WORKING PAPER

INFORMATION SHARING AND PUBLIC-PRIVATE PARTNERSHIPS: PERSPECTIVES AND PROPOSALS

with the support of:

Global Cyber Security Center

unicri
United Nations
Interregional Crime and Justice
Research Institute

United Nations
Interregional Crime and Justice
Research Institute

Working Paper

Information Sharing and Public-Private Partnerships: Perspectives and Proposals

DISCLAIMER

Acknowledgments

This working paper has been developed thanks to the active contributions of the European Electronic Crime Task Force partners and the information shared by ABI Lab.
Special gratitude is also owed to Arthur Brocato of UNICRI for editing the document.

With the support and participation of the Global Cyber Security Center (GCSEC)

GLOBAL CYBER SECURITY CENTER

INDEX

Executive Summary

The purpose of this study aims to explore the issue of information sharing and the formation of public-private partnerships as they pertain to the sphere of cyber security.

Unfortunately, a variety of obstacles exist when attempting to forge public-private partnerships to secure cyberspace. The following obstacles are analyzed in Chapter 1 of this assessment: (a) different mandates and legal capacities (b) privacy rights and security clearances and (c) the dissolution of inter-systemic trust. In turn, the later portion of the chapter offers a series of solutions and practices to overcome these obstacles.

Chapter 2 examines the legislative frameworks available for facilitating information sharing and tackling cyber security issues. These frameworks range from the UN and regional organizations, such as the EU and the Council of Europe, to the national level of policy making for individual states.

Good practices are the focus of Chapter 3, as the report takes into consideration the work of 19 initiatives distributed across the globe and analyzes how they contribute to information sharing. Specific case studies regarding the work of the European Electronic Crime Task Force (EECTF) and the Online Fraud Cyber Centre and Experts Network (OF2CEN) are analyzed in detail.

In the final chapter, we offer a series of recommendations for promoting information sharing and enhancing security in cyberspace. These include:

- the need for legislators to factor in the importance of trust and mutual assurance between the public and private sectors when considering the formulation of any information sharing legislation;
- the need for increased awareness of the existence and function of cyber security exchange mechanisms;
- and finally, the need for a clear understanding of what term Cyber Security means and how each private and public institution can position itself within a secure network of information.

List of Acronyms

ACDC	Advanced Cyber Defence Center
APWG-IPC	Anti-Phishing Working Group - Internet Policy Committee
BYOD	Bring Your Own Device
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CIIP	Policy on Critical Information Infrastructure Protection
CISPA	Cyber Intelligence Sharing and Protection Act
CNAIPIC	National Anti-Cyber-Crime Center for the Protection of Critical Infrastructures
CNCI	Comprehensive National Cybersecurity Initiative
CRITIC	CRimeInformaTionsharing In Cyberspace
CSISP	Cyber Security Information Sharing Partnership
DCC	Digital Crimes Consortium
DDoS	Distributed Denial of Service Attacks
EBF	European Banking Federation
ECHR	European Convention of Human Rights
EECTF	European Electronic Crime Task Force
ENISA	European Network and Information Security Agency
EP3R	European Public Private Partnership on Resilience
EPC	European Payments Council
EU	European Union
EU FI-ISAC	European Financial Institutions Information Sharing and Analysis Centre
FI-ISAC.NL	FI-ISAC Netherlands
FS-ISAC	Financial Services Information Sharing and Analysis Center
GA	United Nations General Assembly
GCSEC	Global Cyber Security Center
ICS-SCADA	Industrial Control Systems- Supervisory Control Data Acquisition forum
ICT	Information and Communication Technology
INSPECT	INformation Sharing PErspeCTives
ISP	Internet Service Provider
ITU	International Telecommunication Union
IWWN	International Watch and Warning Network
J-CSIP	Initiative for Cyber Security Information Sharing Partnership of Japan
LEA	Law Enforcement Agency
MAA	Mutual Aid Agreement
MARIE	Mutual Aid for Resilient Infrastructure in Europe
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIS	Network and Information Security
NATO	North Atlantic Treaty Organization
OF2CEN	Online Fraud Cyber Centre and Experts Network
PARIS	PARtnership in Information Sharing
PPP	Public Private Partnership
SINCE	Sharing Information in CybercrimE
TF-CSIRT	Task Force-Computer Security and Incident Response Team
TGL	Trust Digital Life
UN	United Nations
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNODC	United Nations Office on Drugs and Crime
USA	United States of America
WARP	Warning Advice Reporting Point
WEF	World Economic Forum

Introduction

The age of Information and Communication Technology (ICT) has fully bloomed. According to estimates made by the International Telecommunication Union (ITU), approximately 2.749 billion people worldwide were using the internet in 2013[1]. The total value of online sales in 2011 was €572 billion, which is €61 billion higher than the estimate in 2010[2]. These astonishing figures render merely a portion of the today's overall cybersphere, which continues to expand at an exponential pace. The growth of ICTs has revolutionized all elements of local and global exchange in both licit and illicit frameworks. Email, online banking and social networks have enabled social inclusion and political cooperation; they have allowed for the success of civil movements, like the Arab Spring[3], and they continue to support advances in critical infrastructure worldwide. It is estimated that over the past decade Internet penetration grew by about 3,607% in Africa and 2,640% in the Middle East[4].This accelerating dissemination is generating a variety of issues for regulators like: "the lack of regulations dealing with data messages and electronic signatures", "the absence of specific legislations protecting consumers, intellectual property, personal data, information systems, and networks" and "the dearth of appropriate fiscal and customs legislation covering electronic transactions"[5].

As slow paced bureaucracies struggle to match this exponential growth, illicit uses of ICTs have flourished. In the Budapest Convention[6], the European Council defined 'cybercrime' as substantive criminal conduct in four different categories (1) offences against the confidentiality, integrity and availability (CIA) of computer data and systems(2) computer-related offences, (3) content-related offences and (4) offences related to infringements of copyright and related rights. Defined as such, cybercrime is understood to produce more revenue than the illegal sale of drugs and account for the theft of intellectual property worth over 1 trillion each year[7]. In 2012, the number of victims of cybercrime was estimated at 65% of all Internet users, which was estimated to be 2.4 billion[8] people. The most recent developments in ICTs, namely cloud computing, mobile computing, and 'bring your own device' (BYOD) cultures, are already being targeted and exploited by criminal actors. The

---

[1]International Telecommunication Union (2013)."Key [2006-2013] ICT indicators for developed and developing countries and the world" (totals and penetration rates), Aggregate Data.Online. Accessed on 18/02/2014. Available at: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[2]Brain Statistics (2013) "E-Commerce / Online Sales Statistics." *Statistic Brain RSS*. Online. Accessed on 07/02/2013. Available at: http://www.statisticbrain.com/total-online-sales/

[3]Allagui I.,Kuebler J. (2011). "The Arab Spring and the Role of ICTs." *International Journal of Communication* 5 (1932-8036/2011). Print.

[4]Internet World Stats (2012)

[5]Karake-Shalhoub Z, Al Qasimi L., (2010). "Cyber Law and Cyber Security in Developing and Emerging Economies". Cheltenham, UK: Edward Elgar, 2010. Print. P.9-15

[6]Council of Europe Convention on Cybercrime "Budapest Convention", 23.XI.2001

[7] The Economist (2011) "Measuring the Black Web." *The Economist*. Online. Accessed on 02/02/2013. Available at: http://www.economist.com/node/21532263
Cybercrime is also now ranked the fourth most common form of economic crime, see PwC (2012) "An Australian Snapshot of Economic Crime". Pricewaterhouse Coopers. Online. Accessed on 04/01/2013. Available at: http://www.pwc.com/gx/en/economic-crime-survey/assets/global-economic-booklet-vfa-med.pdf

[8] Internet World Stats (2012) Please refer also to Al-Greene, B. "65% of Internet Users Are Cybercrime Victims [INFOGRAPHIC]." *Mashable*. Online. Accessed on 02/02/2013. Available at: http://mashable.com/2012/11/05/cybersecurity-infographic/
It has also been estimated that the total number of victims is 556 million, see Symantec (2012) "2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually." *Symantec*. Online. Accessed on 07/02/2013. Available at: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02

scale of these potential attacks, coupled with our increasing reliance on ICTs for all aspects of public and private life, is raising serious concerns amongst public and private sectors worldwide. The gravity of the situation calls for the urgent creation of national and international best practices for monitoring and securing the cybersphere.

The rise of cybercriminal activity has been exasperated primarily by two factors (a) that it allows cybercriminals to operate within the particular terminology of a forum and (b) that the Internet can allow perpetrators to hide behind anonymity. The Internet allows for a flexibility of communication and the fast evolution of symbolic paradigms. In so doing it renders a lingual asymmetry between those that are actively involved within forums and those who, like law enforcers, are outliers. This asymmetry in dialogue and communication renders a notion of belonging and comradeship which serves to spur and encourage criminal behavior. Similarly, the fact that the Internet can provide a strong sense of anonymity renders cybercriminal activity more alluring than other physical forms of criminal conduct[9]. Therefore, in order to prevent cybercriminals from taking initiative "it is important for those involved in the fight against cybercrime to try to anticipate qualitative and quantitative changes in its underlying elements"[10], in other words to engage in profiling exercises and to maintain a direct involvement within their sphere of operations .

Although an overview of the typologies of cybercrime is beyond the scope of our analysis, it is worth briefly mentioning some of the modalities of cybercriminal activity to emphasize the need for more accurate scope definitions, both in the social and legal realms. The European Network and Information Security Agency (ENISA) lists "some of the major threat agents in cyberspace" as: corporations that engage in offensive tactics, cybercriminals that operate for financial gain, disgruntled and/or distracted employees, hacktivists that are politically or socially motivated, Nation States and terrorists that have political or religious motives[11]. In its 2013 report, ENISA added Cyber Fighters, which are nationalist-oriented citizens; Script Kiddies, representing young, novice hackers knowing basic code; and Online Social Hackers, utilizing social engineering skills, to the list of major threat agents as well[12]. Within the same report, ENISA, acknowledges that these agents can operate by means of at least 15 different mechanisms within at least seven domains. These figures point to the vastness and dispersed nature of the phenomena which is loosely termed 'cybercrime', and reflect back to the asymmetry of understanding between criminal policy and the active criminal behavior.

One of the routes explored by legislators and policy makers to bridge the gap between cyber-policy and cyber-crime is information sharing between private and public entities. In this study we present the current state of information sharing, at the national and international level, and the impact it can have on the security of our critical infrastructure, financial institutions and transport facilities. The term "information sharing", first gained popularity after the 9/11 attacks on the World Trade Center in New York. It was widely held during the

[9]Bagilli M. (2009) Effects of Anonymity, Pre-Employment Integrity and Antisocial Behavior on Self-Reported Cyber Crime Engagement: An Exploratory Study, CERIAS Tech Report 2009-31. Online. Accessed on 02/02/2013. Available at: http://completosec.wordpress.com/2011/03/06/anonymity-antisocial-behavior-integrity-and-cybercrime/

[10] McAfee (2011) *Prospective Analysis on Trends in Cybercrime from 2011 to 2020.* McAfee. Online. Accessed on 4/02/2013. Available at: http://www.mcafee.com/it/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf

[11] European Network and Information Security Agency (ENISA) (2012) *Threat Landscape: Responding to the Evolving Threat Environment.* ENISA. Online. Accessed on 02/02/2013. Available at: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment

[12]European Network and Information Security Agency (ENISA) (2013) *Threat Landscape 2013: Overview of current and emerging cybe- threats.* ENISA. Online. Accessed on 18/02/2014. Available at:http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

investigations following the event that the government was in possession of information that, had it been shared, could have led to a more effective security strategy. Nowadays Information Sharing has been interpreted in a variety of different ways and can be understood as the collaboration between private and public institutions, or as the collaboration between individual people and private or public institutions[13]. However, within the scope of this essay we will define the term as it was originally intended, meaning the collaboration between public and private institutions, particularly with regards to security weaknesses. We consider Information Sharing as an overall best practice in dealing with cyber-threats because it offers the potential to effectively counter: the diffuse geographical collocation of cybercrime, the ample number of actors it involves and the diverse motivations behind the attacks and the diverse definition of the terms these involve. Though there is a general agreement that Information Sharing is generally beneficial and ought to be included amongst best practice cybersecurity principles, there is little agreement concerning how it should be implemented[14]. Through a review of all the present literature on informationsharing and cybersecurity, we have identified three main contentious topics: the conflict of interests between private and public entities, the degree of balance between privacy rights and information sharing, and a loss of trust in institutions at large.

The first phase of this research is concerned with working through the current debates on these two issues, with the overall aim of establishing a list of best practices that will enable cooperation between public and private institutions. Our analysis at this stage will be entirely based on the literature reviewed. The first section of the paper is concerned with introduction of the primary obstacles that prevent information sharing by inhibiting the flow of information either from private institutions to public bodies, or vice-versa. For the sake of clarity, we have categorized these challenges into: the irreconcilability of mandates, issues of data protection and the breakdown of inter-systemic trust. Having presented these, we will proceed to discuss the various enablers to Information Sharing that we found in the literature. We have divided these into: increasing the level of physical exchange between private and public organizations, the consolidation and simplification of legislation regarding data protection, equal accountability of the participating parties, symmetrical data flow between the participating parties, general awareness schemes that aim to promote a culture of cybersecurity, and the creation of personal data lockers[15].

Having worked through these debates, we will turn to the legislation that impacts upon Information Sharing and we will try and evaluate which jurisdictions are best suited to enact enablers for cooperation mechanisms and cyber-resilience strategies to take effect. At the international level, our analysis will focus in particular on the efforts made by the United Nations and the European Union. As the scope of our research does not stretch to cover matters of intelligence collection, we will not dwell on the role that international military alliances, like NATO, play in this field. At the national level, we will look at which strategies governments have adopted to implement more structured mechanisms of Information Sharing. Though we will briefly consider the cases of Italy and the USA, this section is designed to give an overall idea of the tools available to governments to create a general culture of cybersecurity.

---

[13] Techopedia. (2013) "Information Sharing." *Techopedia*. Online. Accessed on 20/02/2013. Available at: http://www.techopedia.com/definition/24839/information-sharing

[14] National Security Program, Homeland Security Program (2012) *Cyber security Task Force: Public-Private Information Sharing*. Bipartisan Policy Center. Online. Accessed on 07/02/2013. Availableat: http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf

[15] Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Cybersecurity Strategy of the European Union: An Open, Safe, Secure Cyberspace. 07/02/2013. COM (2013) 48 final.

