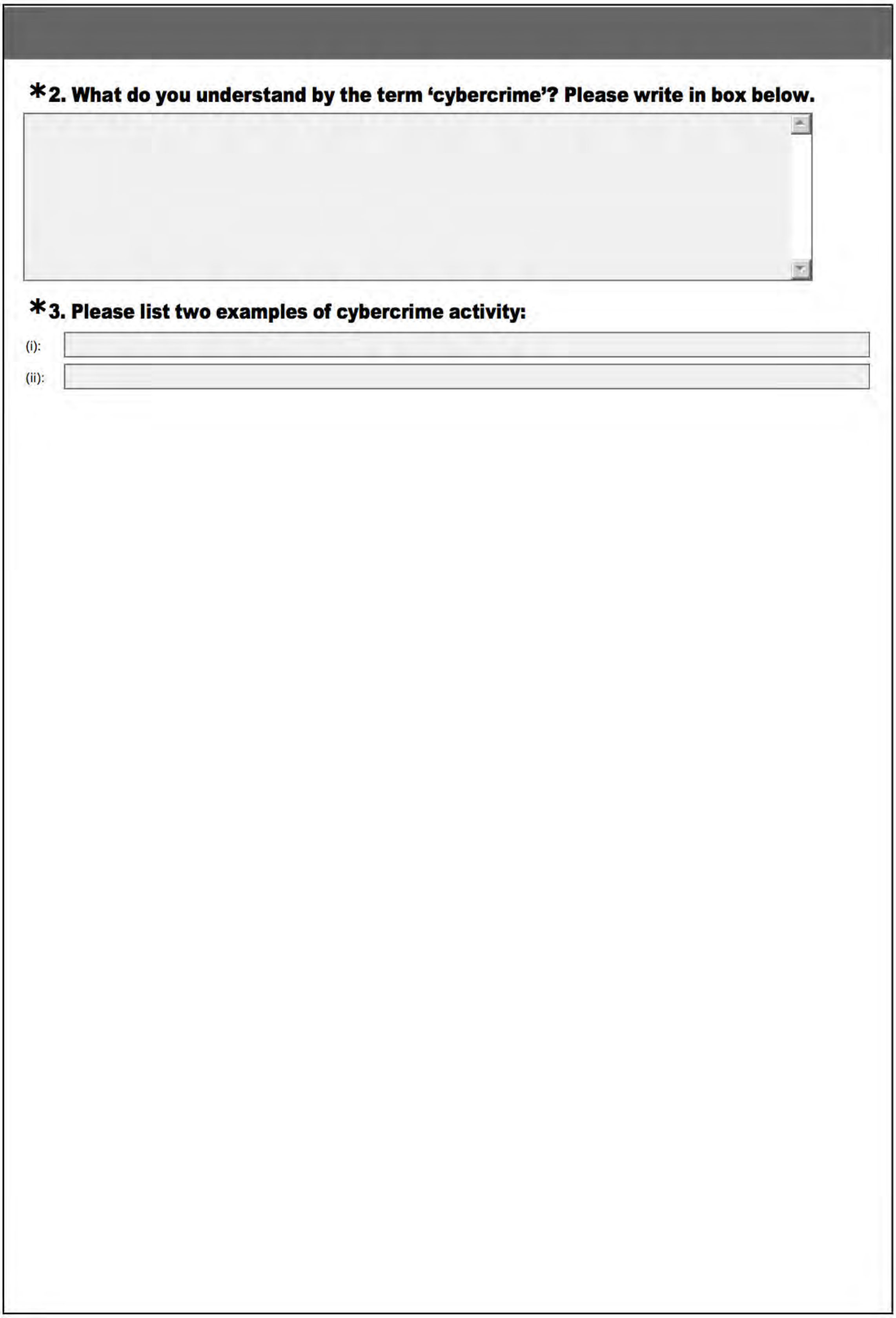
---Ravinder Barn, PhD
---Professor of Social Policy
---School of Law
---Centre for Criminology and Sociology
---Royal Holloway
---University of London
---Egham, Surrey, TW20 0EX
---01784-773678 (Dir)
---r.barn@rhul.ac.uk



*1. I hereby confirm that I consent to participate in this survey:

○ Yes

○ No

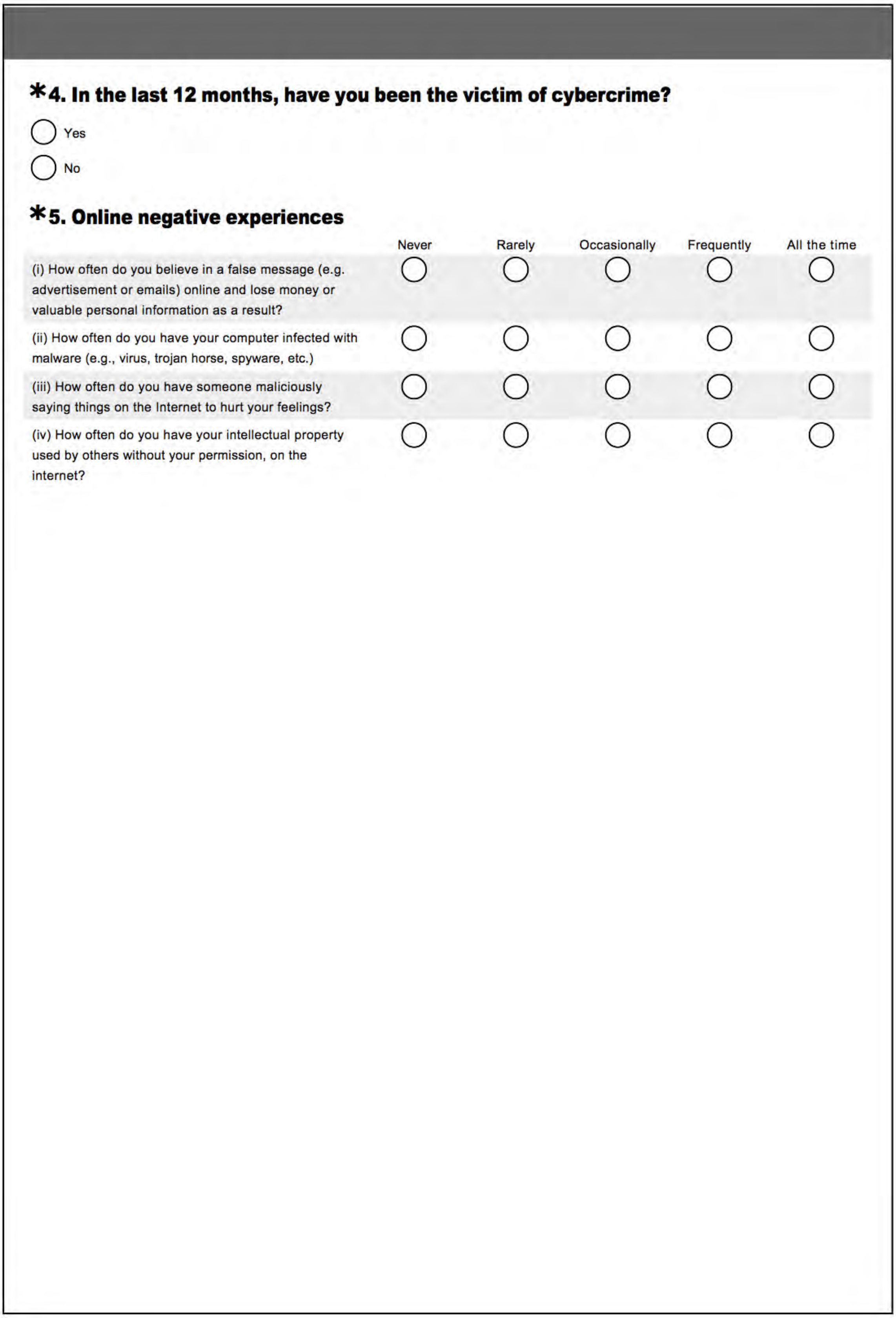


***2. What do you understand by the term ‘cybercrime’? Please write in box below.**

***3. Please list two examples of cybercrime activity:**

(i):

(ii):



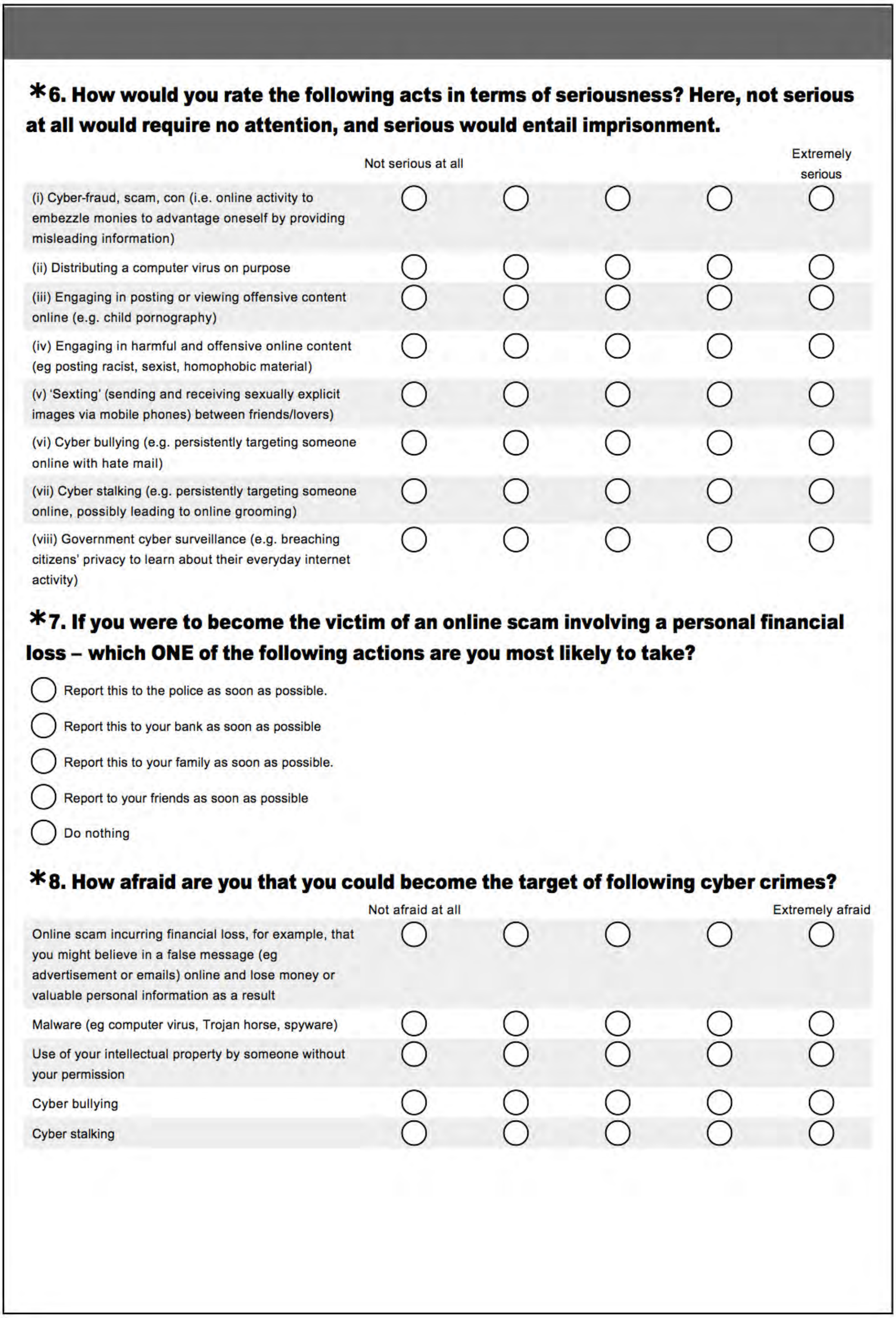
***4. In the last 12 months, have you been the victim of cybercrime?**

○ Yes

○ No

***5. Online negative experiences**

	Never	Rarely	Occasionally	Frequently	All the time
(i) How often do you believe in a false message (e.g. advertisement or emails) online and lose money or valuable personal information as a result?	○	○	○	○	○
(ii) How often do you have your computer infected with malware (e.g., virus, trojan horse, spyware, etc.)	○	○	○	○	○
(iii) How often do you have someone maliciously saying things on the Internet to hurt your feelings?	○	○	○	○	○
(iv) How often do you have your intellectual property used by others without your permission, on the internet?	○	○	○	○	○



***6. How would you rate the following acts in terms of seriousness? Here, not serious at all would require no attention, and serious would entail imprisonment.**

	Not serious at all				Extremely serious
(i) Cyber-fraud, scam, con (i.e. online activity to embezzle monies to advantage oneself by providing misleading information)	○	○	○	○	○
(ii) Distributing a computer virus on purpose	○	○	○	○	○
(iii) Engaging in posting or viewing offensive content online (e.g. child pornography)	○	○	○	○	○
(iv) Engaging in harmful and offensive online content (eg posting racist, sexist, homophobic material)	○	○	○	○	○
(v) 'Sexting' (sending and receiving sexually explicit images via mobile phones) between friends/lovers)	○	○	○	○	○
(vi) Cyber bullying (e.g. persistently targeting someone online with hate mail)	○	○	○	○	○
(vii) Cyber stalking (e.g. persistently targeting someone online, possibly leading to online grooming)	○	○	○	○	○
(viii) Government cyber surveillance (e.g. breaching citizens' privacy to learn about their everyday internet activity)	○	○	○	○	○

***7. If you were to become the victim of an online scam involving a personal financial loss – which ONE of the following actions are you most likely to take?**

○ Report this to the police as soon as possible.

○ Report this to your bank as soon as possible

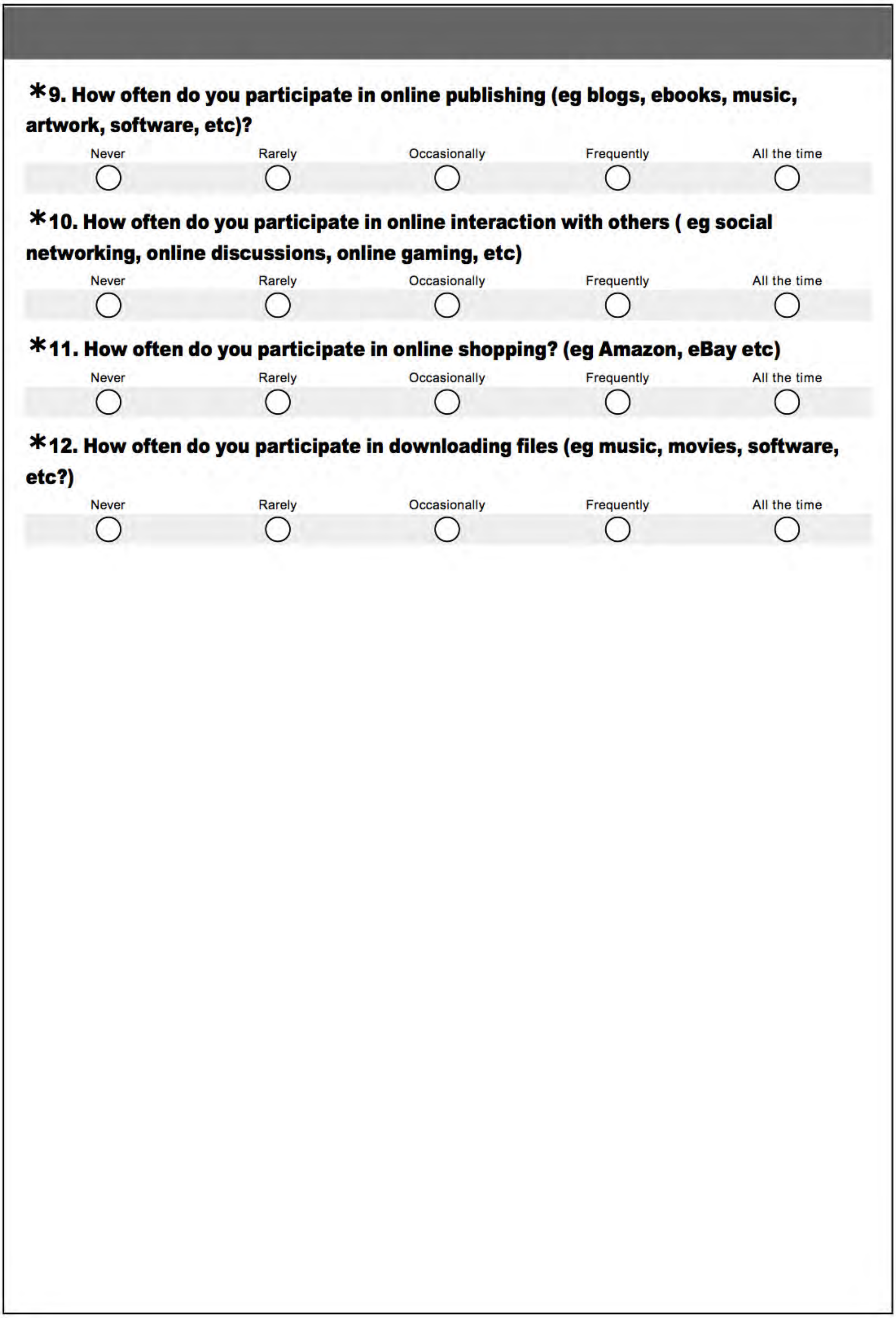
○ Report this to your family as soon as possible.