The third, and final, part of our analysis will present a table, in which we have outlined the different modalities of information sharing that are currently in place and how they operate. This table, by highlighting the details of different Information Sharing initiatives, has allowed us to devise a series of best practice principles that we sustain would enable effective cooperation and exchange. In order to fully understand these principles, it is essential to understand what we mean by private and public cooperation. To this end, we will list below the public, private and international / transnational entities relevant to information Sharing[16]. We use the term 'public' to refer to: the national government and its sub-bodies, independent regulatory bodies, the military and local government. The term 'private' will be used to represent: critical infrastructure sector organizations, ICT service providers, industry and business at large, small and medium enterprises, software and hardware manufacturers, and specialist defense security contractors. Finally with regard to international/transnational actors we will refer to: multinational arrangements (with particular emphasis on the United Nations, European Union and the US-EU working group on Cybersecurity), multi-stakeholder institutions, international standardized bodies and informal international arrangements. For the purposes of this paper, we will consider research and data banks conducted by, and preserved within, universities to be the interface between public and private interests. With these definitions established, the chart and list of best principles that can be found in the last part of our analysis, present a comprehensive aid to enabling mechanisms of Information Sharing.

[16]Our definitions of what constitutes public, private and international/transnational actors was largely influenced by that in Klimburg A. (2012) *A National Cyber Security Framework Manual.* CCDCOE supported by the NATO Science for Peace and SecurityProgramme. Online. Accessed on 07/02/2013. Available at: https://www.ccdcoe.org/4.html

Chapter One- Information sharing and relevant open issues

Information Sharing within the cybersecurity domain is a key element of collaboration between public and private entities aimed at creating a resilient response to cybercrime. The four key themes of Cyber resilience strategies are: deterrence, protection, detection, response and recovery[17]. Although both private and public institutions parade these themes as the foundations of their own cybersecurity strategies, they tend to bolster them through the adoption of different and apparently irreconcilable approaches. Through a detailed analysis of the available literature we have identified that there are three main motives why modus operandi of public and private entities appear so incongruous to one another; these are (a) different mandates and legal capacities (b) privacy rights and security clearances and (c) the dissolution of inter-systemic trust. Each of these factors, in turn, impacts negatively upon the ability and willingness of institutions and corporations to cooperate and share information with one another. The first part of this chapter, entitled Real and Perceived Obstacles to Information Sharing, will evaluate how conflicting mandates, data protection concerns and the dissolution of inter-systemic trust can impact information sharing. The second half of this chapter, entitled Strategies to Overcome Real and Perceived Obstacles to Information Sharing presents an overview of the tools that can be employed to overcome the barriers to information sharing mentioned in the first chapter.

1. Real and Perceived Obstacles to Information Sharing

(a) Different Mandates and legal capacities

As defined in our introductory chapter, public bodies are concerned with legislative and law enforcement aspects of cybersecurity; on the other hand, private institutions are mostly charged with the immediate protection of "their own portion of cyberspace", which they must preserve in order to maintain client satisfaction and avoid business disruptions[18].The public sector's mandate translates to scrupulous and law abiding methods of collecting evidence, diligent analysis and a focus on data that can be collocated within a greater national or international security strategy that is designed to foresee and prevent future attacks. However, these tasks are burdened by lengthy bureaucratic processes, limited financial means[19] and a poor understanding of advanced technical terminology[20]. Inversely, the private sector tends to perceive the role within cybersecurity as that of timely, and efficient resolution to imminent threats and attacks[21]. Within this understanding of the mandates of public and private institutions there appears to be a baseline assumption that qualitative investigations, generally associated with public institutions, cannot be reconciled with timeliness and efficiency,

[17]European Network Security Agency (ENISA) (2012) *National Cyber Security Strategies: An Implementation Guide*. ENISA, Online. Accessed on 07/01/2013. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

[18]European Network and Information Security Agency (ENISA) (2012) *Give and Take: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime; Legal, Regulatory and Operational Factors Affecting CERT Cooperation with other Stakeholders.* European Network and Information Security Agency. Online. Accessed on 07/01/2013. Available at: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime

[19]Particularly since the financial crisis, *Ibid* p.60

[20]Klimburg A. (2012) p. 140-141

[21]*Ibid*

generally linked to private organizations. However, evidence provided in the literature reviewed, suggests that the qualities and faults of private and public institutions are complementary and can easily benefit from mutual cooperation and information sharing.

Public institutions could benefit greatly by data collection capabilities and technical knowledge that private bodies posses. The agility and ability to gather information on threats to different systems is particularly important when tackling cybercrime because of the evasive nature of cybercrime[22], which renders it difficult for an institution working within a law enforcement mandate to invest in widespread monitoring capabilities. Furthermore, the knowledge collected and gathered by private institutions is strengthened by an understanding of the technical terminology which the legal realm sometimes lacks. It follows that real time information sharing would serve to create a concrete threat database and to create an incentive for the introduction of technological discourse within public institutions[23].

Private institutions have an interest in supporting the wider scale cybercrime prevention and deterrence initiatives generated by the public institutions because they do not possess the time or scope to engage in long term investigations stemming from individual incidents[24]. Too often "[the private sector's] focus on efficient problem solving leaves limited time and resources for legal questions and challenges"[25]; this means that the full prosecution and deterrence factors are largely left to public organizations. Information sharing therefore, serves the private sector by ensuring that its particular attackers are being reasonably monitored and active steps are being taken by national and international law enforcement agencies to counter them.

On a different note, The *Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime; Legal, Regulatory and Operational Factors Affecting CERT Cooperation with other Stakeholders*[26] report published by ENISA, points out that the divergent mandates of the public and private sectors also create operational barriers to information sharing. Namely, the report states that a focus on time efficiency prevents private institutions from collecting evidence in a way that is legally endorsed. However, the report also notes that this failure to meet adequate standards is more likely attributable to a lack of legal training rather than to a commitment to efficiency, or general neglect. Information Sharing, would be also beneficial in this aspect as it would encourage the public sector to instruct the private sector on the legal definitions of evidence collection.

(b) Data Protection

Data protection, or the preservation of privacy, is among the most hotly debated catchwords of our time. In 2012, news agencies across the world thrived on stories like Google's changes to its online privacy policy, the UK's phone hacking scandal and the controversy surrounding

[22] *Ibid*, p. 140
[23] International Telecommunications Union (ITU) (2012) *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* ITU. Online. Accessed on 25/01/2013. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf p. 228
[24] European Network and Information Security Agency (ENISA) (2012) *Give and Take: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime; Legal, Regulatory and Operational Factors Affecting CERT Cooperation with other Stakeholders*. European Network and Information Security Agency p.54
[25] *Ibid*, p.54
[26] *Ibid*

the proposed Cyber Intelligence Sharing and Protection Act (CISPA)[27]. Like many other catch-phrases, privacy does not have a clear meaning, in either the civil or legal realms[28]; its ambiguity adds to its mysticism and renders it a word that individuals and businesses are anxious to toy with. The reason why the term has such a strong, often detrimental, effect on information sharing is that the widespread public scrutiny of data preservation renders institutions (both public and private) anxious about exchanging anything that might corrupt their image in the public sphere[29].

This sensitivity and caution with regard to sharing information which might be traced back to an individual is exasperated by the vast amount, and confusing nature, of privacy legislation. Within the European framework alone, there are three key directives regulating the use of data to ensure the protection of the right to privacy as established by Article 8 of the European Convention on Human Rights[30]. These are the Data Protection Directive, which prevents personal data from being processed unless there is a transparent, legitimate, purposeful and proportionate reason; the Directive on Privacy and Electronic Communications, which complements the data Protection Directive by rendering it applicable to ICTs; and the Data Retention Directive obliges Member States to retain their citizens' telecommunications data for a maximum of twenty-four months unless there is a legitimate and proportional reason [31].

The combination of stringent legislation derived from multiple sources of legislation and a blurry notion of privacy render corporations weary of sharing information both internally and externally. Corporations not only need to guard against potential lawsuits but also need to guard their reputation and maintain a favorable public image, in order to do this they must abide by the cultural sensitivities regarding data protection, which often exceed those stipulated by legal norms. The spectrum of privacy sensitivities varies greatly, for example, in the US customers perceive personal financial information as "highly sensitive" whilst in Norway tax and income are published openly[32]. Overall cultural conceptions of privacy pose two strains on information sharing systems: firstly, and most obviously, they render companies reluctant to share information for fear that their reputation might be damaged and secondly, the disparity between them makes it hard to envision a uniform international system of cooperation.

In the past, organizations used a variety of de-identifying techniques to be able to communicate data in a meaningful, yet privacy abiding way[33]. Personal identifiers could successfully be removed from all data, creating a truly anonymous set of information. However, modern technology is currently breaking down the barriers that once enable anonymity. "Data miners" can be extremely crafty in deriving personal data. This was first demonstrated by Arvind Narayanan and VitalyShmatikov, who identified several people on

---

[27] World Economic Forum (WEF) (2012)*Rethinking Personal Data: Strengthening Trust*. WEF. Online. Accessed on 28/01/2013. Available at: http://www.weforum.org/reports/rethinking-personal-data-strengthening-trust

[28] European Network and Information Security Agency (ENISA) (2012) "Give and Take…" Accessed on 07/01/2013. p. 57; see also World Economic Forum (WEF) (2012)

[29] World Economic Forum (WEF) (2012)

[30]European Convention of Human Rights (ECHR) Art 8 and The Charter of Fundamental Rights of the European Union (Treaty of Lisbon) Art. 2

[31]Council Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector [2002] OJ L201, Council Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281, Council Directive 2006/24/EC On the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Networks and Amending Directive2002/58/EC [2006] OJ L 105/54.

[32] World Economic Forum (WEF) (2012)

[33]*Ibid*

an anonymous list posted by Netflix back in 2006, but has since become a common issue for servers and social networking sites[34]. Because de-identification has been overhauled, the success of information sharing in overcoming the 'privacy' barrier is dependant on the creation of alternative assurances which we will continue to discuss in the second part of this chapter.

A similar barrier to information sharing is that of security clearances and national security concerns. On the one hand, governments are increasingly using personal data for law enforcement and national security, and employing both personal data and data about security breaches to profile potential threats to national security[35]. In order to do this, they often rely on information that is provided to them by private agencies[36]. On the other hand, given the surge in national security concerns over the past decade[37], governments are understandably reluctant to divulge "classified" information [38] .Shan Henry, former head of the FBI's Cybercrime Division, even goes as far to say that even though the FBI was often aware that their information sharing policy could contribute to ongoing investigations, it would opt not to disclose it for fear of compromising national security[39]. In sum, the social anxiety that is associated with national security discourse acts as an obstacle to information sharing because it renders governments weary of divulging information to private institutions. In this respect, it recalls the notion of privacy, which acts as a barrier to information sharing because it makes private companies wary of sharing information with public bodies for fear that it may harm their image among consumers.

(c) Trust

At the foundation of the concerns for privacy and national security is the breakdown of traditional 'trust' mechanisms between public and private entities, and individual citizens[40]. The World Economic Forum, in its report *Rethinking Personal Data: Strengthening Trust*[41], points out that the "data ecosystem", like most other transaction systems today, is something that is largely misunderstood. This lack of knowledge renders people, and the institutions they run, generally skeptical and not trusting of its operations. This lack of trust creates a barrier to information sharing by exasperating the differences between the mandates of public and private entities, and by maximizing concerns of privacy and national security.However, as the report also notes, ordinary people interact on a daily basis with systems of which they don't understand the full extent (e.g. banking or plumbing). Although it is impossible to offer an exact explanation of why, information sharing mechanisms are not as trusted as other specialized mechanisms In the following section, we point to some aspects of the relationship

[34] *Ibid,* see also: Schneier B. (2007) "Why 'Anonymous' Data Sometimes Isn't." *Wired.com*. Conde Nast Digital, 13 Dec. 2007. Online. Accessed on 01/02/2013. Available at: http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213

[35]Dilanian K. (2012) "A new brand of cyber security: hacking the hackers" in the *Los Angeles Times*. Journal. Online. Accessed on 21/01/2013. Available At: http://articles.latimes.com/2012/dec/04/business/la-fi-cyber-defense-20121204

[36]European Network and Information Security Agency (ENISA) (2012) *Give and Take: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime; Legal, Regulatory and Operational Factors Affecting CERT Cooperation with other Stakeholders*. European Network and Information Security Agency. Online. Accessed on 07/01/2013. p. 57

[37] Tierney J. (2008) "The Endless Fear of Terrorism." *Tierney Lab*. The New York Times, Online: Accessed on 02/02/2013. Available at: http://tierneylab.blogs.nytimes.com/2008/01/16/the-endless-fear-of-terrorism/

[38]*Ibid,* see also Dilanian K. (2012)

[39]Dilanian K. (2012)

[40]European Network and Information Security Agency (ENISA) (2012) "Give and Take…"

[41] World Economic Forum (WEF) (2012)

between private and public institutions that could be improved in an effort to strengthen trust and foster information sharing.