○ Report to your friends as soon as possible

○ Do nothing

***8. How afraid are you that you could become the target of following cyber crimes?**

	Not afraid at all				Extremely afraid
Online scam incurring financial loss, for example, that you might believe in a false message (eg advertisement or emails) online and lose money or valuable personal information as a result	○	○	○	○	○
Malware (eg computer virus, Trojan horse, spyware)	○	○	○	○	○
Use of your intellectual property by someone without your permission	○	○	○	○	○
Cyber bullying	○	○	○	○	○
Cyber stalking	○	○	○	○	○



***9. How often do you participate in online publishing (eg blogs, ebooks, music, artwork, software, etc)?**

Never	Rarely	Occasionally	Frequently	All the time
○	○	○	○	○

***10. How often do you participate in online interaction with others (eg social networking, online discussions, online gaming, etc)**

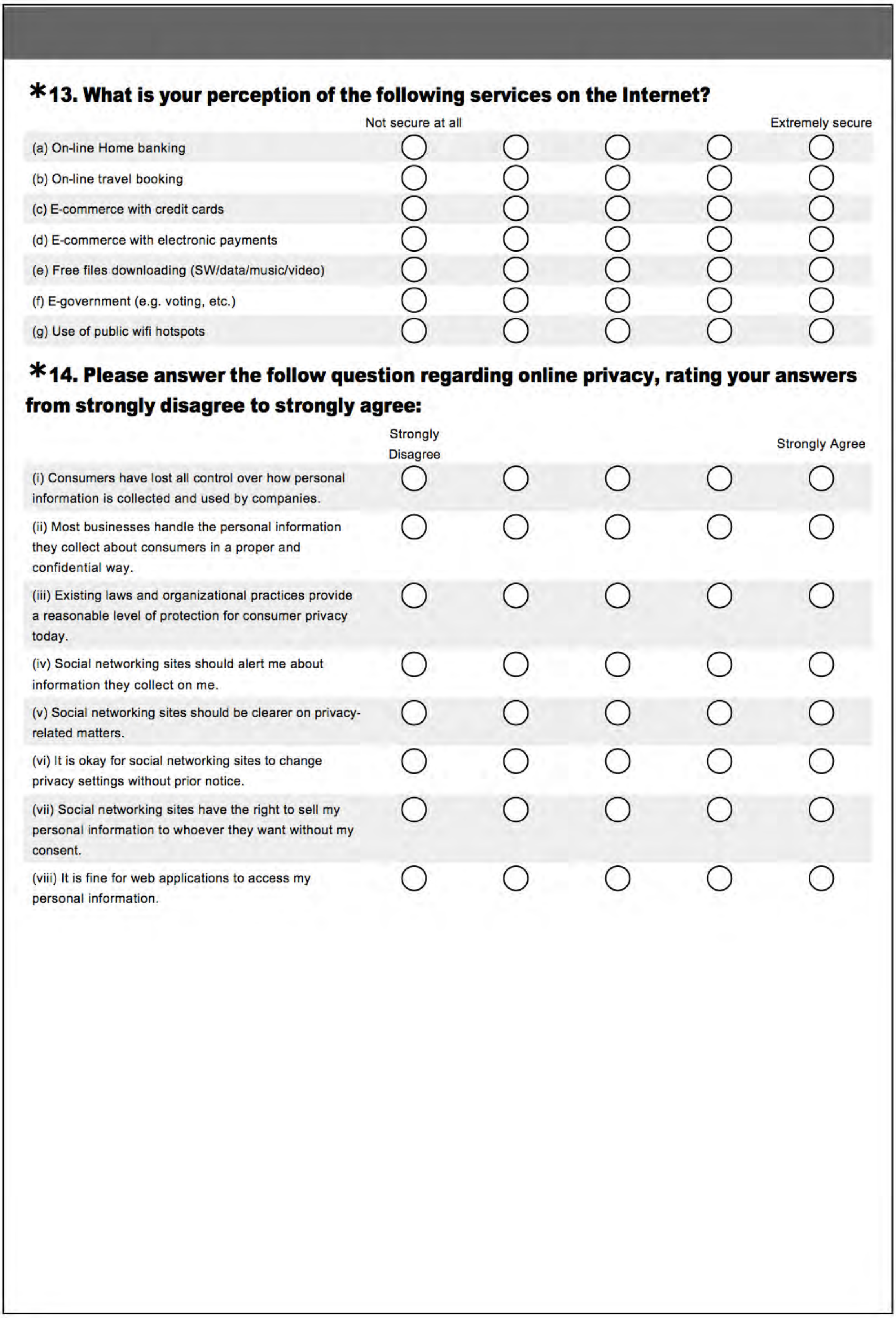
Never	Rarely	Occasionally	Frequently	All the time
○	○	○	○	○

***11. How often do you participate in online shopping? (eg Amazon, eBay etc)**

Never	Rarely	Occasionally	Frequently	All the time
○	○	○	○	○

***12. How often do you participate in downloading files (eg music, movies, software, etc?)**

Never	Rarely	Occasionally	Frequently	All the time
○	○	○	○	○

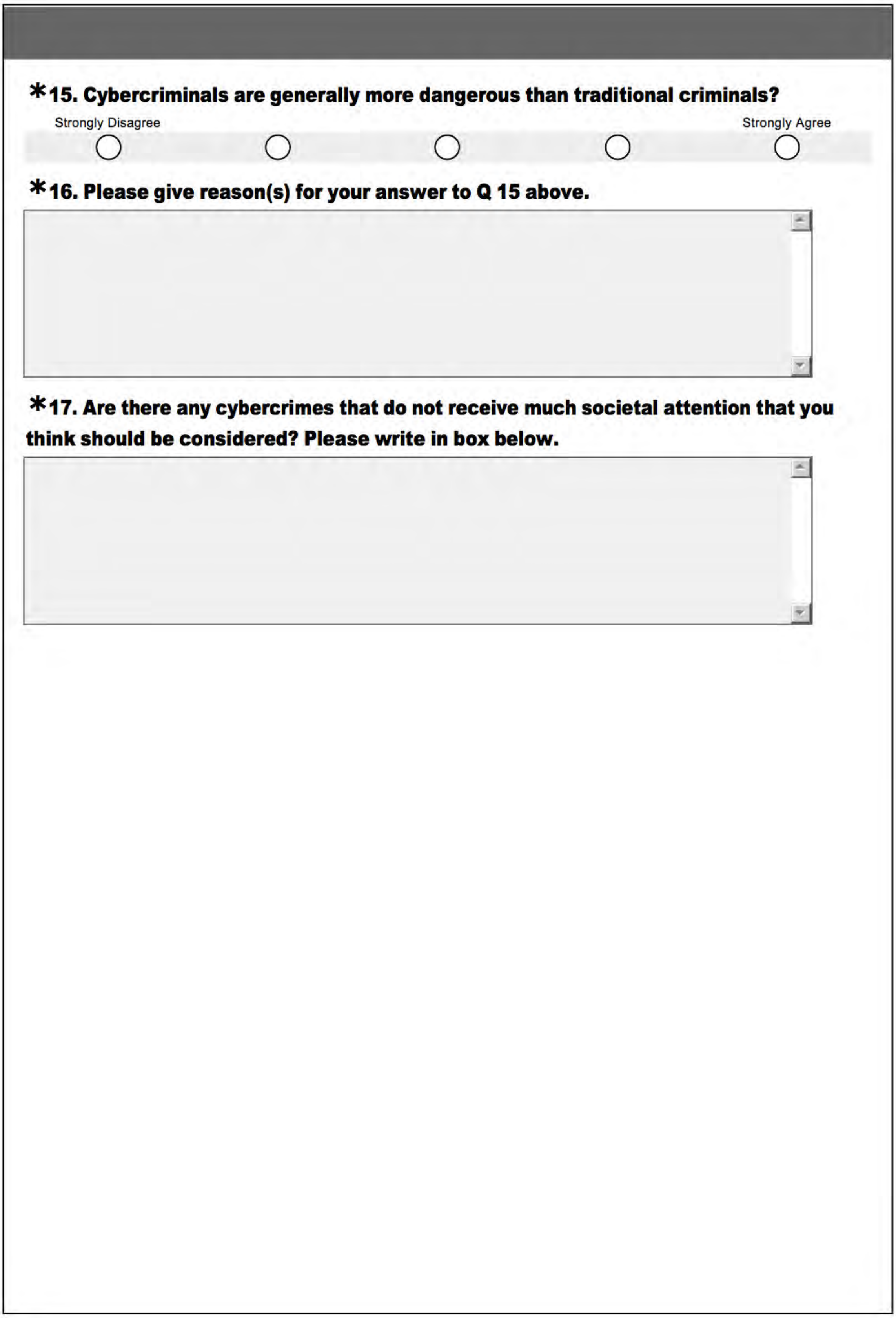


***13. What is your perception of the following services on the Internet?**

	Not secure at all				Extremely secure
(a) On-line Home banking	○	○	○	○	○
(b) On-line travel booking	○	○	○	○	○
(c) E-commerce with credit cards	○	○	○	○	○
(d) E-commerce with electronic payments	○	○	○	○	○
(e) Free files downloading (SW/data/music/video)	○	○	○	○	○
(f) E-government (e.g. voting, etc.)	○	○	○	○	○
(g) Use of public wifi hotspots	○	○	○	○	○

***14. Please answer the follow question regarding online privacy, rating your answers from strongly disagree to strongly agree:**

	Strongly Disagree				Strongly Agree
(i) Consumers have lost all control over how personal information is collected and used by companies.	○	○	○	○	○
(ii) Most businesses handle the personal information they collect about consumers in a proper and confidential way.	○	○	○	○	○
(iii) Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	○	○	○	○	○
(iv) Social networking sites should alert me about information they collect on me.	○	○	○	○	○
(v) Social networking sites should be clearer on privacy-related matters.	○	○	○	○	○
(vi) It is okay for social networking sites to change privacy settings without prior notice.	○	○	○	○	○
(vii) Social networking sites have the right to sell my personal information to whoever they want without my consent.	○	○	○	○	○
(viii) It is fine for web applications to access my personal information.	○	○	○	○	○

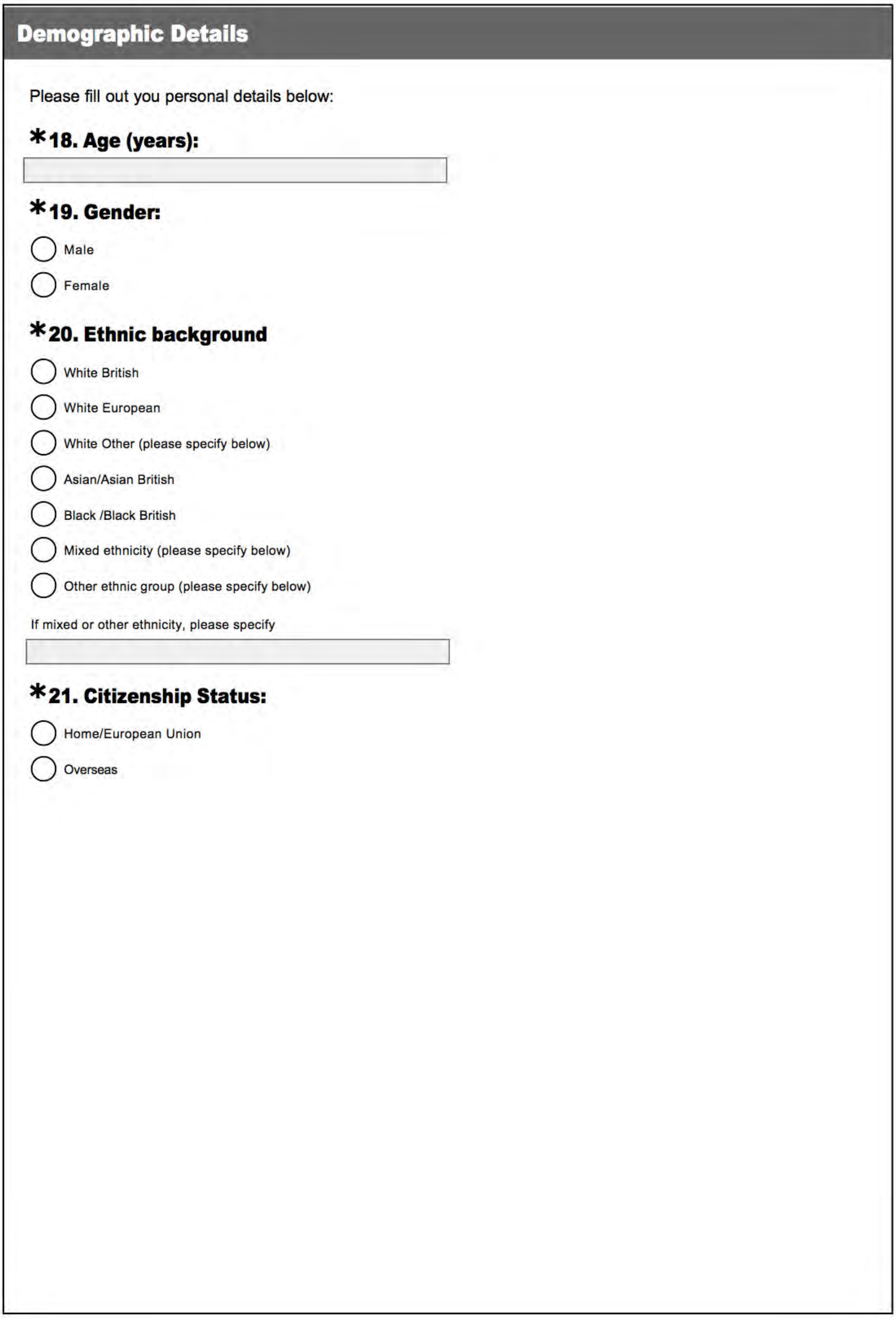


*15. Cybercriminals are generally more dangerous than traditional criminals?

Strongly Disagree ○ ○ ○ ○ ○ Strongly Agree

*16. Please give reason(s) for your answer to Q 15 above.

*17. Are there any cybercrimes that do not receive much societal attention that you think should be considered? Please write in box below.



Demographic Details

Please fill out you personal details below:

***18. Age (years):**

***19. Gender:**

○ Male

○ Female

***20. Ethnic background**

○ White British

○ White European

○ White Other (please specify below)

○ Asian/Asian British

○ Black /Black British

○ Mixed ethnicity (please specify below)

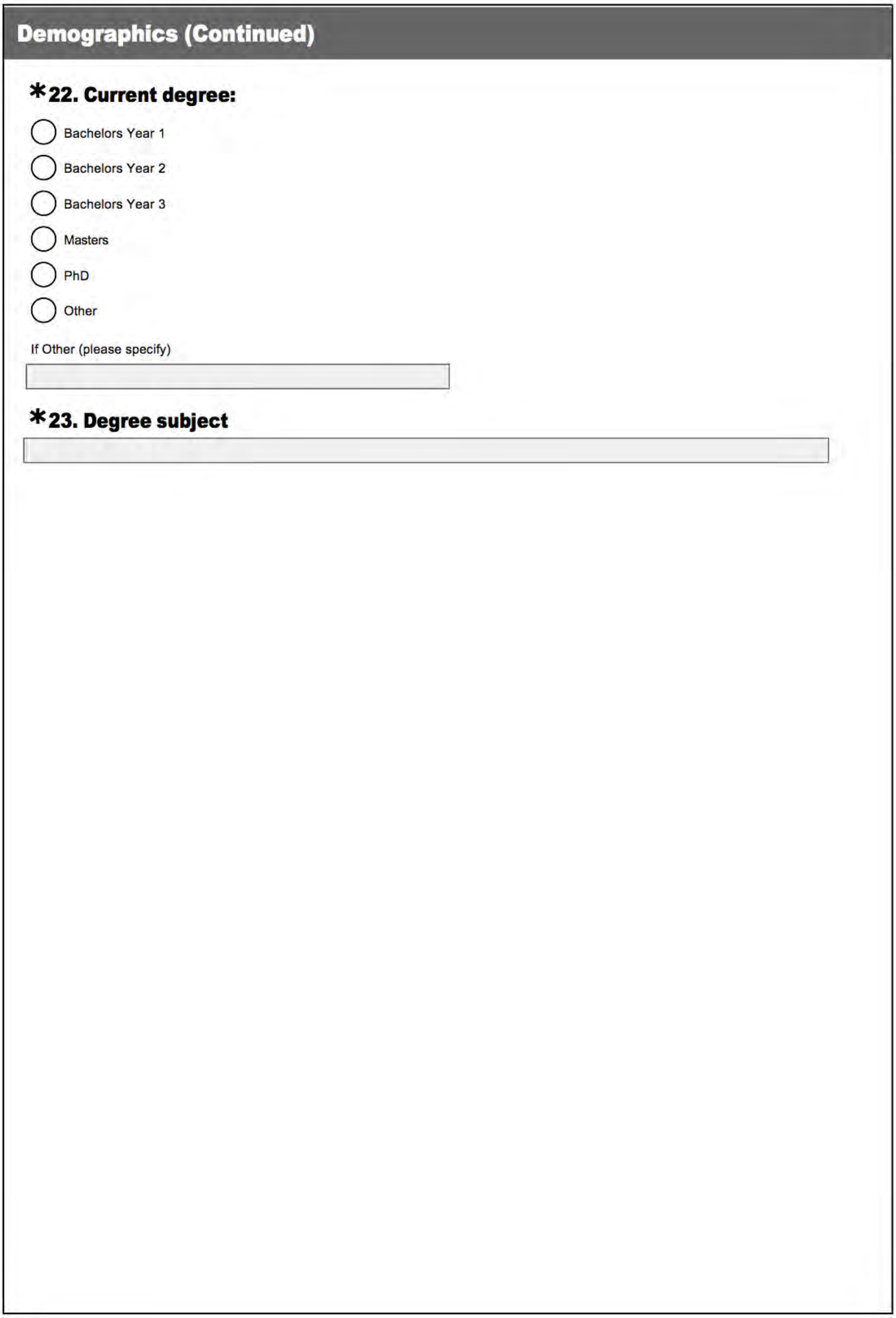
○ Other ethnic group (please specify below)