2. Suggestions to Overcome Real and Perceived Obstacles

In the previous section we identified that the three most common barriers to information sharing are: the lack of a perceived common mandate, concerns for data protection and a lack of inter-systemic trust. Now we will present the key suggestions to overcoming these obstacles. Our observations at this stage are entirely based on the literature reviewed, and each of the strategies we refer to can help overcome any of the three obstacles aforementioned in section 1. The findings reviewed can broadly be categorized into: (a) increasing the level of physical exchange between private and public organizations (b) the consolidation and simplification of legislation regarding data protection (c) equal accountability of the participating parties (d) symmetrical data flow between the participating parties (e) general awareness schemes that aim to promote a culture of cybersecurity and (f) the creation of personal data lockers.

a) Increasing the Level of Physical Exchange Between Public and Private Institutions

Several sources suggest that the physical exchange of personnel and the creation of working groups, that bring together members from private and public institutions, benefit the reinforcement (or *strengthening*) of trust between institutions. It is suggested that this exchange could come in a multitude of forms, from the creation of liaison posts and personnel exchange between private and public institutions, to interactive data-breach reporting forums to encourage individuals to partake in being vigilant[42]. The Netherlands, Germany, Poland and France are all countries that have created national-level physical exchange mechanisms between police forces and private institutions. Although it is clearly difficult to quantify the benefits that these mechanisms have rendered, the representatives involved in ENISA's study, *Give and Take: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime*, reported that the exchanges were vastly beneficial to encourage mutual trust and cooperation[43].

b) The Consolidation and Simplification of Legislation Regarding Data Protection

As mentioned in the first section, data protection concerns constitute a significant barrier to information sharing because they inhibit institutions from sharing information for fear of public backlash. It is widely agreed that simplifying the legislation concerning data protection could help ease concerns about privacy by removing some of the uncertainty that they carry. At present, companies struggle to assert what their role is in the protection of personal information, and to what extent the law allows them to share the information they have obtained[44]. For example, "mobile phone providers may have the right to track a user's location and call patterns to determine the cell tower that routes their calls and provide a better service", or to aid a criminal investigation; however, they may not be able to use the

[42]European Network and Information Security Agency (ENISA) (2012) "Give and Take…" See also McAfee (2011)
[43]*Ibid*
[44]*Ibid* p. 54

same data to market consumer-targeted products[45]. Because data acquires different meanings depending on the institutional context in which it is placed, the creation of standardized norms and best practices relating to each context becomes fundamental. These guidelines would ideally include a scale of possible threats and accompany these with the affiliated models of operation. It has also been suggested that the integration of legal council specialized in privacy law within companies of all sizes could have a strong beneficial impact on the willingness of private firms to share information with public regulators[46]. There are already some national and international initiatives that appear to be heading towards the simplification and consolidation of legislation relating to the uses of personal data. In the next chapter we will outline what these are and what criticisms they have received. In sum, recommendations that point to the simplification of data protection legislation, argue that less ambivalence as to one's legal standing with regards to its customers, will ease fears of social retribution and enable trust and a freer movement of information.

c) Equal Accountability of the Participating Parties

Symmetrical accountability of the parties involved in information sharing exercises was also broadly considered to render a positive impact on the success of information sharing mechanisms. Because of its intrinsic dependence on trust between the cooperating institutions, any form of sharing requires a base line accountability of the parties involved. It is argued diffusely that, where there is an established mechanism for information sharing, the liability for the protection of this information could be held by both the recipient and the lender. The liability of each party in the transaction would then be established on the basis of their use of the data and the sensitivity of the information involved[47]. Establishing this common liability, however, involves the potential prosecution of both public and private institutions alike[48], and attributing a value to a possible compromise of national security. Overall, those presenting the view that establishing similar liability for data protection upon both the public and the private agents in the information sharing exercise could help foster trust argue that prosecutors should promote the importance of generating trust within public-private communication.

d) Symmetrical Data Flow Between the Participating Parties

As mentioned in the first section, reluctance to share classified information, and a commitment to protect national security, can at times render the impression that information sharing only operates to the benefit of the public sector[49].

---

[45]World Economic Forum (WEF) (2012)
[46]European Network and Information Security Agency (ENISA) (2012) "Give and Take…"
[47]Techdirt (2012) "There Is A 'Right Way' To Do Cybersecurity Information Sharing, But CISPA Is Not It." *Techdirt.* Online. Accessed on 07/02/13. Available at: http://www.techdirt.com/articles/20120426/07560218668/there-is-right-way-to-do-cybersecurity-information-sharing-cispa-is-not-it.shtml
[48]European Network and Information Security Agency (ENISA) (2012) "Give and Take…" p. 57
[49]Rockvam, D. (2013) "Comment: Cybersecurity and Information Sharing Is a Two-way Street." *Infosecurity-Magazine*. Online, Accessed on 07/02/ 2013. Available at: http://www.infosecurity-magazine.com/view/27282/comment-cybersecurity-and-information-sharing-is-a-twoway-street/ , see also Deichler A. "AFP Fraudwatch: Information Sharing Key for Cybersecurity." *AFP Fraudwatch: Information Sharing Key for Cybersecurity*. Online. Accessed on 07/02/2013. Available at:http://www.afponline.org/pub/res/news/AFP_Fraudwatch__Information_Sharing_Key_for_Cybersecurity.html and European Network and Information Security Agency (ENISA) (2012) "Give and Take…"

The balancing of this asymmetric flow of information between public and private corporations is often referred to throughout literature as a positive enabler of trust and information sharing [50]. Those that support this position point to the strengthening of exclusively private information-sharing forums like the Red Sky Alliance and FS-ISAC[51] as evidence that the private sector is particularly enthusiastic about information sharing initiatives. Indeed ENISA also sustains that the "black hole" in which information shared with law enforcement seems to disappear, is a considerable hindrance to the process of information sharing[52]. Feedback on the uses of the information provided by the contributor is also strongly regarded as a means of installing trust and mutual cooperation because it provides a sense of collaboration and contribution towards a definite end[53].

e) General Awareness Schemes that Aim to Promote a Culture of Cybersecurity

With reference, again, to the notion of data protection, several contributors noted that the introduction of awareness campaigns that informed the public about national and international responses to cyber threats were largely beneficial to the establishment of information sharing[54]. The pillars of this argument are that greater awareness regarding information sharing mechanisms in place serves to ease tensions around data protection and reassures companies that their consumers support them in interactions with public institutions[55]. However, those that sustain this view also argue that we need to redefine how we measure public consent and approval for information sharing mechanisms. Consent is currently based on information gathered through the traditional notification-on-site models, which are effectively consent agreements that customers must agree to in order to progress to their desired web address. If consent were to be gathered using this format for all data sharing initiatives web surfers' experiences would likely be highly degraded and no greater awareness would reach the general public[56].Though, this last portion of the debate is beyond the scope of our analysis; the fact remains that increased awareness of ongoing information sharing mechanisms and cyber resilience plans are likely to reduce the anxieties regarding the protection of personal data which hinder private organizations from sharing information with public organizations.

f) The Creation of Personal Data Lockers

More than a suggestion to foster information sharing, this section presents an alternative that has recently gained significant popularity. The central theme is an attempt to overcome the concerns for data protection, which can inhibit private institutions from sharing information with their public counterparts.

This alternative to information sharing involves by-passing the role of private institutions in handling personal data and passing it directly back to the individual through data lockers.

---

[50] *Ibid*

[51] Deichler A. (2013) "AFP Fraudwatch: Information Sharing Key for Cybersecurity." *AFP Fraudwatch: Information Sharing Key for Cybersecurity*. Online. Accessed on: 07/02/2013. Available at:http://www.afponline.org/pub/res/news/AFP_Fraudwatch__Information_Sharing_Key_for_Cybersecurity.html

[52] European Network and Information Security Agency (ENISA) (2012) "Give and Take…" p. 54-57

[53] European Network and Information Security Agency (ENISA) (2012) "Give and Take…"

[54] *Ibid.*

[55] *Ibid* , see also World Economic Forum (WEF) (2012)

[56] *Ibid, s*ee in particular the mention of the experiment conducted by IAB Europe on the Dutch version of the European e-Privacy Directive.

Data Lockers are a mechanism that replaces organizations' control and analysis of data with a system wholly directed by the individual. It is argued that through these mechanisms individuals would be better able to manage and control how information about them is used and at the same time be able to support the programs they choose by endorsing them with their personal details[57]. Some organizations, like Connect.Me, DropBox and Mydex claim to already be offering these services. Furthermore, they are supported by organizations like Mydata, which encourage organizations holding large amounts of data to release the information they hold back to customers so they may store it at their own accord. These Data Lockers, by giving the individual control of his or her own data, also ensure that an individual gains a personal and direct interest in the security of that data. However, as mentioned above, this does not qualify as an improvement on existing mechanisms of information sharing. There is indeed a value to the notion that interest in the protection of personal data could be used to the advantage, rather than the disadvantage, of information sharing.

[57] *Ibid*

Chapter Two- Information Sharing and Legislation

Having highlighted those that are the open issues relating to mechanisms for information sharing, and having presented potential points of improvement, we will now turn to the legislative measures that affect the cooperation between public and private institutions. Our analysis will commence by analyzing the legislative framework at the international level, which will take into account initiatives coined by the United Nations, the Council of Europe and the European Union. The second section will instead present the different approaches that nation states have adopted to generate legislative measures that create and re-enforce mechanisms of cooperation. Though we dwell on the cases of Italy and the USA in more detail, this section is not intended to focus on the legislative framework of any given country, rather it is intended to evaluate the measures available to nations, at large, to generate a general culture of cyber resilience.

1. International Legislative Framework

a) United Nations

International cooperation is a key element in establishing effective cyber security strategies because of the liquidity and geographical complexity that characterizes cybercriminal activity. Any chance of creating a resilient defense to cyber-threats will inevitably involve the collection and analysis of information acrossborders, so to reveal trends that are not currently visible[58]. The United Nation's General Assembly (GA) has been raising this point, through various resolutions, for over a decade. In Resolution 55/63 of the 22 January 2001[59], the GA asserted its position along three key points, namely that: technological advancements have created new possibilities for criminal activity, that mutual assistance should ensure the timely investigation of the criminal misuse of information and recalling the Millennium Declaration, which was signed by Member States who thereby committed to ensure that the benefits of new technologies are available to all. This overall stance, that international cybersecurity efforts must complement and support the ongoing spread of technology, was reviewed and reinforced in Resolution 56/121 of 23 January 2002[60] where the GA renewed its call to "Member States" to "take into account their efforts to combat criminal misuse of information technologies". However, it was not until Resolution 57/52 of 30 of December 2002[61], that the GA broke from its previous policy of advocating self-monitoring for each member state to addressing the necessity of encouraging cooperation among states with a view to create a "global culture of cybersecurity". The first mention of collaboration between private and public institutions as a fundamental pillar to the creation of a sustainable form of cyber-resistance appears in Resolution 58/199 of 30of January 2004[62]; here it is stated that the Member States should take it upon themselves to "promote partnerships among stakeholder

[58]From European Network Security Agency (ENISA) (2012) *EU Cyber Cooperation: the Digital Frontline*. ENISA, Greece.Online. Accessed on 07/02/2013. Available at: http://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2012/eu-cyber-cooperation-the-digital-frontline
[59]UNGA Res 55/63 (22 January 2001) UN Doc A/RES/55/593
[60]UNGA Res 56/121 (23 January 2002) UN Doc A/RES/56/574
[61]UNGA Res 57/52 (30 December 2002) UN Doc A/RES/57/53

both private and public. To share and analyze critical infrastructure information in order to prevent, investigate and respond to damage to, or attacks on… infrastructure". The same Resolution also calls for international cooperation aimed at creating emergency response systems, suggesting a combination of national self-monitoring and adherence to homogeneous information sharing protocols only in extreme cases. This position was to be contrasted with the more recent Resolution 64/211 of 17 March 2010[63], which encouraged Member States and "relevant… international organizations", which could be both public or private, to share all best practices and measures that could assist other nations. The gradual shift in the stance of the GA with relation to cyber-policy can indeed be attributed to the spread of ICTs and the increasingly global nature of cyber-threats. The key point, however, is that regulation concerning ICTs almost invariably involves member states monitoring the upkeep of their own cybersecurity legislation and mechanisms of information sharing by actively engaging with the global systems of operation. However, it should be noted that these resolutions, though they provide a general understanding that information sharing ought to happen on an international scale, fail to enact an exact system of cooperation which addresses issues of privacy, trust and scope.

Outside of the United Nations General Assembly, theUnited Nations Interregional Crime and Justice Research Institute (UNICRI), United Nations Office on Drugs and Crime (UNODC), and the ITU, are all United Nations agencies concerned with generating and promoting best practice principles and international cooperation in the prevention and response to cyber-threats and cyber crime. UNICRI is particularly well-equipped to forge alliances between entities within the UN system, national governments, leading researchers, as well as NGOs and private entities, developing and implementing immediate responses to new global threats as soon as they emerge.

b) The Council of Europe

The Council of Europe's Convention on Cybercrime[64] is the only binding international instrument on the issue[65]. The convention tackles three main issues: the harmonization of terms and definition of cybercrime[66], guidance as to issues of jurisdiction and domestic powers[67], and measures for international cooperation[68]. The terms of the convention were agreed to by the forty-seven member states of the Council of Europe, Canada, Japan, the USA and the Republic of South Africa. In terms of information sharing, the Council of Europe's Convention on Cybercrime led to the establishment of a 24/7 Network[69] that calls for the creation of several Points of Contact for technical advice, which are available twenty-four hours a day, seven days a week. The creation of these networks was a key step in asserting the importance of information sharing at the international level.

c) The European Union

[63] UNGA Res 64/211 (17 March 2010) UN Doc A/RES/64/211

[64]Convention on Cybercrime and Protocol to the said Convention - Council of Europe Treaty Series No. 185-189 (2011)

[65]The Council of Europe (2001) *Cybercrime*.Council of Europe. Online. Accessed on 02/02/2013. Available at: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

[66]*Ibid,* see article 1-14

[67]*Ibid,* see article 14-25

[68]*Ibid,* see article 25-36

[69]*Ibid,* see article 35, this network is modeled on the ideas put forth by the G8 Sub Group on High-Tech Crime that established its own 24/7 Network in 1997.

The European Union, which by virtue of article 26 of the 'Consolidated Version of the Treaty on the Functioning of the European Union'[70], is concerned with establishing and maintaining the functioning of the internal market; thus, it is also directly concerned with all aspects of cyber threat resilience. As a union of nations,the EU is ideally positioned to create networks of cooperation between public and private stakeholders and to promote a system of information sharing that respects the interests of both entities. In recognition of this, the Council, Parliament and Commission have been active in implementing proposals that move toward the creation of a pan-European cyber-security strategy.

From the legislative point of view, the primary provisions dictated by the EU are: Regulation (EC) No 460/2004 and Council Resolution (2009/C 321/01)[71], which together define ENISA; the revised regulatory framework for electronic communications [72], which imposes a minimum standard for the security measures adopted by communications providers and data controllers [73]; and Directive 2008/114/EC [74] which outlines an overall approach to the protection of critical infrastructure, but "does not oblige operators to report significant breaches of security and does not set up mechanisms for the Member States to cooperate and respond to incidents"[75].

To further the European commitment to generating cybersecurity reliance mechanisms that can ensure the proper functioning of the internal market, theCommission has created three active working groups: the Information Society, Cert-EU, ENISA and the European Cybercrime Centre (EC3).