If mixed or other ethnicity, please specify

***21. Citizenship Status:**

○ Home/European Union

○ Overseas



Demographics (Continued)

***22. Current degree:**

○ Bachelors Year 1

○ Bachelors Year 2

○ Bachelors Year 3

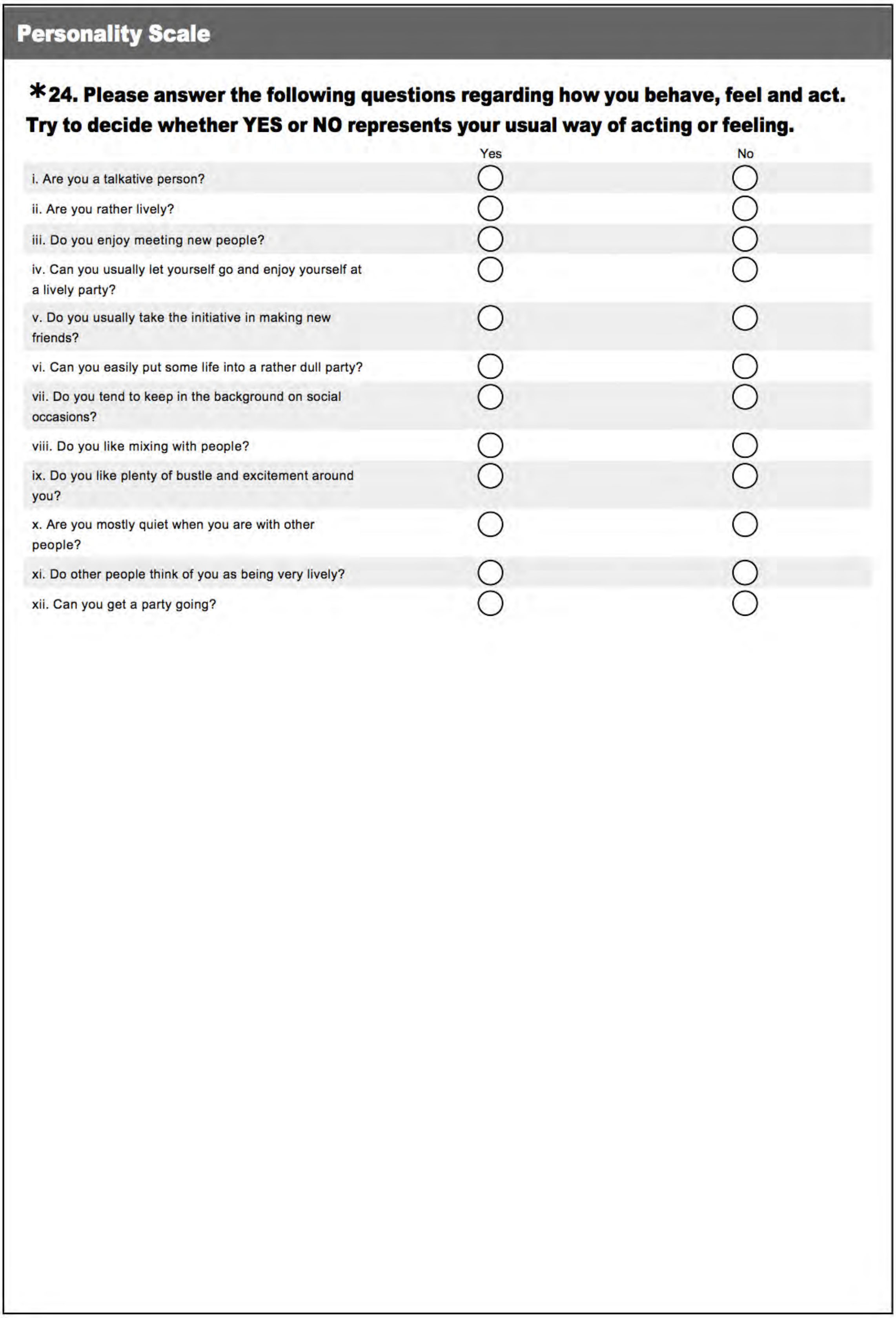
○ Masters

○ PhD

○ Other

If Other (please specify)

***23. Degree subject**



Personality Scale

***24. Please answer the following questions regarding how you behave, feel and act. Try to decide whether YES or NO represents your usual way of acting or feeling.**

	Yes	No
i. Are you a talkative person?	○	○
ii. Are you rather lively?	○	○
iii. Do you enjoy meeting new people?	○	○
iv. Can you usually let yourself go and enjoy yourself at a lively party?	○	○
v. Do you usually take the initiative in making new friends?	○	○
vi. Can you easily put some life into a rather dull party?	○	○
vii. Do you tend to keep in the background on social occasions?	○	○
viii. Do you like mixing with people?	○	○
ix. Do you like plenty of bustle and excitement around you?	○	○
x. Are you mostly quiet when you are with other people?	○	○
xi. Do other people think of you as being very lively?	○	○
xii. Can you get a party going?	○	○

Adams, A, and Sasse. M.A., "Users are not the enemy." Communications of the ACM 42.12 (1999): 40-46.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J. G., Levi, M., Moore, T. & Savage, S. 2013. Measuring the Cost of Cybercrime. In: Böhme , R. (ed.) The Economics of Information Security and Privacy. Heidelberg: Springer.

Andreas, P. & Greenhill, K. M. 2010. Introduction: The Politics of Numbers. In: Andreas, P. & Greenhill, K. M. (eds.) Sex, Drugs, and Body Counts. The Politics of Numbers in Crime and Conflict. Ithaka: Cornell University Press.

Archick, K. 2006. Cybercrime. The Council of Europe Convention. CRC Report for Congress. Version updated September 28, 2006, Washington, Congressional Research Service.

Ashford, C. (2008). Sex work in cyberspace: who pays the price?. Information & Communications Technology Law, 17(1), 37-49.

Axelrod, R., & Ostrom's, E. (2010, June). Governing the cyber commons. In Review Symposium: Beyond the Tragedy of the Commons.

Barnard-Wills, D., and Ashenden, D.M.. 2010. Public sector engagement with online identity management. Iden- tity in the Information Society, pages 1–18.

Barrinha, A. & Carrapico, H. 2014. The EU's emerging security actorness in cyber space and its proclamation implementation gap. Paper presented at the ECPR General Meeting 2014, Glasgow, September.

Bauman, S., & Bellmore, A. (2015). New Directions in Cyberbullying Research. Journal of School Violence, 14(1), 1-10.

BBC 2014. Top EU court rejects EU-wide data retention law (8 April 2014) Online at http://www.bbc.co.uk/news/world-europe-26935096, last access on January 1, 2015.

Beck., U. (1992) Risk society: Towards a new modernity (Vol. 17). Sage.

Benson, V., Saridakis, G., & Tennakoon, H. (2014). Purpose of social networking use and victimisation: are there any differences between university students and those not in HE?. Computers in Human Behavior,

Blackman, S. (2005) Youth subcultural theory: A critical engagement with the concept, its origins and politics, from the Chicago school to postmodernism. Journal of youth studies, 8(1), 1-20.

Boehm, J., Lyubomirsky, S., and Sheldon, K. (2011) A longitudinal experimental study comparing the effectiveness of happiness-enhancing strategies in Anglo Americans and Asian Americans. Cognition and Emotion, 25, p. 1152-1167.

Bollinger, J. (2004). Economies of disclosure. ACM SIGCAS Computers and Society, 34(3), 1-1.

Boni, B. (2001). The Threat of Cyber-Sabotage: The new Internet economy has recently seen a spate of layoffs. E-business' had better watch out for their ex-technical employees—and guard against the potentially crippling effects of cyber-sabotage. Network Security, 2001(3), 18-19.

Bonneau J., & Preibusch, S., "The privacy jungle: On the market for data protection in social networks", Economics of Information Security and Privacy, pp. 121-167, 2010.

Bourdieu, P. (1984) Distinction: A Social of the Judgements of Taste. London: Routledge.

Brenner, S. W. (2001) Is There Such a Thing as "Virtual Crime"?. Berkeley Journal of Criminal Law, 4, 1, p. 1-72.

Brinson, A., Robinson, A., & Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. digital investigation, 3, 37-43.

Broadhurst, R., Grabosky, P., Alazab, M., and Chon, S. (2014) Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in CyberCrime. International Journal of Cyber Criminology, 8, 1, p.1-20.