The Information Society, which runs the Critical Information Infrastructure Protection (CIIP) program, is responsible for devising an EU strategy for "a flourishing digital economy by 2020"[76]. The CIIP action plan involves close cooperation between the Commission and other monitoring bodies (ENISA and EC3) to tackle five pillars of cyber-threats: preparedness and prevention, detection and response, mitigation and recovery, international cooperation and criteria for European Critical Infrastructures in the field of ICT. The planned activities within these five pillars complement the European Program for Critical Infrastructure Protection (EPCIP) and the Council Directive on the identification and designation of European Critical Structures [77]. This said, the plan serves more as a general representation of the active engagement of the Commission in the fight against cybercrime. In actuality, most of the initiatives which it sponsors are conducted through vessels lead by ENISA.

---

[70]Consolidated Version of the Treaty on the Functioning of the European Union art. [26], 2008 O.J. C 115/47

[71]Council Resolution (2009/C 321/01) (EC) on a Collaborative European Approach to Network and Information Security [2009] OJ C 321/1 and Council Regulation (EC No 460/2004) establishing the European Network and Information Security Agency [2004] OJ L 077 P. 0001-0011

[72]Which includes five directives and one regulation, for more details refer to European Commission. (2012) *Regulatory framework for electronic communication in the EU* Online. Accessed on 02/02/2013. Available at: http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm

[73]See specifically, Art 13a and 13b of Council Directive 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services [2002] OJ L108/33

[74]Council Directive 2008/114/EC on the Identification and designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection [2008] OJ L345/75

[75]Commission Proposal for a Directive of he European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union [2013] SWD 31 final and SWD 32 final, COM(2013) 48 final.

[76]European Commission (2012) *Policy on Critical Information Infrastructure Protection (CIIP).*Online. Accessed on 02/02/2013. Available at: http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip

[77]Council Directive 2008/114/EC on the Identification and designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection [2008] OJ L345/75

ENISA is the European agency that has come the longest way in providing mechanisms for information sharing. By its current mandate[78], ENISA tackles barriers to information sharing by encouraging a homogeneous and simplified regime for "network and information security", "[encourage] economic growth and ensuring trust", "bridging the gap between technology and policy" and "encourage and improve multi-stakeholder models…which need to have a clear added value for benefiting end-users and industry". Crucially, these goals closely mimic best practices that we highlighted in the first chapter: simplification and homogenization of existing legislation, establishing clear liability structures, increasing the frequency of exchanges between private and public entities and ensuring that truly bilateral cooperation is taking place. In striving towards the enactment of these guidelines, ENISA has created several networks that facilitate information sharing between private and public entities. These can be divided into two categories. On one hand, it has developed projects that focus on how the collection of information and cooperation amongst private stakeholders needs to be strengthened, most notable of which are: the Industrial Control Systems- Supervisory Control Data Acquisition forum (ICS-SCADA), interconnected networks, mutual aid agreements and the creation of Computer Emergency Response Teams (CERTs). A notable CERT is the CERT-EU, which strives to support the European institutions to protect themselves again "intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU"[79]. On the other hand, they have conducted specific projects, which focus on the interaction between industry and government bodies by exploring the topics of information sharing and Public Private Partnerships (PPPs).

Closely related to our research scope, ENISA has produced several reports relating to Cybersecurity Information Sharing, Public and Private Partnerships and more recently on the cooperation between CERTs and Law Enforcement Agencies (LEAs)[80]. Together, these reports render a comprehensive list of obstacles to the cooperation between public and private institutions, which we summarized and categorized in the first chapter. What these reports do not include is how to apply the principles outlined to an evaluation of the existing information sharing systems and the relevant legislation that applies to them. It is our objective to add these analytical elements to the overall discussion on information sharing.

The strengthening of private partnerships is vastly beneficial to information sharing because it creates a more-or-less uniform set of interests and preoccupations that public bodies can then try to overcome. In this field, ENISA has conducted a number of interesting studies that we will introduce in this paragraph. The ICS-SCADA forum comprises a series of projects aimed at re-enforcing the remote control of critical infrastructures, such as power plants, transportation systems, oil refineries, chemical factories and manufacturing facilities[81]. The

[78]Council Resolution (2009/C 321/01) (EC) on a Collaborative European Approach to Network and Information Security [2009] OJ C 321/1

[79] CERT-EU. (2012) *Mission Statement.*CERT-EU News Monitor. Online. Accessed on 02/02/2013. Available at: http://cert.europa.eu/cert/plainedition/en/cert_about.html

[80]The primary reports include: European Network and Information Security Agency (ENISA) (2010*) Incentives & challenges for cyber security information sharing.*ENISA. Online. Accessed on 07/01/2013. Available at: http://www.enisa.europa.eu/media/press-releases/incentives-challenges-for-cyber-security-information-sharing-in-europe-identified, European Network Security Agency (ENISA) (2012) "National Cyber Security Strategies…",European Network and Information Security Agency (ENISA) (2012) "Give and Take…" ,European Network Security Agency (ENISA) (2012) EU Cyber Cooperation: the Digital Frontline. ENISA. Online. Accessed on 07/02/2013. Available at: http://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2012/eu-cyber-cooperation-the-digital-frontline, European Network Security Agency (ENISA) (2012) Cyber Europe 2012, Key Findings and Recommendations. ENISA Online. Accessed on 04\02\2013. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report

[81]European Network and Information Security Agency (ENISA) (2013) "Industrial Control Systems/SCADA".ENISA. Online. Accessed on 02/02/2013. Available at:

major stakeholders that these projects aim to involve are: major exponents of research and development in the field, providers of ICT security tools, ICT software and hardware manufacturers, infrastructure operators, public bodies which have an interest in the efficiency of these infrastructure and standardization bodies. The interconnected network studies that ENISA has undertaken relate mostly to the way in whichInternet service providers (ISPs) and network operators interact. In this field, ENISA has involved stakeholders like data centers, network operations centers, cabling infrastructure, router/switches operators, and management and monitoring services in its studies. The main focus of the interconnected network studies was to devise how to create a network ecosystem which is resilient in the face of threats and challenges. The two main reports produced in this field are the *Inter-X: Resilience of the Internet Interconnection Ecosystem* and the *Resilience of Internet Interconnections* study[82]. The Mutual Aid Agreement (MAA), to which we owe the *Mutual Aid for Resilient Infrastructure in Europe (MARIE)*[83]report, seeks to establish the characteristics of successful mutual aid agreements between critical infrastructure stakeholders to increase their response to challenges and threats. The greatest of ENISA's achievements in generating a structured resilience to potential threats for the benefit of the industry and the internal market was the establishment of CERTs across Europe. CERTs, which are supported by the central agency but are for all intensive purposes independent, offer a more-or-less united set of interests representative of all thestakeholders and consequently facilitate prospects of information sharing. Although they do not directly address the additional conundrums of public-private interaction, all of these studies provide an excellent depiction of the issues that are raised by information sharing and incident reporting within specific industries, and comparing them can be instrumental in deciphering how instances of regulation, trust and privacy concerns play out in practical interactions.

To test the results of the aforementioned studies, ENISA put in action a series of national and international exercises in which various networks were employed to collaborate and remedy a staged crisis. Cyber Europe 2010 and Cyber Europe 2012 tested response mechanisms to fictional Distributed Denial of Service Attacks (DDoS) against public and private electronic services across Europe, with a focus on e-government and e-finance systems[84]. Similarly, a Cyber Atlantic exercise was organized by the EU-US Working Group on Cybersecurity and Cybercrime comprised of ENISA and the Department of Homeland Security that was established as a result of the EU-US Summit of 2010. Although the exercise in this case was more politically focused, it proved useful to the understanding of the international dimension of information sharing and the potential issues it may raise[85].

To aid and reinforce the work conducted by ENISA, and to handle the deterrence and law enforcement elements of cybercrime, Europol has launched the EC3, which was first proposed in the Commission's *EU Internal Security Strategy in Action*[86]. The center is

---

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/industrial-control-systems#_ftnref1

[82]European Network and Information Security Agency (ENISA) (2013) "Internet Interconnections".ENISA. Online. Accessed on 02/02/2013. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x

[83]European Network and Information Security Agency (ENISA) (2013) "Mutual Aid for Resilience in Europe". ENISA. Online. Accessed on 02/02/2013. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance

[84]European Network Security Agency (ENISA) (2012) "Cyber Europe 2012…"

[85]European Network Security Agency (ENISA) (2012) "Cyber Atlantic 2011".ENISA. Online. Accessed on 04/02/2013. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic/cyber-atlantic-2011

[86]MEMO/12/221 see European Commission (2012) *European Cybercrime Centre (EC3) opens on 11 January. EC* IP/13/13. Online. Accessed on 02/02/2013. Available at: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

expected to work closely with ENISA and is likely to be hugely influential in the consolidation and harmonization of European affairs. However, the full collaboration of the CERTs with the new law enforcement body is dependent on their ability to promote trust between each other in their operations. The center is not expected to be fully operational until 2015[87], andtherefore it is not yet possible to assert how prepared it will be to partake in bilateral mechanisms of information sharing.

In February 2013, following much debate, the Commission launched an official proposal for a Directive 'concerning measures to ensure a high common level of network and information security across the Union'[88]. Overall, the proposed directive imposes upon "market operators and public administrators" a "procedure for the provision of information in the field of technical standards and regulations and that of rules on Information Society Services"[89]. The Commission has sustained that such measures ought to be implemented through a regulatory framework to "improve the protection of EU consumers, business and governments against [network and information security] NIS incidents. In particular, the obligations placed on the Member States would ensure adequate preparedness at national level and would contribute to a climate of mutual trust, which is a precondition for effective cooperation at EU level". Furthermore, it claims that a regulatory framework is the only way of providing a strong enough incentive for public administrators and other public actors to manage security risks effectively and in a transparent manner[90].

The Directive specifies that "to ensure transparency and properly inform EU citizens and market operators, the competent authorities should set up a common website to publish non-confidential information on the incidents and risks"[91] .Considering the extent of the concerns surrounding privacy and the data mining operations discussed in the previous chapter, it is unsurprising that the directive has caused a significant amount of controversy. That said, it is reiterated throughout the directive that "the exchange of sensitive and confidential information", and the publishing of data, "shall take place through secure infrastructure"[92]. Furthermore, it is considered that to ensure privacy, data haveto be better and more centrally controlled, which will always imply trust to be given to a third party agent[93]. Within the Directive it is also mentioned that a form of cooperation whereby "the competent authorities… shall provide early warnings within the cooperation network on those risks and incidents that fulfill at least one of the following criteria: (a) they grow rapidly or may grow rapidly in scale (b) they exceed or may exceed national response capacity (c) they affect or may effect more than one member state"[94]. Though this statement intends to place a positive incentive for private stakeholders to share their data, it does not appear thorough enough to match those sentiments widely expressed in the literature that arecalling for a type of bilateral cooperation within the limits of national security[95]. The fact that the Directive fails to present sanctions and liabilities for institutional failures to protect the security network also stands in sharp contrast with the views expressed by experts, who call for more concrete assurances that the information shared would be kept safe.

---

[87] *Ibid*
[88] *Ibid*
[89] *Ibid,* p.24 and Art. 1 (2c)
[90] Commission Proposal for a Directive of he European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union [2013] SWD 31 final and SWD 32 final, COM(2013) 48 final. See the Impact Assessment on p 7-8
[91] *Ibid,* p. 13-16
[92] *Ibid,*Art. 9
[93] Humphreys S. (2011) *Navigating the Dataverse: Privacy, Technology, Human Rights*. International Council on Humans Rights Policy, 2011. Print.
[94] *Ibid,* Art. 10
[95] See chapter 1

Broadly, those who have supportedDirective have argued that people must be able to turn to a reliable system of information sharing, which inspires trust and confidence "that new technologies, such as cloud computing, are safe"[96]. The Directive has therefore been perceived as an incentive for "private companies to improve their track records in network security and help national governments" to improve overall cybersecurity infrastructure[97]. Those who have opposed the legislation have instead argued that the voluntary approach to information sharing, encouraged by incentives and increased mechanisms for generating trust, would be more effective than the centralization of data input because (a) the centralization of data input could overreach the separation of powers between intelligence services and the police[98]; (b) there is no assurance that the public information collection can operate efficiently; (c) perceptions of privacy are not universal or homogenized[99].

In the end, however, the NIS Directive was successfully adopted by the European Parliament, albeit in an amended form, on March 13, 2014.[100] The measure passed overwhelmingly, with 521 members voting in favor, 22 against, and 25 abstaining. The amended version has significantly weakened the reporting and regulatory frameworks proposed in the original directive of the Commission. For example, in the Parliament's version, major market operators, including social networks, search engines, cloud computing services, application stores, e-commerce platforms, and internet payment gateways are not subject to regulation.[101] The final text of the Directive is now set to be negotiated between the Parliament and the Council of the EU, with the hope that a final version will be in force by the end of 2014.

2. National Level Policy Making

Having observed the way in which the international communityis taking action to counter cyber-threats and create networks of resilience, our attention will now switch to the action taken at the National Level. Across the globe, governments are mobilizing to create their own legislative frameworks to counter and prevent cyber-emergencies[102]. Though these are not

[96]NeelieKroes, EU Commissioner for the Digital Agenda of Europe, from European Electronic Crime Task Force (2012) *Cybernews*. Year III Number 11; Journal, Print. November 2012.
[97]Infosecurity-Magazine (2013) "New EU Cyber Security Directive (a European CISPA) Expected within Weeks." Infosecurity Magazine, 22 Jan. 2013. Online, Accessed on 7/02/ 2013. Available at:http://www.infosecurity-magazine.com/view/30351/new-eu-cyber-security-directive-a-european-cispa-expected-within-weeks/
[98]*Ibid.*
[99]WEF and the Boston Consulting Group (2012*) Rethinking Personal Data: Strengthening Trust*. WEF. Online. Accessed on 28/01/2013. Available at: http://www.weforum.org/reports/rethinking-personal-data-strengthening-trust
[100] EU Commission – STATEMENT/14/68, "Great news for cybersecurity in the EU: The EP successfully votes through the Network and Information Security (NIS) directive." *European Commission*. Online. Accessed on 02/05/2014. Available at: http://europa.eu/rapid/press-release_STATEMENT-14-68_en.htm
[101]European Parliament legislative resolution of 13 March 2014 on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)) (Ordinary legislative procedure: first reading). Accessed on 02/05/2014. *European Parliament*. Online. Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//EN&language=EN
[102]NTV Uguanda (2013) "Ugandan Govt Unit to Fight Cyber Crime." *AllAfrica*. Online. Accessed on 22/02/2013. Available at: http://allafrica.com/view/resource/main/main/id/00060212.html , SC Magazine (2013) "Infosecurity Europe Preview 2013." *SC Magazine UK*. Online. Accessed on 23/02/2013. Available at http://www.scmagazineuk.com/infosecurity-europe-preview-2013/article/281280/ , The White House (2013) "Executive Order - Improving Critical Infrastructure Cybersecurity." *The White House*. Online. Accessed on

necessarily aimed at creating information sharing mechanisms *per se*, they always involve the creation of cyber security resilience structures that will encourage cooperation between public and private stakeholders. Securing cybersphere is a process that can be more problematic at the national level than at the international level; this is mostly due to two factors. Firstly, it involves a variety of areas of National law to be reformed or adapted[103]. Secondly, the widespread public concern for all affairs that may involve personal data often stunts national governments that are concerned with positive polls. A report produced by the NATO Cooperative Cyber Defense Center of Excellence states it best, "citizens that are happy to allow their government to decide how to combat terrorists or negotiate with neighbors can be easily enraged if they feel their own personal computer, their personal information or access to favorite social media sites is put at risk without their consent"[104].

Different governments have responded very differently to these difficulties and have taken widely different approaches to producing legislative frameworks to monitor the cybersphere. France and the United Kingdom, for example, have both adopted what can be defined as "top-down" approaches. This means that the central governments have kept particularly tight control over the content and communication of their national cyber security strategies and have established select committees charged with clear mandates to devise regulatory proposals[105]. On the other hand, Germany and the Netherlands have devised more "societal approaches" to the creation of their national cybersecurity policy-making by appointing prominent members of the private sector and the hacker community to the relevant committees[106]. Each of these models has its own advantages; policy created behind 'closed doors' is likely to generate a more streamlined set of policies.However, the 'open' model is more likely to produce material that will pass the legislative process and will be accepted within civil society.

The United States, as the first country to attempt to develop a national cyber security system, has tried both approaches mentioned above. In the development of the National Strategy to Secure Cyberspace, the White House undertook a wholly inclusive approach working with private experts and technology consultants[107]. However, the terms of the policies constructed collaboratively were soon deemed inefficient, and the US has since adopted a top-down approach[108]. By adopting this approach the government has put forth several controversial proposals like the Comprehensive National Cybersecurity Initiative (CNCI) and the Cyber Intelligence and Protection Act (CISPA)[109], neither of which have yet been fully implemented. More recently, US President Barack Obama signed an executive order aimed at improving critical infrastructure security. Similar to CISPA, the order allows for breaches of cyber systems and other detected threats to ICTs to be reported to a central agency; however, unlike its predecessor, it creates a mechanism for the government to share classified information

---

20/02/2013. Available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[103] International Telecommunications Union (2012) *Understanding Cybercrime: Phenomena Challenges and Legal Response.* ITU. Online. Accessed on 25/01/2013. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

104Klimburg A (2012)

[105]*Ibid.* p. 89-95

[106]The Dutch model is commonly known as the 'polder' model. *Ibid.*

[107]*Ibid*

[108]*Ibid*

[109] For more detailed information relating to the acts see The White House (2010) "The Comprehensive National Cybersecurity Initiative." *The White House*. Online. Accessed on 22/02/2013. Available at: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative and Sheets C. A.(2012) "What Is CISPA 2012? Inside The Bill That Has Internet Privacy Advocates Up In Arms." *International Business Times*. Online. Accessed on 22/02/2013.Available at: http://www.ibtimes.com/what-cispa-2012-inside-bill-has-internet-privacy-advocates-arms-693333

with critical infrastructure companies[110]. In effect, widespread support for the executive order[111], combined with the failure of the much disputed CISPA, are signs that progressive policy making must incorporate the views of private actors when assessing national cyber security strategies.

Similar to that of the US, the current state of Network and Information Security (NIS) in Italy is a system that combines a bottom-up and top-down approach to NIS policy. Operating at a legislative level, there are: the data protection code[112], the legislative decree on Electronic Commerce[113], the Electronic Communication Code[114]and the integration of the Criminal Code and the Criminal Procedure Code involving Cyber Crime[115]. In terms of information sharing, this legal landscape sets obligations to monitor NIS and hire qualified personnel to ensure that these security systems are maintained and updated. Notably, however, the current landscape does not present the obligation to disclose security breaches[116]. Through the legal powers created by this legislative framework, a wide variety of public institutions are tasked with the prosecution and prevention of cybercriminal activity, among these are: the Postal Police, the National Technical Committee on Cyber Security, the Network Security and Communications Protection Observatory and the Personal Data Protection Authority. These authorities operate by creating their own information sharing mechanisms in conjunction with prominent partnersfrom the private sector. There are various examples of these modes of cooperation; the Italian State Police has a network called National Anti-Cyber-Crime Center for the Protection of Critical Infrastructures (*Centro NazionaleAnticrimineInformatico per la ProtezionedelleInfrastruttureCritiche, CNAIPIC*) that serves to connect various public and private agents in a constant exchange of data[117]. Another form of non-institutionalized information sharing can be found in the alliance forged between the Postal Police and Facebook in 2010. This information sharing mechanism has strived to help build a system of rules to discourage people from creating false identities and engaging in online criminal behavior. This type of voluntary cooperation is widely accepted as a functional method of cyber-resilience; however, not being a centrally controlled activity makes it difficult to be accountable on an international level. With the objective of rectifying this issue of accountability, Mario Monti, the formerPrime Minister of Italy, issued a legislative decree that

[110]The proposed CISPA would have allowed private companies to share otherwise personal information with the government. See Magid L. (2012) "What Is CISPA And Why Would The President Veto It?" *Forbes*. Forbes Magazine, 25 Apr. 2012. Accessed on 22/02/2013. Available at: http://www.forbes.com/sites/larrymagid/2012/04/25/what-is-cispa-and-why-would-the-president-veto-it/2/ , Albanesius C. (2013) "Obama's Cybersecurity Executive Order vs. CISPA: Which Approach Is Best?" *PCMAG*. Online. Accessed on 22/02/2013. Available at: http://www.pcmag.com/article2/0%2C2817%2C2415380%2C00.asp and Financial Times (2013) "US Cyber Security Executive Order Falls Short for the Private Sector." *Financial Times*. Online. Accessed on 22/02/2013. Available at: http://www.ft.com/intl/cms/s/0/fe33ef2e-778b-11e2-9e6e-00144feabdc0.html

[111]Magid L. (2013) "Privacy Advocates Prefer Obama's Cybersecurity Plan Over CISPA." Forbes. Forbes Magazine, 21 Feb. 2013. Online. Accessed on 22/02/2013. Available at:http://www.forbes.com/sites/larrymagid/2013/02/21/privacy-advocates-prefer-obamas-cybersecurity-plan-over-cispa/

[112] Italian Data Protection Code Legislative Decree no. 196 of 30 June 2003

[113]Italian Legislative Decree on Electronic Commerce, Legislative Decree no. 70 of 9 April 2003

[114] ItalianElectronic Communications Code, Legislative Decree no. 259 of 1 August 2003

[115]Italian integration of the Criminal Code and the Criminal Procedure Code involving Cyber Crime, Act nº 547 of 13 December 1993

[116]European Network Security Agency (ENISA) (2011) *Italy Country Report.*ENISA. Available at: http://www.enisa.europa.eu/activities/stakeholder-relations/country-reports

[117] Polizia Dello Stato. CNAIPIC - Centro Nazionale Anticrimine Informatico per La Protezione Delle InfrastruttureCritiche. Polizia Dello Stato. Online. Accessed on:11/06/2014. Availableat: http://www.poliziadistato.it/articolo/23401/

promotes a more centralized public focus for cybersecurity from which all cooperation agreements with the private sector ought to stem[118].

In regard to Italy, progress on the issue has been made, but of course there is still a long road ahead. In December 2013, the Presidency of the Council of Ministers of Italy published a report entitled, the "National Strategic Framework for Cyberspace Security." The document identifies and offers a comprehensive approach to tackling a range of cyber issues placed into the categories of cybercrime, cyber espionage, cyber terrorism, and cyber warfare. Among its multiple strategies for tackling these issues, the report highlights promoting international cooperation and the creation of public-private partnerships as key objectives.

The reason why there are no traces of legislation specifically defining modalities of information sharing at the national level is that there is not, at present, unity of purpose across levels and types of jurisdictions[119]. For example, whilst it may be possible to create legislation concerning information sharing between critical infrastructure providers and the government[120], it might be more difficult to regulate (or justify the regulation)the exchange with medium range producers like software companies. In light of (a) the asymmetry of the private individual, corporate and public interests in NIS and (b) the influence of private concerns on the success of NIS policy, it becomes clear that it is vital that governments work towards creating a commitment to civil-cyber-security before they consider passing legislation regulating information sharing.

Evidence provided by the European Commission[121] suggests that 72% of Europeans are concerned that private websites do not handle their private information safely, whilst 66% share concerns that their information is not being handled properly by public authorities. These figures are highly symbolic of the lack of transparency and knowledge that exist about the security systems that are in place throughout Europe. Before hoping to implement legislative frameworks for information sharing, governments must look to tackle this deficit in knowledge and information.

For European Member States, ENISA has created a model compilation of instructive tools which can be adapted to different cultural settings to raise awareness about the threats and policies relating to cybersecurity and the way it operates[122]. For example, the appropriately named "Cyber Security Month" was comprised of a series initiatives developed through TV and radio ads, social media campaigns and quizzes, news articles, conferences and student events. The countries thatparticipated in the project in October 2012 were the Czech Republic, Luxembourg, Norway, Portugal, Romania, Slovenia, Spain and the United Kingdom. Although it may bestill too early to evaluate the full extent of the benefits for building a legislative framework, these initiatives were certainly popular[123]. A similar initiative in the US, also appropriately name "Cyber Security Month", was organized by the Department of Homeland Security in collaboration with the National Cyber Security Alliance and the Multi-

[118]ANSA (2013) Monti Vara Decreto per Strategia Sicurezza Informatica. *PRIM*A 24/01/2013. Online, Accessed on 05/02/2013. Available at: http://www.primaonline.it/2013/01/24/113475/monti-vara-decreto-per-strategia-sicurezza-informatica/

[119]Klimburg A. (2012)

[120]Such as the one proposed by the executive order.

[121]TNS Opinion & Social (2012)*Cyber Security Reports- Special Eurobarometer 390/wave EB77.2* at the request of the European Commission, Directorate-General Home Affairs. Online. Accessed on 02/02/2013. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

[122]European Network Security Agency (ENISA) (2012) "EU Cyber Cooperation"

[123]European Network and Information Security Agency (ENISA) (2012) *European Cyber Security Month.* ENISA. Online. Accessed on 02/02/2013. Available at:.http://www.enisa.europa.eu/activities/cert/security-month

State Information Sharing and Analysis Center[124]. In Italy, there are several campaigns aimed at promoting secure Internet usage; however, there are not yet any directed at explaining cyber security mechanisms or introducing information sharing into the public sphere[125].

Overall, the observations regarding national level policy frameworks for information sharing are that

- they face considerable challenges given their dependence on public scrutiny;
- neither a top-down model, or a bottom-up model of policy formation has been particularly instrumental in establishing a legal framework for information sharing;
- widespread ignorance of how cybersecurity mechanisms operate is a hindrance to the formation of national legislation.

These realities of Information Sharing at the national level stand in stark contrast to those observed at the international level (particularly with regard to the proposed EU Directive), which appear to project a somewhat premature account for the potential of centralization without offering enough consideration to the need for leveling the asymmetries in the communication of cybersecurity operations.

[124]Department of Homeland Security (2012) *National Cyber Security Awareness Month*.Department of Homeland Security. Online. Accessed on 22/02/2013. Available at: http://www.dhs.gov/national-cyber-security-awareness-month

[125]European Network and Information Security Agency (ENISA) (2011) "Italy Country Report"

Chapter Three- Information sharing and current good practices

As outlined in the Introduction, the term "information sharing" is hereby understood as the collaboration between private and public institutions and is considered to be mutually beneficial and an overall best practice in dealing with cyber-threats. However, through a literature review, we have identified three major obstacles to the development of a smooth process of information sharing between private and public entities: the different mandates and legal capacities held by private and public entities; the anxiety deriving from the blurred nature of the meaning and legislation regarding data protection; the lack of trust existing between public and private entities, as well as individual citizens. Accordingly, we have also pointed out some possible suggestions to overcome these real and perceived obstacles: increasing the level of physical exchange of personnel between public and private institutions; consolidating and simplifying the legislation regarding data protection; allowing equal accountability amongst the participating parties; ensuring a symmetrical data flow between participants; promoting general awareness schemes aimed at furthering a culture of cyber-security.

Following on from these considerations, the aim of the chapter is that of comparing several initiatives of information sharing currently in place in order to identify patterns of good practice and detect those aspects that still need improving. We hereby took into consideration nineteen initiatives of information sharing worldwide, aggregating publicly available information:

1. Warning Advice Reporting Point (WARP);
2. Trust Digital Life (TGL);
3. European Public Private Partnership on Resilience (EP3R);
4. PresidioInternet ABI Lab;
5. European Financial Institutions Information Sharing and Analysis Centre (EU FI-ISAC);
6. US Financial Services Information Sharing and Analysis Center (FS-ISAC);
7. Digital Crimes Consortium (DCC);
8. Anti-Phishing Working Group - Internet Policy Committee (APWG-IPC);
9. European Banking Federation IT Fraud Working Group (EBF - IT Fraud WG);
10. FI-ISAC Netherlands (FI-ISAC.NL)
11. Task Force-Computer Security and Incident Response Teams (TF-CSIRT);
12. International Watch and Warning Network (IWWN);
13. Advanced Cyber Defence Center (ACDC);
14. Cyber Security Information Sharing Partnership (CSISP);
15. Initiative for Cyber Security Information Sharing Partnership of Japan (J-CSIP);
16. European Payments Council (EPC);
17. Multi-State Information Sharing and Analysis Center (MS-ISAC);
18. **European Electronic Crime Task Force (EECTF)**;
19. **Online Fraud Cyber Centre and Experts Network (OF2CEN)**.