Broadhurst, R. (2006) Developments in the global law enforcement of cybercrime. Policing: An International Journal of Police Strategies & Management, 29, 3, p. 408-433.

Bryant, F. (2003) Savouring Belief Inventory (SBI): A scale for measuring beliefs about savouring. Journal of Mental Health, 12,p.175-196

Bravo, R. (2011 йил November). Do espectro de conflitualidade nas redes de informação : por uma reconstrução conceptual do terrorismo no ciberespaço. (A. /. PJ, Ed.) REVISTA DE INVESTIGAÇÃO CRIMINAL - N.º 2 .

Buchanan, E., Aycock, J., Dexter, S., Dittrich, D., & Hvizdak, E. (2011). Computer science security research and human subjects: Emerging considerations for research ethics boards. Journal of Empirical Research on Human Research Ethics, 6(2), 71-83.

Buchanan, T., Reips, U-D., Paine C and Joinson, A.N., "Development of measures of on-line privacy concern and protection for use on the Internet." Journal of the American Society for Information Science and Technology, Vol. 58, Issue 2, pp. 157 – 165, 2007.

Böhme, R. (2006). A comparison of market approaches to software vulnerability disclosure. In Emerging Trends in Information and Communication Security (pp. 298-311). Springer Berlin Heidelberg.

Böhme , R., & Moore, T. (2012). How do consumers react to cybercrime?. In eCrime Researchers Summit (eCrime), 2012 (pp. 1-12). IEEE.

Calderoni, F. 2010. The European Legal Framework on Cybercrime: Striving for an Effective Implementation. Crime, Law and Social Change, 54, 339-357.

Cas, J. (2005). Privacy in pervasive computing environments-a contradiction in terms?. Technology and Society Magazine, IEEE, 24(1), 24-33.

Castronova, J. R. (2006). Operation Cyber Chase and Other Agency Efforts to Control Internet Drug Trafficking The “Virtual” Enforcement Initiative Is Virtually Useless. The Journal of legal medicine, 27(2), 207-224.

Cavoukian, A 2009. Privacy by Design: The answer to overcoming negative externalities arising from poor management of personal data. A presentation to the Trust Economics Workshop, London, England, 2009, (Available from: http://www.ipc.on.ca/images/Resources/2009-06-23-TrustEconomics.pdf)

Cavusoglu, H., & Raghunathan, S. (2007). Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. Software Engineering, IEEE Transactions on, 33(3), 171-185.

Cavusoglu, H., & Raghunathan, S. (2005, June). Emerging Issues in Responsible Vulnerability Disclosure. In WEIS.

Cencini, A., Yu, K., & Chan, T. (2005). Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure.

Chadwick, A. 2003. Bringing e-democracy back in - Why it matters for future research on e-governance. Social Science Computer Review, 21, 443-455.

Chadwick, A. & May, C. 2003. Interaction between states and citizens in the age of the internet: "e-government" in the United States, Britain, and the European Union. Governance-an International Journal of Policy and Administration, 16, 271-300.

Chen, Y. C., Chen, P., Song, R., & Korba, L. (2004). Online gaming crime and security issue-cases and countermeasures from taiwan.

Choucri, N., Madnick, S. & Ferweda, J. 2014. Institutions for Cybersecurity: International Responses and Global Imperatives. Information Technoology for Development, 20, 96-121.

Cloward, R. and Ohlin, L. (1960) Delinquency and Opportunity: A theory of Delinquent Gangs. New York: Free Press.

Cohen, A. (1955) Delinquency Boys: The Culture of the Gang: New York: Free Press.

Cohen, S. 1971, 1980 (2002). Folk devils and moral panics: The creation of the mods and rockers, 3rd edition, London: Routledge.

Cohen, L.E., and Felson, M. (1979) "Social change and crime rate trends: A routine activity approach." American sociological review.

Coleman, G. (2010) The hacker conference: A ritual condensation and celebration of a lifeworld. Anthropological Quarterly, 83(1), 47-72. Cornwell

Couch, D., & Liamputtong, P. (2008). Online dating and mating: The use of the internet to meet sexual partners. Qualitative Health Research, 18(2), 268-279.

Council Of Europe 2001. Convention on Cybercrime. Explanatory Report. Online at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, last access in July 2011.

Council Of Europe 2004. Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Online at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=&CL=ENG, last access in July 2011.

Council Of Europe 2011. Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Chart of Signatures and Ratifications. Online at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG, last access in July 2011.

Council Of Europe 2015. Convention on Cybercrime. Status as of 1/1/2015. Online at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, last access on 1 January 2015.

Crawford, Heather, and Renaud. K., "Understanding User Perceptions of Transparent Authentication on a Mobile Device." Journal of Trust Management 1.1 (2014): 7.

Csikszentmihalyi, M. (1990) Flow: The Psychology of Optimal Experience. New York: Harper and Collins.

Csikszentmihalyi, M. (2000) Beyond Boredom and Anxiety: Experiencing Flow in Work and Play, 2nd ed. San Francisco: Jossey Bass.

Daase, C. 2002. Internationale Risikopolitik. Ein Forschungsprogramm für den sicherheitspolitischen Paradigmenwechsel. In: DAASE, C., FESKE, S. & PETERS, I. (eds.) Internationale Risikopolitik. Der Umgang mit neuen Herausforderungen in den internationalen Beziehungen. Baden-Baden: Nomos.

Deci, E.L. and Ryan, R. M. (2000) The 'what' and 'why' of goal pursuits: human needs and the self-determination of behaviour. Psychological Inquiry, 11(4) p. 227-268.

Deci, E.L. and Ryan, R. M. (1985) Intrinsic Motivations and Self-determination in Human Behaviour. New York: Plenum.

DIE ZEIT 2014. Gerichtshof kippt Richtlinie zur Vorratsdatenspeicherung (8 April 2014). Online at http://www.zeit.de/digital/datenschutz/2014-04/vorratsdatenspeicherung-europaeischer-gerichtshof-eugh, last access on January 3, 2015.

Detica, (2011). The Cost of Cybercrime. [online] Cabinet Office. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Djelic, M-L. and K. Sahlin-Anderson (eds) (2006) Transnational Governance. Institutional Dynamics in Regulation. Cambridge: Cambridge University Press.

Döring, N. (2002). Personal home pages on the Web: A review of research. Journal of Computer-Mediated Communication, 7(3), 0-0.

Dowd, M. “Contextualised Concerns: The Online Privacy Attitudes of Young Adults”, Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology, 2011, pp. 78-79

Dourish, P Grinter, B., Delgado de la Flor,I, Joseph, M.,.: Security in the wild: user strategies for managing security as an everyday, practical problem, PUC (2004)

Durkheim, E. (1965 - original 1885) The Rules of Sociological Method. New York: The Free Press.

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

Ebenezer, J. A., & Elizabeth, O. I. (2014). Cyber Risks and Fraud in the Nigeria’s Business Environment: A Postmortem of Youth Crime. Journal of Social and Development Sciences, 5(4), 258-265.

European Commission (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (full text available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML)

European Commission (2000) EU Charter of Fundamental Rights (full text available from: http://www.europarl.europa.eu/charter/pdf/text_en.pdf)

European Commission (2001) Regulation (EC) no 45/2001 of the European Parliament and of the Council (full text available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF)

European Commission (2002) Data Protection in the Electronic Communications Sector (full text a available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML)

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

European Commission 2006. Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. Online http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=DE, last access on January 1, 2015.

Eurostat (2011) “Information society statistics,” http://epp.eurostat.ec.europa. eu/statistics explained/index.php/Information society statistics, 2011.

FBI, (2015). Uniform Crime Reporting. [online] Available at: http://www.fbi.gov/about-us/cjis/ucr/ucr

Fafinski, S., Dutton, W. H., & Margetts, H. Z. (2010). Mapping and measuring cybercrime.

Farrell, G. (2010) Situational crime prevention and its discontents: rational choice and harm reduction versus ‘cultural criminology’. Social Policy & Administration, 44, 1, p. 40-66.

Fearther, N. (1981) Expectations and Actions: Expectancy-value Models in Psychology. Abingdon: Lawrence Erlbaum Associates Inc.

Ferkiss, V. C. 1973. Review: Man's Tools and Man's Choices: The Confrontation of Technology and Political Science. The American Political Science Review, 67, 973-980.

Fette, G. Hsieh, M. Prabaker, J. Rao, K. Tang, K. Vaniea, L. Bauer, L. Cranor & J. Hong (2007), "User-controllable security and privacy for pervasive computing", Mobile Computing Systems and Applications, 2007. HotMobile 2007. Eighth IEEE Workshop, pp. 14.

Finn R.L, Wright, D., Friedewald, M., (2013) “European Data Protection: Coming of Age”, Section “Privacy by Design”, Springer Science + Business Media,

Florêncio, D., Herley, C., and Coskun. B., "Do strong web passwords accomplish anything?." HotSec 7 (2007): 6.