The first part of the chapter will compare these different initiatives on the basis of thirty-one parameters ranging from the date of birth of the initiative and its objectives, to its promoter(s), its constituency and the tools used to exchange information. Such parameters can be grouped

into five macro parameters: references; content; governance; processes/ methodology of information sharing; and modus operandi. During this comparison phase we will draw attention to some positive as well as negative trends in the establishment of good practices of information sharing. The chapter will then conclude with a specific focus on two of these initiatives: EECTF and OF2CEN, which report trends that could be particularly positive in the establishment of beneficial standards of good practice for information sharing.

In terms of the macro-parameter of 'references,' the only observable trend, albeit not applicable to all cases, concerns the relationship between the parameter 'date of commencement' and the type of service offered by the initiative. For instance, the example of OF2CEN, whichas of November 2013 is the most recent initiative analyzed in the table, highlights that the nature of information offered by information sharing initiatives is changing.Early examples of information sharing initiatives focused on raw information and began by distributing them from their collection phase (classical intelligence cycle: collection, analysis, decision, dissemination), thuswasting the time and energy of the participating parties who had to filter and analyze information themselves. Instead, nowadays the trend is changing in order to meet the increasing demand for bulk information, already processed and ready to be utilized. Indeed, OF2CEN, for instance, offers a customized interface for each participant that is tailored to their activity and information needs. It offers valuable data analysis and it enables timely warnings and real-time statistics about fraudulent transactions.

When considering the second macro parameter used in the table named 'content', one of the first considerations that can be deduced refers to the parameter 'number of members'. One-size-fits-all is certainly not an applicable rule to the initiatives of information sharing that have hitherto been taken into account. Indeed, it goes without saying that the size of the initiatives varies greatly depending mainly on their aims, their promoter and the type of information shared.For example, FI-ISAC.NL, a national initiative of the Dutch National Cyber Security Centre aimed at supporting incident response, sharing lessons learned and developing and offering joint services, counts thirteen members. Alternatively, DCC, an initiative promoted by Microsoft with the aim of enhancing connections and relationships across various agencies and organizations worldwide needed to fight digital crime, is the largest among all initiatives, with over 3000 professionals involved. Clearly, if the group is kept small, trust can be ensured more easily, but circulation of knowledge might be limited.Therefore, mechanisms to include general knowledge sharing at an informational level are advisable, finding thus the proper trade-off between trust and competency. In some initiatives, such as the EECTF, this is dealt with via 2-level (or more) differentiated participation by Members.

Moreover, a comparison amongst the 'missions', 'objectives' and 'information shared' of the different initiatives highlights that each case retainsits own individual characteristics. For instance, the aim of the APWG-IPC initiative(i.e. unifying the global response to cyber crime), its long-term objectives and the types of information shared greatly differ from the more specifically security-targeted mission, objectives and types of information shared in the TF-CSIRT initiative. This is especially true for the even more specific aims, objectives, and types of information shared in FI-ISAC, an initiative exclusively targeting banking and financial services. Moreover, the financial sector appears to be one of the more active promoters of information sharing activities, and this fact is hardly surprising if we consider that the financial/ banking context is where cyber crime developed first and grew fastest. However, it can be noted that the vast majority of the initiatives share the primary or implicit aim of facilitating collaboration and coordination among their members, encouraging the development of effective mechanisms of information sharing and promoting the adoption of

good cyber resilience practices. Therefore, it is evident that the need of establishing good practices of information sharing is a tangible reality and not a mere academic speculation.

Moving on to the macro parameter of 'governance', a comparison between the 'promoters' of the various initiatives highlights that eight out of nineteen are public bodies, six are international bodies (ENISA holding a leading role as a promoter of information sharing initiatives) and five are instead private entities. This relatively balanced picture shows that, despite the difficulties and obstacles existing in the process of information sharing, all three types of actors are conferring great value on these types of initiatives, marking thus the prominent role of information sharing in developing a culture of cyber-security. This remark is further highlighted when observing the 'sponsorship/patronage' parameter. Indeed, it can be noted that almost all activities (the exceptions being DCC, APWG) have at least one sponsorship or patronage. In addition, it is noticeable that sponsorship and patronage are mainly offered by international/ transnational actors. This trend underlines how, as the Director of Europol Rob Wainwright remarked, international cooperation is a crucial ingredient in the establishment of a culture of cyber-resilience that is able to effectively tackle the borderless nature of cyber crimes[126].

Moreover, when looking at the parameters relative to the 'constituency' of the initiatives, it emerges that the vast majority of them are a mixture between private and public entities, with just three being fully private (EPC; EBF; FS-ISAC) and two fully public (IWWN; MS-ISAC).This trend highlights the importance of complementary qualities and the deficiencies of the private and public entities.As seen in Chapter 1, private and public mandates may often appear to be in severe contradiction to one another; however, closely examining the pros and cons of each type reveals a profitable complimentary relationship. For instance, in a private/public partnership the timely and more efficient nature of the services requested by private mandates, and their usually more extensive financial means, could notably mitigate the shortcomings that might arise due to the lengthily bureaucratic processes and limited financial means of public mandates. However, the capacity of public entities to offer timely and efficient resolutions to imminent threats often hides a lack of a long term vision and a focus on legal questions and challenges. From this point of view, thelaw-abiding methodsof collecting evidence of public mandates and their focus on the legislative and law enforcement aspects of cyber-security can greatly complement private entities' flaws. As previously noted, there is a general urgency to consolidate the legislation regarding privacy and information sharing, and thus the importance of creating long-term legal objectives is as important for private entities as it is for public bodies involved in information sharing.

Remaining within the macro parameters of 'governance' and looking at the parameters of 'international law/regulation' and 'national law/regulation', it is striking that just one initiative is supported by an international regulation (EP3R)[127] and just two by a national official provision (CISP;J-CSIP)[128]. Indeed, most of the initiatives were createdthrough a private party agreement with public bodies, as a PPP program, with no specific decrees or regulations acting as a basis. These findings are quite revealing if we consider that one of the main obstacles to information sharing is indeed the lack of clear regulations and the confusing

[126]Europol (2011).
[127] Policy initiative adopted by the European Commission COM(2009)149 relative to the Critical Information Infrastructure Protection (CIIP) program run by the Information Society. For further information on EU regulations see pp. 16-20.
[128] UK Cabinet Office (2013) *Government launches information sharing partnership on cyber security*. Cabinet Office. Online. Accessed on 12/02/2014. Available at:https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security

and evasive nature of privacy legislation. The consolidation and simplification of legislation regarding data protection has, in fact, been identified as a catalyst in the overcoming of real and perceived obstacles to information sharing. Therefore, the overall remark is that there is a substantial lack of good practice in this respect.

However, the development of unambiguous laws and regulations concerning information sharing and data protection does not come without hindrances. Acting as part of a vicious cycle, the cultural sensitivity surrounding data protection acts as a powerful obstacle to the development of less ambiguous and more systematic public and international laws and regulations; in return, the confusing nature of privacy legislation and information sharing regulations intensifies the general worry regarding data protection. Therefore,it is highly advisable to accompany effortsaimed at simplifying and consolidating the legislation of data protection with the creation of general awareness schemes. Such schemes should be focused on explaining the risks of cyber attacks, cyber security mechanisms, introducing the importance of information sharing and reassuring citizens/customers on how their personal data would be handled. In fact, operational information is mostly shared where LEAs are actively involved in the community.

At present, principal awareness campaigns have been promoted by international and public actors[129]. However, the existing examples point out that the development of good practice in this field is still in an embryonic stage and that it needs wider and deeper consolidation. Ideally, awareness schemes should be carried forward by the private as well as the public parties involved in information sharing. Such collaboration would first of all constitute an additional chance for private and public participants to exchange different expertise and knowledge, thus resulting in awareness campaigns that have been thoroughly designed and adequately financed and are then capable of ensuring optimum community impact. Moreover, establishing a partnership in this field could increase the level of exchange between private and public personnel and, therefore, indirectly have a positive influence on the establishment of mutual trust, which is indeed considered to be one of the major obstacles to the development of effective mechanisms of information sharing.

Moving on to the parameters of ‘agreements’, ‘organizational structure’ and ‘engagement’, the general observations are that the vast majority of initiatives presuppose formal agreements between members, and are characterized by formal organizational structures. Moreover, just two initiatives (J-CSIP and MS-ISAC) have free access on a voluntary basis, and all initiatives are sustained by a formal subscription procedure with the sole exception of the DCC. In most of the cases,in fact, participation is allowed on an invitation-only basis, and formalization is required.However, no economic contribution is asked and the exchange is voluntary.

The last remark concerning the macro parameter of ‘governance’ refers to the findings emerging from the comparison of the initiatives within the parameters of ‘anonymization’ and ‘trust’. Six initiatives guarantee anonymity and seven do not. Moreover, six are characterized by a centralized all-trust-one mechanism and nine report distributed all-trust-all mechanisms. Hence, the picture highlights that the overall practice may be slowly moving towards an equal accountability of the participant parties and perhaps an increased level of transparency. In turn this trend could positively influence the lack of trust between public and private parties. Nonetheless, as stressed by these relative balanced data, the development of a good practice of transparency and mutual accountability still appears to be a weak and reversible trend.

[129]See ENISA and US initiatives pp.23-24

In scrutinizing the macro parameter 'processes/methodology of information sharing' we note that the initiatives report several similarities: they are all characterized by an individually defined process to share information, and eleven initiatives are characterized by specifically designed mutual methodologies to classify information. However, the most interesting trends are identified after shifting attention to the macro parameter 'modus operandi' and comparing the parameter of 'tools for information sharing' with that of 'physical meetings'. While twelve initiatives require physical meetings at least once a year, just four presuppose face-to-face meetings to share information in addition to the usual tools of mailing lists, web platforms and conference calls. This suggests that if it is true that many of the public and private entities involved in information sharing initiatives are meeting on a annual basis, there is no remarkable physical exchange between public and private institutions when it comes to activities of concrete information sharing. As seen in the first chapter, increasing the physical exchange of personnel would greatly benefit the reinforcement of mutual trust between private and public institutions and allow smoother processes of information sharing. Consequently, while the actual process of sharing information cannot be sustained through physical meetings (for obvious reasons of technical, geographical, timing and budgetary obstacles),it remains highly advisable to promote more frequent meetings between the personnel involved in these initiatives.

Case study: EECTF

European Electronic Crime Task Force (EECTF)

The EECTF is an information sharing initiative founded in 2009 by an agreement between Poste Italiane, the United States Secret Service and the Italian Ministry for Internal Affairs.

EECTF's mission isto promote the sharing of information and analyses of best practices against Cyber Crime in European countries through a strategic alliance between LEAs, academia, legal, and private sector entities.
Such a goal is pursued through three main lines of activities: analysis of the current scenario; cross-sector networking between peers; and the development of suitable communication initiatives. The EECTF started as a closed three-party cooperative, but after one year and a half it allowed for the participation of other entities, giving birth to a collective information sharing initiative.
The EECTF Modus Operandi relays today on three different layers of operational involvement, which imply differentiated tasks and levels of contribution:

- the Founder Members, chaired by Poste Italiane, steer the activities and define strategic goals;
- the Permanent Members, organizations who voluntarily committed to the development of the EECTF via a formal subscription to a MoU, who take part in the initiatives activated by the EECTF and periodically gather in closed-door meetings where technical information on ongoing attacks or recent investigations are shared and countermeasures discussed;
- a wide Community of professionals, selected by invitation-only, who gather three times per year in the context of plenary meetings and represent the available basis of knowledge. Community figures have been continuously growing since 2009, This is especially noticeable from the increased attendance and participation in the plenary sessions.

In order to achieve the active status of Permanent Member, the applying organization has to

agree to the EECTF modus operandi, which has been conceived on the basis of three pillars:

- **pro-activity** in bringing knowledge, expertise and proposals to the Group,
- **non-disclosure** of sensitive information, in accordance to a Traffic Light Protocol, undersigned by each Permanent Member
- **non-competition** among counterparts commercially active in the same business field

Technical information such as attack reports, investigations outcomes, fraudsters' modus operandi and live demo of innovative attack methodologies are exchanged during physical meetings, while operational information such as fraudulent IP addresses, money mules, frauded accounts and so forth are exchanged one-to-one on a daily basis, by using suitable encryption technologies.

As of December 2013, the EECTF Constituency was made up of:

- **3 Founder Members** – Poste Italiane, the United States Secret Service and PoliziaPostale e delleComunicazioni
- **19 Permanent Members** – ABI Lab, American Express, Bulgarian Police, CA, Citibank, Consip, Global Cyber Security Center, Italian Ministry of Economy and Finance, Kaspersky, Mastercard, NTTData, Romanian Police, RSA, Selex ES, Symantec, VISA Europe, Unicredit, UNICRI, and Verizon
- **A Community of around 500 professionals**, evenly distributed between the public sector, financial institutions, LEAs, international organizations, research & academia and ICT vendors.

The possibility to acquire information from a cross-sector base of expertise makes the EECTF a valuable resource to help tackle the current situation at the institutional level. To cite an example, the EECTF acted as a witness in a public hearing on the state of network and information security held at the Chamber of Deputies of the Italian Parliament in 2011.

The EECTF's method of tackling cyber crime takes on a multifaceted, well-rounded approach. Comparing EECTF with another successful information sharing activity, OF2CEN, allows us to understand information sharing techniques that are targeted to a specific dimension of cyber crime, in this case financial fraud.

Focus: OF2CEN

Online Fraud Cyber Centre and Experts Network (OF2CEN)

The OF2CEN model and platform are born out of a mutual understanding between both law enforcement and the banking sector. The goal is to fight against online financial fraud transactions.

The Italian PoliziaPostale e delleComunicazioni used its expertise and experience to launch a project to create a center for the analysis and prevention of cyber threats to online banking services and money-handling mechanisms. Thanks to the European Union Prevention of and Fight against Crime (ISEC) programme, a Project Consortium of private sector organizations and representatives of the law enforcement community, OF2CEN along with its advanced information sharing platform were developed.

The project Consortium includes: **PoliziaPostale e delleComunicazioni, ABI Lab, Unicredit, BancaSella and Booz & Co, Global Cyber Security Center (GCSEC), General**

Inspectorate of the Romanian Police and NCA-Crime Agency, UK.

OF2CEN and its advanced information exchange platform consolidates suspicious transaction warnings communicated by banks to the police, facilitates information exchange of fraudulent IP and IBAN data through a secure channel.

The platform provides real time warnings on suspicious bank transactions to all the participants and correlates data, such as the IBANs of mules and compromised IPs to support Police investigations.