Floridi, L. (2005). Is semantic information meaningful data?. Philosophy and Phenomenological Research, 70(2), 351-370.

Foucault, M. (1977) Discipline and punish: The birth of the prison, Random House LLC.

Frankl, V. (1965) The Doctor and the Soul. New York: Bantam Books.

Fredrickson, B. (2001) The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions. American Psychologist, 56, p. 218 – 226.

Freedom House 2013. Freedom on the Net 2013. A Global Assessment of Internet and Digital Media. Summary of Findings. Online at https://freedomhouse.org/sites/default/files/resources/FOTN%202013%20Summary%20of%20Findings.pdf, last access on January 5, 2015.

Froomkin, A. M. (1995). The metaphor is the key: cryptography, the clipper chip, and the constitution. University of Pennsylvania Law Review, 709-897.

Froomkin, A. M. (1996). It Came From Planet Clipper: The Battle Over Cryptographic Key Escrow. U. Chi. Legal F., 15.

Furedi, F. (2006). Culture of fear revisited. A&C Black.

Gai, L. I., & Shan, C. O. N. G. (2012). On the Criminal Regulation of Cyber Homicide. Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition), 3, 008.

Geers, K. 2009. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective, 18, 1-7.

Gordon, S., and Ford, R. (2006) On the definition and classification of cybercrime. Journal in Computer Virology, 2, 1, p. 13-20.

Grabosky, P., Smith, R., & Urbas, G. (2004) Cyber criminals on trial. Criminal Justice Matters, 58, 1, p. 22-23.

Halder, D. (2013). Examining the Scope of Indecent Representation of Women (Prevention) Act, 1986 in the Light of Cyber Victimization of Women in India. *National Law School Journal*, *11*, 188-218.

Hampson, N. (2012). Hacktivism, Anonymous & a New Breed of Protest in a Networked World. Boston College International and Comparative Law Review, 35(6), 511.

Hayward, K. (2007) Situational crime prevention and its discontents: rational choice theory versus the 'culture of now'. Social Policy & Administration, 41, 3, p. 232-250.

Heichel, S., Pape, J. & Sommerer, T. 2005. Is there convergence in convergence research? an overview of empirical

Heidelberg, p. 527-534, http://link.springer.com/chapter/10.1007/978-3-642-25905-0_68, accessed 30/03/14.

Herley, C. "More is not the Answer", IEEE Security and Privacy, 2014

Hilley, S. (2006). Five years for Californian botmaster. Network Security, 2006(6), 1-2.

Hinkle, K. C. (2011). Countermeasures in the Cyber Context: One More Thing to Worry About. Yale Journal of International Law, 37, 11.

Holt, T. J. 2013. Examining the Forces Shaping Cybercrime Markets Online. Social Science Computer Review, 31, 165-177.

Hunton, P. 2012. Data attack of the cybercriminal: Investigating the digital currency of cybercrime. Computer Law & Security Review, 28, 201-207.

Inglesant, P. G., and Sasse. M.A. "The true cost of unusable password policies: password use in the wild." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010.

Internet Rights And Principles Coalition 2014. The Charter of Human Rights and Principles in the Internet. Online at http://internetrightsandprinciples.org/site/charter/, last access on January 5, 2015.

Jakobi, A. P. 2013. Non-State Actors All Around: The Governance of Cybercrime. In: JAKOBI, A. P. & WOLF, K. D. (eds.) The Transnational Governance of Violence and Crime. Non-State Actors in Security. Palgrave.

Jakobi, A. P. 2015. Non-State Actors in Global Crime Governance. Explaining the Variance in Public Private Interaction. British Journal of Politics and International Relations, forthcoming.

Jones, D., & Choo, K. K. R. (2014) Should There Be a New Body of Law for Cyber Space? Available at: http://ecis2014.eu/E-poster/files/0433-file1.pdf, accessed 28/09/14.

Joseph, J. (2003). Cyberstalking: An International Perspective (From Dot. cons: Crime, Deviance and Identity on the Internet, P 105-126, 2003, Yvonne Jewkes, ed.--See NCJ-199525).

Kam, S. (2004). Intel Corp. v. Hamidi: Trespass to chattels and a doctrine of cyber-nuisance. Berkeley Tech. LJ, 19, 427.

Keyser, M. 2003. The Council of Europe Convention on Cybercrime. Journal of Transnational Law and Policy, 12, 287-326.

Kierkegaard, S. 2007. Cybercrime Convention: Narrowing the Cultural and Privacy Gap? . International Journal of Intercultural Information Management, 1, 17-32.

Kigerl, A. 2012. Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review, 30, 470-486.

Kim, S. H., Wang, Q.-H. & Ullrich, J. B. 2012. A Comparative Study of Cyberattacks. Communications of the ACM, 55, 66-73.

Korns, S. W., and Kastenberg, J. E. (2008) Georgia's cyber left hook. Parameters, 38, 4, p. 60-76.

Kshetri, N. (2006) The simple economics of cybercrimes. Security & Privacy, IEEE, 4, 1, p. 33-39.

Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.

Kshetri, N. 2013. Cybercrime in the Former Soviet Union and Central and Eastern Europe: current status and key drivers. Crime, Law and Social Change, 60, 39-65.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers & Security, 45, 58-74.

Lakhani, K. R., and Wolf, R. G. (2005) Why hackers do what they do: Understanding motivation and effort in free/open source software projects. Perspectives on free and open source software, 1, p. 3-22.

Layous, K., Nelson, S. K., & Lyubomirsky, S. (2013) What is the optimal way to deliver a positive activity intervention? The case of writing about one's best possible selves. Journal of Happiness Studies, 14, 2, p. 635-654.

Lazarus, R. and Folkman, S. (1984a). Stress, appraisal and coping. New York: Springer.

Lazarus, R. and Folkman, S. (1984b) Stress, coping and adaptation. New York: Springer.

Lee, O., & Shin, M. (2004). Addictive consumption of avatars in cyberspace. CyberPsychology & Behavior, 7(4), 417-420.

Levi, M., Innes, M., Reuter, P. and Gundur, R. (2013). The economic, financial & social impacts of organised crime in the European Union. Directorate General for Internal Policies (European Parliament), p.68. Available: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493018/IPOL-JOIN_ET%282013%29493018_EN.pdf

Lewis, J. A. (2002, 12). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats:. Retrieved from http://www.enhyper.com/content/0211_lewis.pdf

Liss, C. & Sharman, J. C. 2015. Global corporate crime-fighters: Private transnational responses to piracy and money laundering. Review of International Political Economy, forthcoming.

Livingstone, S., Helsper, E.J., (2007) Taking risks when communicating on the Internet: The role of offline social-psychological factors in young people's vulnerability to online risks. Information, Communication and Society 10(5), 619-644.

Loo, E. and Yeap, S. B.(1998). Cyber-colonialism in Asia : more imagined than real? In AMIC 7th Annual Conference: Asia's Information Marketplace, Race for Technology, Content and Competence, Bangkok, May 21-23, 1998. Singapore: Asian Media Information and Communication Centre.

Luiijf, H., Besseling, K., de Graaf, P., and Spoelstra, M. (2013) "Ten National Cyber Security Strategies: A Comparison." Critical Information Infrastructure Security. Springer Berlin Heidelberg, p. 1-17.

LUSA. (2009, 10 14). DN Ciências. Retrieved 3 10, 2015, from Diário Notícias: http://www.dn.pt/inicio/ciencia/interior.aspx?content_id=1390758&seccao=Tecnologia&page=-1

LUSA. (2015, 3 3). SICNOTICIAS. Retrieved 3 10, 2015, from http://sicnoticias.sapo.pt/pais/2015-03-03-Ministra-garante-que-Portugal-e-dos-paises-mais-seguros-do-Mundo

Maslow, A. (1954) Motivation and Personality. New York: Harper & Row.

Matwyshyn, A. M., Cui, A., Keromytis, A. D., & Stolfo, S. J. (2010). Ethics in security vulnerability research. Security & Privacy, IEEE, 8(2), 67-72.

Matza, D., & Sykes, G. M. (1961). Juvenile delinquency and subterranean values. American sociological review, 712-719.

Matza, D. (1964). Delinquency and drift. Transaction Publishers.

McAfee (2014) Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II available from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2

McDonald, A.M., & Cranor, L.F. (2009) "The cost of reading privacy policies", ISJLP, vol. 4, pp. 543-897,.

McGuire, M. and Dowling, S. (2013) 'Cybercrime: A review of the evidence', available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf, accessed 28/09/14.

McQueen, M., Wright, J. L., & Wellman, L. (2011, September). Are vulnerability disclosure deadlines justified?. In Security Measurements and Metrics (Metrisec), 2011 Third International Workshop on (pp. 96-101). IEEE.

Mendez, F. 2005. The European Union and cybercrime: insights from comparative federalism. Journal of European Public Policy, 12, 509-527.

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

Neufeld, D. J. (2010, January). Understanding Cybercrime. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on* (pp. 1-10). IEEE.