OF2CEN at glance:

- Implements a secure channel to share information and to guarantee data protection security.
- Offers a customized interface for each participant tailored to their activity and information needs.
- Enables timely warnings about fraudulent transactions, mirror sites and suspected IPs used to make malicious money transactions or host phishing websites.
- Performs valuable data analysis, automatic correlation and analysis of up-to-date statistical trends.

The platform has been operational since November 2013. The pilot was developed in Italy and is currently running and sharing information between 15 banks.

The project consortium aspires to broaden collaboration to include Europe-wide stakeholders. Each bank uploads its own data (suspicious IBAN numbers, compromised IPs…) onto the OF2CEN Platform and downloads data uploaded by the other banks. In a second step, the banks upload the OF2CEN downloaded data to their antifraud systems to prevent potential fraud against their clients.

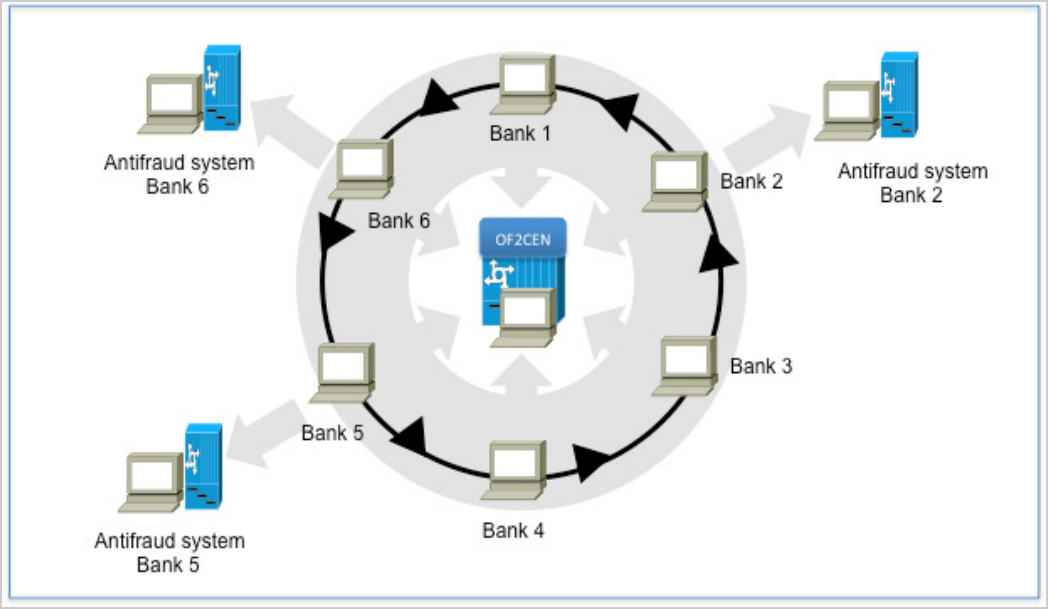

Figure: OF2CEN System and interaction with Antifraud system

The added value of the platform is to share information on fraud already perpetrated in a system and prevent further online fraud attacks by the same perpetrators.

The OF2CEN Platform has the capability to provide statistics, which are updated in real-time and show the typology of warnings as well as the destinations of the fraudulent transactions (in terms of quantity per country). It also shows the amount in Euros per typology (Credit Card, Online bank account, online game, mobile recharge or others) and destination, as well as the quantity of fraudulent transactions per typology and destination.

The next steps of the project are:

- The involvement of more banks inside the Italian circuit
- The deployment of OF2CEN in other EU Member States, creating other national hubs
- The connection of each national hub with a central hub, which could be EUROPOL

Chapter Four- Final considerations

In this final chapter, in light of the collected information and the preliminary inventory of good practices, we are drafting some potential recommendations on the basis of the analyzed material. This preliminary study does not aim to be exhaustive, but it may be considered a viable stepping stone to increasing knowledge, awareness and discussion on the future of information sharing.

The first viable recommendation that we have deducted through the creation of this overview is that the current trend to legislate and institutionalize models of information sharing needs to ensure respect for the current data sharing environment. Throughout the report, and within the table we constructed, it is clear that the current data ecosystem is comprised of a careful balance between national and international initiatives. It is also clear that some of these initiatives are tightly industry-linked, while others stretch across various disciplines. The multitude of mechanisms that are present allow for individual institutions, both private and public, to rely on the information sharing forum they trust most. We recommend that legislators take this element of trust into serious consideration given that, for all the reasons outlined in Chapter 1, it is fundamental to the creation of sustainable information sharing mechanisms.

A recurring suggestion from all three chapters is the need for increased awareness of cybersecurity exchange mechanisms. Data protection concerns ranked high among the reasons that private and public institutions were unwilling to engage in information sharing exercises. The reason we propose to increase awareness and education on the topic is that an understanding of the positive advantages of information sharing is likely to ease tensions regarding data protection. When looking for a best practice to address this predicament, we refer in particular to ENISA's Cyber Security Month initiative and all other proposals that seek to bridge the gap between governments and citizens. Also, as mentioned in Chapter 3, it would be important to recreate a private/public partnership, especially in this extremely important area.

Finally, the last recommendation we wish to put forth is that in order to develop effective Cyber Security mechanisms, we need to consider more closely what the term Cyber Security means and how each private and public institution can position itself within a secure network of information. Our chart in Chapter Three can be interpreted as an attempt to do just this. It is our hope that highlighting several of the existing forums for information sharing will enable different actors, who up until now have been reluctant to cooperate with their private or public counterparts, to find a network that effectively addresses their needs and anxieties.

Utilizing public-private partnerships and creating a trusting environment where responsible information sharing can take place is paramount when tackling issues within the rapidly changing world of cybercrime. The illustrated frameworks set up by the United Nations, the Council of Europe, and the EU should be seen as significant first steps for addressing cybercrime in the context of international organizations, while examples of good practices carried out by such enterprises as EECTF and OF2CEN offer practical approaches to information sharing. All sectors of society, from the local through the national and up to the international level should be involved in making cybersecurity a reality across the globe.

References

Albanesius C. (2013) "Obama's Cybersecurity Executive Order vs. CISPA: Which Approach Is Best?" PCMAG. Online. Accessed on 22/02/2013. Available at: http://www.pcmag.com/article2/0%2C2817%2C2415380%2C00.asp

Al-Greene B. (2012) "65% of Internet Users Are Cybercrime Victims [INFOGRAPHIC]." Mashable. Online. Accessed on 02/02/2013. Available at: http://mashable.com/2012/11/05/cybersecurity-infographic/

Allagui I., Kuebler J. (2011) "The Arab Spring and the Role of ICTs." International Journal of Communication 5 (1932-8036/2011). Print.

ANSA (2013) Monti Vara Decreto per Strategia Sicurezza Informatica. PRIMA 24/01/2013. Online. Accessed on 05/02/2013. Available at: http://www.primaonline.it/2013/01/24/113475/monti-vara-decreto-per-strategia-sicurezza-informatica/

Arthur C. (2012) "Google 'faces $22.5m Fine over Safari Privacy Breach'" The Guardian. Guardian News and Media. Online. Accessed on 15/02/2013. Available at: http://www.guardian.co.uk/technology/2012/jul/10/google-fine-iphone-ipad-privacy

Bagilli M. (2009) “Effects of Anonymity, Pre-Employment Integrity and Antisocial Behavior on Self-Reported Cyber Crime Engagement: An Exploratory Study”CERIAS Tech Report 2009-31. Online. Accessed on 02/02/2013. Available at: http://completosec.wordpress.com/2011/03/06/anonymity-antisocial-behavior-integrity-and-cybercrime/

Bennardo A., Pagano M., and Piccolo S. (2008) Multiple Bank Lending, Creditor Rights and Information Sharing. Centre for Studies in Economics and Finance. Online. Accessed on 5/02/2013 Available at: http://www.csef.it/WP/wp211.pdf

Bos H., Etalle S., Poll E. (2012) National Cyber Security Research Agenda: Trust and Security for our Digital Life. ICT Innovatinve Platform VeiligVerbonden, Print.

Brain Statistics (2013) "E-Commerce / Online Sales Statistics." Statistic Brain RSS. Online. Accessed on 07/02/2013. Available at: http://www.statisticbrain.com/total-online-sales/

Brown M., Jappelli T., Pagano M. (2008) "Information Sharing and Credit: Firm Level." Journal of Financial Intermediation.Elsevier, 2008. Online. Accessed on 5/02/ 2013. Available at: http://www.eief.it/files/2011/03/pagano-e-altri_joffinint_2009.pdf

Brookes A. (2006) "US Plans to 'fight the Net' Revealed." BBC News. BBC, 27 Jan. 2006. Online. Accessed on 02/022013. Available at: http://news.bbc.co.uk/2/hi/americas/4655196.stm

CERT-EU (2012) Mission Statement.CERT-EU News Monitor. Online. Accessed on 02/02/2013. Available at: http://cert.europa.eu/cert/plainedition/en/cert_about.html

Chabrow E. (2012) “Obama Unveils National Info Sharing Strategy:Balancing Need to Share Information with Safeguarding Liberties.”Info-Banking. Online. Accessed on 23/01/2013.

Available at: http://www.bankinfosecurity.com/obama-unveils-national-info-sharing-strategy-a-5368

Cobb S. (2012) Study Finds 90 Percent Have No Recent Cybersecurity Training. ESET Threat Blog. Online. Accessed on 22/01/2013. Available at: http://blog.eset.com/2012/10/10/study-finds-90-percent-have-no-recent-cybersecurity-training

Deichler A. (2013) "AFP Fraudwatch: Information Sharing Key for Cybersecurity." AFP Fraudwatch: Information Sharing Key for Cybersecurity. Online. Accessed on 07/02/2013. Available at: http://www.afponline.org/pub/res/news/AFP_Fraudwatch__Information_Sharing_Key_for_Cybersecurity.html

Department of Homeland Security (2012) National Cyber Security Awareness Month.Department of Homeland Security. Online. Accessed on 22/02/2013. Available at: http://www.dhs.gov/national-cyber-security-awareness-month

Dilanian K. (2012) “A new brand of cyber security: hacking the hackers” in theLos Angeles Times. Journal. Online. Accessed on 21/01/2013. Available at: http://articles.latimes.com/2012/dec/04/business/la-fi-cyber-defense-20121204

Donohue B. (2013) "Senate Introduces Cybersecurity Bill That Prioritizes Information Sharing." Threatpost (blog).N.p., 24 Jan. 2013. Online. Accessed on 7/02/2013. Available at: http://threatpost.com/en_us/blogs/senate-introduces-cybersecurity-bill-prioritizes-info-sharing-012413

European Commission (2012) Critical Information Infrastructure Protection.Online. Accessed on 02/02/2013. Available at: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

European Commission (2012) European Cybercrime Centre (EC3) opens on 11 January. EC IP/13/13. Online. Accessed on 02/02/2013. Available at: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

European Commission. (2012) Regulatory Framework for Electronic Communications in the EU Today. Online. Accessed on 02/02/2013. Available at: http://ec.europa.eu/information_society/policy/ecomm/eu-rules/index_en.htm

European Electronic Crime Task Force (2012) Cybernews. Year III Number 11; Journal, Print. November 2012.

European Network Security Agency (ENISA) (2011) Italy Country Report.ENISA, Print, Greece. Available at: http://www.enisa.europa.eu/activities/stakeholder-relations/country-reports

European Network Security Agency (ENISA) (2012) 7th CERT Workshop Part II Report. ENISA, Print, Greece. Available at: http://www.enisa.europa.eu/activities/cert/events/7th-cert-workshop-partII

European Network Security Agency (ENISA) (2012) EU Cyber Cooperation: the Digital Frontline. ENISA, Greece.Online. Accessed on 07/02/2013. Available at:

http://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2012/eu-cyber-cooperation-the-digital-frontline

European Network Security Agency (ENISA) (2012) "Cyber Europe 2012, Key Findings and Recommendations". ENISA. Online. Accessed on 04/02/2013. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report

European Network Security Agency (ENISA) (2012) "Cyber Atlantic 2011". ENISA.Online, Accessed on 04\02\2013.Availble at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic/cyber-atlantic-2011

European Network and Information Security Agency (ENISA) (2012) "Give and Take: Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime; Legal, Regulatory and Operational Factors Affecting CERT Cooperation with other Stakeholders". European Network and Information Security Agency. Online. Accessed on 07/01/2013. Available at: http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime

European Network Security Agency (ENISA) (2012) "National Cyber Security Strategies: Practical Guide on the Development and Execution". ENISA, Online. Accessed on 07/01/2013. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

European Network and Information Security Agency (ENISA) (2012) "European Cyber Security Month".ENISA. Online. Accessed on 02/02/2013. Available at: http://www.enisa.europa.eu/activities/cert/security-month

European Network and Information Security Agency ENISA (2012)"The Digital Frontline".ENISA. Online. Accessed on 7/01/2013. Available at: http://www.enisa.europa.eu/events/enisa-events/enisa-high-level-event-2012/eu-cyber-cooperation-the-digital-frontline

European Network and Information Security Agency (ENISA) (2013) "Resilience of Networks and Services and Critical Information Infrastructure Protection".ENISA. Online. Accessed on 02/02/2013. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP

European Network and Information Security Agency (ENISA) (2013) "Mutual Aid for Resilience in Europe".ENISA. Online. Accessed on 02/02/2013. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance

European Network and Information Security Agency (ENISA) (2013) "Industrial Control Systems/SCADA".ENISA. Online. Accessed on 02/02/2013. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/industrial-control-systems#_ftnref1

European Network and Information Security Agency (ENISA) (2013) "Internet Interconnections".ENISA. Online. Accessed on 02/02/2013. Available at:

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x

European Network and Information Security Agency (ENISA) (2013) “Threat Landscape: Responding to the Evolving Threat Environment”.ENISA. Online. Accessed on 02/02/2013. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x

Financial Times (2013) "US Cyber Security Executive Order Falls Short for the Private Sector." Financial Times. Online. Accesed on 22/02/2013. Available at: http://www.ft.com/intl/cms/s/0/fe33ef2e-778b-11e2-9e6e-00144feabdc0.html

Friess S. (2013) "Can the FTC enforce Google deal." POLITICO. Online. Accessed on 02/02/2013. Available at: http://www.politico.com/story/2013/01/can-the-ftc-monitor-googles-voluntary-deal-85818.html

Gehrig T., Stenbacka R. (2000) “Information Sharing in Banking: A Collusive Device." Econometric Society. Swedish School of Economics, Universitat Freiburg, Online. Accessed on 05/02/2013. Available at: http://www.econometricsociety.org/meetings/wc00/pdf/1837.pdf

Greenwald G. (2013) “Pentagon’s new massive Expansion of ‘Cyber-Security’ unit is about everything except defense.”The Guardian, Journal. Online. Accessed on 29/01/2013. Available at: http://www.guardian.co.uk/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-stuxnet

Humphreys S. (2011) Navigating the Dataverse: Privacy, Technology, Human Rights.International Council on Humans Rights Policy, 2011. Print.

Infosecurity-Magazine (2013) "New EU Cyber Security Directive (a European CISPA) Expected within Weeks." Infosecurity Magazine. N.p., 22 Jan. 2013. Online. Accessed on 7/02/ 2013. Available at: http://www.infosecurity-magazine.com/view/30351/new-eu-cyber-security-directive-a-european-cispa-expected-within-weeks/

Insinna V. (2012) “State to Rump Up Cybersecurity Information Sharing”. National Defense (NDIA). Online. Accessed on 02/02/2013. Available at: http://searchsecurity.techtarget.com/magazineContent/Cybersecurity-information-sharing-initiatives-on-the-rise

International Telecommunications Union (ITU) (2010) ITU Toolkit for Cybercrime Legislation. American Bar Association’s Privacy & Computer Crime Committee. Geneva, CH. Online. Accessed on 07/01/2013. Available at: http://www.ictparliament.org/node/2130

International Telecommunications Union (ITU) (2012) Understanding Cybercrime: Phenomena Challenges and Legal Response. ITU. Online. Accessed on 25/01/2013. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

International Telecommunications Union (ITU) (2013) “What does ITU do?”ITU. Online. Accessed on 02/02/2013. Available at: http://www.itu.int/en/about/Pages/whatwedo.aspx

International Telecommunications Union (ITU) (2013) "ITU-D ICT Applications and Cybersecurity (CYB): Cybersecurity." ITU-D ICT. Online. Accessed on 02/02/2013. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/unodc.html

Internet World Stats (2012)"World Internet Users Statistics Usage and World PopulationStats." World Internet Users Statistics Usage and World PopulationStats. Online. Accessed on 07/02/2013. Available at: http://www.Internetworldstats.com/stats.htm

Kaspersky Lab (2012) Global IT Security Risks. Online. Accessed on 22/02/2013. Available at: http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf

Karake-Shalhoub Z.,Al Qasimi L. (2010)"Cyber Law and Cyber Security in Developing and Emerging Economies." Cheltenham, UK: Edward Elgar, 2010. Print. P.9-15

KlimburgA. (2012) A National Cyber Security Framework Manual.CCDCOE supported by the NATO Science for Peace and Security Programme. Online. Accessed om 07/02/2013. Available at: http://www.ccdcoe.org/369.html

Marcus D., Sherstobitoff R. (2012) Dissecting Operation High Roller. McAfee and Guardian Analytics. Online. Accessed on 31/01/2013. Available at http://www.guardiananalytics.com/researchandresources/operation-high-roller.php

MacWillson A. (2012)"Cyber Security Strategies for Banks Transcript." Interview. Accenture. Online. Accessed on 4/02/2013. Available at: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Cyber-Security-Banking-Transcript.pdf

Magid L. (2012) "What Is CISPA And Why Would The President Veto It?" Forbes. Forbes Magazine, 25 Apr. 2012. Online. Accessed on 22/02/2013. Available at: http://www.forbes.com/sites/larrymagid/2012/04/25/what-is-cispa-and-why-would-the-president-veto-it/2/

Magid L. (2013) "Privacy Advocates Prefer Obama's Cybersecurity Plan Over CISPA." Forbes. Forbes Magazine, 21 Feb. 2013. Online. Accessed on22/02/2013. Available at: http://www.forbes.com/sites/larrymagid/2013/02/21/privacy-advocates-prefer-obamas-cybersecurity-plan-over-cispa/

McAfee (2011) Prospective Analysis onTrends in Cybercrime from 2011 to 2020. McAfee. Online. Accessed on 4/02/2013. Available at: http://www.mcafee.com/it/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf

National Security Program, Homeland Security Program (2012) Cyber security Task Force: Public-Private Information Sharing. Bipartisan Policy Center. Online. Accessed on 07/02/2013. Available at: http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf

Next Generation Communications Interoperability (NGCI) (2013) Information Sharing - Next Generation Communication Interoperability Workshop. Online. Accessed on 05/02/2013. Available at:http://www.ngcicommunity.org/wiki/index.php/Information_Sharing

NTV Uguanda (2013) "Ugandan Govt Unit to Fight Cyber Crime." AllAfrica. Online. Accessed on 22/02/2013. Available at: http://allafrica.com/view/resource/main/main/id/00060212.html

Europe's Information Society (2012) "European Public-Private Partnership for Resilience (EP3R)." NIS. Online. Accessed on 02/02/2013. Available at: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm

Europol (2011) Cybercrime presents a major challenge for law enforcement;The Hague. Available at: https://www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523

Opinion & Social (2012) Cyber Security Reports- Special Eurobarometer 390/wave EB77.2 at the request of the European Commission, Directorate-General Home Affairs. Online. Accessed on 07/01/2013. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

Pepitone J. (2011) "Facebook Settles FTC Charges over 2009 Privacy Breaches." CNNMoney. Cable News Network, 29 Nov. 2011. Online. Accessed on 15/02/2013. Available at: http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.htm

Piwowar H.A., Becich M.J., Bilofsky H., Crowley R.S., on behalf of the BIG Data Sharing and Intellectual Capital Workspace (2008) Towards a Data Sharing Culture: Recommendations for Leadership from Academic Health Centers. PLoS Med 5(9). Online. Accessed on 05/02/2013. Available at: http://www.plosmedicine.org/article/info%3Adoi%2F10.1371%2Fjournal.pmed.0050183

Polizia Dello Stato. CNAIPIC - Centro Nazionale Anticrimine Informatico per La Protezione Delle Infrastrutture Critiche. PoliziaDelloStato. Online. Accessed on02/02/2013. Available at: http://www.poliziadistato.it/articolo/18494/

PwC (2012) "An Australian Snapshot of Economic Crime." PricewaterhouseCoopers. Online. Accessed on 04/01/2013. Available at: http://www.pwc.com/gx/en/economic-crime-survey/assets/global-economic-booklet-vfa-med.pdf

Rockvam D. (2013) "Comment: Cybersecurity and Information Sharing Is a Two-way Street." Infosecurity-Magazine. Online. Accessed on 07/02/ 2013. Available at: http://www.infosecurity-magazine.com/view/27282/comment-cybersecurity-and-information-sharing-is-a-twoway-street/

SC Magazine (2013) "Infosecurity Europe Preview 2013." SC Magazine UK. Online. Accessed on 23/02/2013. Available at http://www.scmagazineuk.com/infosecurity-europe-preview-2013/article/281280/

Santos M. (2012) "Over 1.5M Are Cybercrime Victims Daily Worldwide." Inquirer Technology. Online. Accessed on:20/20/2013. Available at: http://technology.inquirer.net/19074/over-1-5m-are-cybercrime-victims-daily-worldwide-study

SegerA. (2012) Cybercrime Strategies (Discussion Paper). Global Project on Cybercrime funded by Council of Europe, Microsoft, United Kingdom, Romania. Online. Accessed on 09/01/2013. Available at: www.coe.int/cybercrime

Sheets C. A. (2012) "What Is CISPA 2012? Inside The Bill That Has Internet Privacy Advocates Up In Arms." International Business Times. Online. Accessed on 22/02/2013.Available at: http://www.ibtimes.com/what-cispa-2012-inside-bill-has-Internet-privacy-advocates-arms-693333

Schneier B. (2007) "Why 'Anonymous' Data Sometimes Isn't." Wired.com. Conde Nast Digital, 13 Dec. 2007. Online. Accessed on: 01/02/2013. Available at: http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213

Symantec (2012) "2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually." Symantec. Online. Accessed on 07/02/2013. Available at: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02

Taut B. J. E. (2012) Timely Cyber Crime Information Sharing Between ISPs/Telcos and Banks/Police. Building International Cooperation for Trustsworthy ICT. BIC. Online. Accessed on 5/02/2013.Available at: http://www.bic-trust.eu/files/2013/01/Taute_TimelyCybercrimeInfoSharing_Nov2012.pdf

Techdirt (2012) “There Is A ‘Right Way’ To Do Cybersecurity Information Sharing, But CISPA Is Not It.” Techdirt. Online. Accessed on 07/02/13. Available at:http://www.techdirt.com/articles/20120426/07560218668/there-is-right-way-to-do-cybersecurity-information-sharing-cispa-is-not-it.shtml

Techopedia. (2013) "Information Sharing." Techopedias. Online. Accessed on 20/02/2013. Available at: http://www.techopedia.com/definition/24839/information-sharing

The Council of Europe (2001) Cybercrime.Council of Europe. Online. Accessed on 02/02/2013. Available at: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

The Economist (2013) "War on Terabytes." The Economist.Online. Online. Accessed on 4/02/ 2013. Available at: http://www.economist.com/news/finance-and-economics/21571152-banking-has-gone-electronic-it-has-also-become-vulnerable-war-terabytes

The Economist. (2011) "Measuring the Black Web." The Economist. Online. Accessed on 02/02/2013. Available at: http://www.economist.com/node/21532263

The White House (2013)"Executive Order - Improving Critical Infrastructure Cybersecurity." The White House. Online. Accessed on 20/02/2013. Available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

The White House (2010) "The Comprehensive National Cybersecurity Initiative." The White House. Online. Accessed on 22/02/2013. Available at: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Thompson L. D. (2003) “Intelligence Collection and Information Sharing within the United States.”The Brookings Institution. Online. Accessed on 05/02/2013. Available at: http://www.brookings.edu/research/testimony/2003/12/08terrorism-thompson

Tierney J. (2008) "The Endless Fear of Terrorism." TierneyLab. The New York Times. Online: Accessed on 02/02/2013. Available at: http://tierneylab.blogs.nytimes.com/2008/01/16/the-endless-fear-of-terrorism/

TNS Opinion & Social (2012)Cyber Security Reports- Special Eurobarometer 390/wave EB77.2 at the request of the European Commission, Directorate-General Home Affairs. Online. Accessed on 02/02/2013. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

Transport Canada (2010) Transportation Security Clearances / Criminal Information Sharing. Transport Canada. Online. Accessed on 05/ 02/ 2013. Available at: http://www.tc.gc.ca/eng/aviationsecurity/page-199.htm

United Nations Interregional Crime and Justice Research Institute (UNICRI) (2013) Cyber Crime. United Nations Interregional Crime and Justice Research Institute. Online. Accessed on 02/02/2013. Available at: http://www.unicri.it/special_topics/cyber_threats/cyber_crime/ .

United Nations Office on Drugs and Crime (UNODC) (2011) UNODC and ITU Join Forces to Make the Internet Safer. United Nations Office on Drugs and Crime. UNODC, 16 May 2011. Online. Accessed on 19/02/2013. Available at: https://www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-more-closely-to-make-the-Internet-safer.html

United Nations Office on Drugs and Crime (UNODC) (2013).Criminal Justice, Prison Reform and Crime Prevention. UnitedNations Office on Drugs and Crime. Online. Accessed on 02/02/2013. Available at: http://www.unodc.org/unodc/en/justice-and-prison-reform/index.html?ref=menuside

U.S. GAO (2010)Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. U.S.GAO. Online. Accessed on 05/02/2013. Available at: http://www.gao.gov/products/GAO-10-628

World Economic Forum (WEF) (2013) Partnering For Cyber Resiliance. WEF. Online. Accessed on 28/0172013. Available at: http://www.weforum.org/issues/partnering-cyber-resilience-pcr

World Economic Forum(WEF) (2012) Rethinking Personal Data: Strengthening Trust. WEF. Online. Accessed on 28/01/2013. Available at: http://www.weforum.org/reports/rethinking-personal-data-strengthening-trust

Case Law and Legislation

Commission Communication to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions on a Cybersecurity Strategy of the European Union: An Open, Safe, Secure Cyberspace. 07/02/2013. COM (2013) 48 final.

Commission Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union [2013] SWD 31 final and SWD 32 final, COM(2013) 48 final.

Consolidated Version of the Treaty on the Functioning of the European Union art. [26], 2008 O.J. C 115/47

Convention on Cybercrime and Protocol to the said Convention - Council of Europe Treaty Series No. 185-189 (2011)

Council Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communication networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for enforcement of consumer protection laws [2009] OJ L337 P.0011-0036

Council Directive 2009140/EC amending Directives 2002/21/EC on common regulatory framework for electronic communication networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communication networks and services [2009] OJ L 337/37

Council Directive 2008/114/EC on the Identification and designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection [2008] OJ L345/75

Council Directive 2006/24/EC On the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Networks and Amending Directive [2006] OJ L 105/54

Council Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector [2002] OJ L201

Council Directive 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services [2002] OJ L108/33

Council Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281

Council Regulation (EC No 460/2004) establishing the European Network and Information Security Agency [2004] OJ L 077 P. 0001-0011

Council Resolution (2009/C 321/01) (EC) on a Collaborative European Approach to Network and Information Security [2009] OJ C 321/1

Council of Europe Convention on Cybercrime "Budapest Convention", 23.XI.2001

European Convention of Human Rights (ECHR) Art 8 and The Charter of Fundamental Rights of the European Union (Treaty of Lisbon) Art. 2

Italian integration of the Criminal Code and the Criminal Procedure Code involving Cyber Crime, Act nº 547 of 13 December 1993

Italian Data Protection Code Legislative Decree no. 196 of 30 June 2003

Italian Legislative Decree on Electronic Commerce, Legislative Decree no. 70 of 9 April 2003

Italian Electronic Communications Code, Legislative Decree no. 259 of 1 August 2003

UNGA Res 55/63 (22 January 2001) UN Doc A/RES/55/593

UNGA Res 56/121 (23 January 2002) UN Doc A/RES/56/574

UNGA Res 57/52 (30 December 2002) UN Doc A/RES/57/53

UNGA Res 57/293 (31 January 2003) UN Doc A/RES/57/293

UNGA Res 58/199 (30 January 2004) UN Doc A/RES/58/199

UNGA Res 64/211 (17 March 2010) UN Doc A/RES/64/211