Newman, G. R., & Clarke, R. V. (2013). Superhighway robbery. Routledge.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5(1), 773-793.

NIST (2010) Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (full text available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF)

NIST (2013) Security and Privacy Controls for Federal Information Systems and Organisations (Full text available from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Nosek, B. A., Banaji, M. R., & Greenwald, A. G. (2002). E-Research: Ethics, Security, Design, and Control in Psychological Research on the Internet. Journal of Social Issues, 58(1), 161-176.

Oates, B. (2001). Cyber crime: How technology makes it easy and what to do about it. Information systems management, 18(3), 92.

Office for National Statistics - ONS (2014) 'Discussion paper on the coverage of crime statistics', available at: http://www.ons.gov.uk/ons/search/index.html?newquery=Discussion+paper+on+the+coverage+of+crime+statistics, accessed 28/09/14.

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. Vulnerable Children and Youth Studies, 8(4), 298-309.

Pearson, E. (2009). All the World Wide Web'sa stage: The performance of identity in online social networks. First Monday, 14(3).

Peterson, C. (2013) Pursuing the Good Life: 100 Reflections in Positive Psychology. New York: Oxford University Press.

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

Pocar, F. (2004) New challenges for international rules against cyber-crime. European Journal on Criminal Policy and Research, 10, 1, p. 27-37.

PONEMON INSTITUTE (2014) *Global Report on the Cost of Cyber Crime*. Available, http://www8.hp.com/uk/en/software-solutions/ponemon-cyber-security-report/

Portugal, C. –T. (October de 2007). COMMITTEE OF EXPERTS ON TERRORISM (CODEXTER). Obtido de Council of Europe: http://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/Portugal.pdf

Powers, T. M. (2003). Real wrongs in virtual communities. Ethics and Information Technology, 5(4), 191-198.

Prevelakis, V., & Spinellis, D. (2007). The athens affair. Spectrum, IEEE, 44(7), 26-33.

Radcati Group, (2015) Email Statistics Report, 2015-2019 Executive Summary (available from http://www.radicati.com/?p=10644)

Rahman, M. M., Khan, M. A., Mohammad, N., and Rahman, M. O. (2009) Cyberspace claiming new dynamism in the jurisprudential philosophy: A substantive analysis of conceptual and institutional innovation. International Journal of Law and Management, 51, 5, p. 274-290.

Ransbotham, S., & Mitra, S. (2013). The Impact of Immediate Disclosure on Attack Diffusion and Volume. In Economics of Information Security and Privacy III (pp. 1-12). Springer New York.

Rauscher, K.F, Cox, E.F. 2013. Measuring the Cybersecurity Problem, East West Institute. Available: http://www.ewi.info/idea/measuring-cybersecurity-problem

Reiner, R. (1988) 'British criminology and the state', British Journal of Criminolgy, 29(1), 138-58

Richardson, R. (2011) CSI computer crime and security survey," available at: http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf, accessed 03/04/15.

Ruginis, C. & Rughinis, R. 2014. Nothing ventured, nothing gained. Profiles of online activity, cybercrime exposure, and security measures of end-users in the European Union Computers and Society, 43, 111-125.

Roberts, P. and Kielstra, P. (2013). What's in a number? Estimating the cost of cybercrime. The Economist Insights. [online] Available at: http://www.economistinsights.com/technology-innovation/analysis/measuring-cost-cybercrime

Rogers, M. K., & Seigfried-Spellar, K. C. (2014). Using Internet Artifacts to Profile a Child Pornography Suspect. Journal of Digital Forensics, Security and Law, 9(1), 57-66.

Sangarasivam, Y. (2013). Cyber Rebellion: Bradley Manning, WikiLeaks, and the Struggle to Break the Power of Secrecy in the Global War on Terror. Perspectives on Global Development and Technology, 12(1-2), 69-79.

Schechter S., et al., "The Emperor's New Security Indica- tors: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies," Proc. IEEE Symp. Security and Privacy, IEEE CS, 2007, pp. 51–65.

Schrittwieser, S., Mulazzani, M., & Weippl, E. (2013, May). Ethics in security research which lines should not be crossed?. In Security and Privacy Workshops (SPW), 2013 IEEE (pp. 1-4). IEEE.

Shepherd, S. (2003). Vulnerability Disclosure: How Do We Define Responsible Disclosure?. GIAC SEC Practical Repository, SANS Inst, 9.

Solow, Robert M. (1977) "Leff's Swindling and Selling: The Spanish Prisoner and Other Bargains." The Bell Journal of Economics, 8, 2, p. 627-629, available at:

http://www.jstor.org/stable/3003313, accessed 30/09/14.

Steinmetz, K. F., & Gerber, J. (2014) "The Greatest Crime Syndicate since the Gambinos": A Hacker Critique of Government, Law, and Law Enforcement. Deviant Behavior, 35(3), 243-261.

Steinmetz, K. F. (2015). Craft (y) ness An Ethnographic Study of Hacking. *British Journal of Criminology*, 55(1), 125-145.

Sukenik, M. D. Y. (2011) Distinct Words, Discrete Meanings: The Internet & Illicit Interstate Commerce. Jounal of Law, Technology and policy, p. 1-38.

Symantec Corporation (2011) “Norton 2011 cybercrime report,” available at: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf, accessed 02/04/15.

Tade, O. (2013) A spiritual dimension to cybercrime in Nigeria: The ‘yahoo plus’ phenomenon. Human Affairs, 23(4), 689-705.

Taylor, P. A. (2001). Editorial: Hacktivism. The Semiotic Review of Books, 12(1), 1-4.

Taylor, M., & Quayle, E. (2003). Child pornography: An internet crime. Psychology Press.

Tripathi, S. (2015). Cyber: Also a Domain of War and Terror. Strategic Analysis, 39(1), 1-8.

Trustwave (2015) ‘Security Pressures Report 2015’, available at: https://www2.trustwave.com/rs/trustwave/images/Trustwave_2015SecurityPressuresReport-FINAL.pdf, accessed 30/4/2015.

Tynes, B. M. (2007). Internet safety gone wild? Sacrificing the educational and psychosocial benefits of online social environments. Journal of Adolescent Research, 22(6), 575-584.

Von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). Radicalisation in the digital era: The use of the Internet in 15 cases of terrorism and extremism. Brussels: RAND.

Wales, E. 2001. Global Focus on Cybercrime. Computer Fraud & Security, 2001, 6-6.

Weaver, N., Paxson, V., Staniford, S., & Cunningham, R. (2003) A taxonomy of computer worms. In Proceedings of the 2003 ACM workshop on Rapid malcode (pp. 11-18). ACM.

Wehmeyer, M and Little, T. (2009) Self-determination. In S. Lopez (Ed.) Encyclopedia of Positive Psychology, (pp. 868-874). Chichester: Blackwell Publishing Ltd.

Wall, D. S. (2013). Policing identity crimes. Policing and Society, 23(4), 437-460.

Weintraub-Reiter, R. (1998). Hate speech over the Internet: A traditional constitutional analysis or a new cyber constitution. BU Pub. Int. LJ, 8, 145.

Wu, S. Y., Chen, P. Y., & Anandalingam, G. (2003). Fighting information good piracy with versioning. ICIS 2003 Proceedings, 51.

Yar, M. (2006) Cybercrime and Society. London: SAGE

Yazdanifard, R., Oyegoke, T., & Seyedi, A. P. (2011) Cyber-Crimes: Challenges of the Millennium Age. In Advances in Electrical Engineering and Electrical Machines (pp. 527-534). Springer Berlin Heidelberg.

Zhao, S., Grasmuck, S., & Martin, J. (2008). Identity construction on Facebook: Digital empowerment in anchored relationships. Computers in human behavior, 24(5), 1816-1836.

Zavrsnik, A. (2007) Absence of Body in Cyberspace Criminal Justice Impact, The. Masaryk UJL & Tech., 1, 43.

Zeller, T. (2005). Black market in stolen credit card data thrives on Internet. *New York Times*.

Annex A

Victimisation Survey

Website references: section 3.1

Group-IB http://report2014.group-ib.ru/

IDC (2014) http://www.idc.com/prodserv/maps/securityproducts.jsp

World Wide Web Consortium (2015) http://www.internetlivestats.com/internet-users/

RIPE (2015) https://www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing

Internet Telecommunications Union (2015) http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Bots vs Browsers (2015) http://www.botsvsbrowsers.com/

Barracuda (2015) www.barracudacentral.org/data/spam

Spamhaus (2014) www.spamhaus.org

AV-Test (2015) http://www.av-test.org/en/statistics/malware

Akaimai (2014) http://www.akamai.com/html/technology/dataviz1.html

Squid Blacklist (2014) www.squidblacklist.org/downloads.html

Shadowserver (2014) https://www.shadowserver.org/wiki/

HostExploit (2014) http://hostexploit.com/?p=reports