COMPUTERS & SECURITY 60 (2016) 154–176

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing

Florian Skopik *, *Giuseppe Settanni*, *Roman Fiedler*

Digital Safety and Security Department, Austrian Institute of Technology, Donau-City-Straße 1, 1220 Vienna, Austria

ARTICLE INFO

Article history:
Received 3 December 2014
Received in revised form 15 March 2016
Accepted 7 April 2016
Available online 13 April 2016

Keywords:
Survey
Cyber security
Information sharing
Cyber incident reporting
Organizational aspects
Standardization

ABSTRACT

The Internet threat landscape is fundamentally changing. A major shift away from hobby hacking toward well-organized cyber crime can be observed. These attacks are typically carried out for commercial reasons in a sophisticated and targeted manner, and specifically in a way to circumvent common security measures. Additionally, networks have grown to a scale and complexity, and have reached a degree of interconnectedness, that their protection can often only be guaranteed and financed as shared efforts. Consequently, new paradigms are required for detecting contemporary attacks and mitigating their effects. Today, many attack detection tasks are performed within individual organizations, and there is little cross-organizational information sharing. However, information sharing is a crucial step to acquiring a thorough understanding of large-scale cyber-attack situations, and is therefore seen as one of the key concepts to protect future networks. Discovering covert cyber attacks and new malware, issuing early warnings, advice about how to secure networks, and selectively distribute threat intelligence data are just some of the many use cases. In this survey article we provide a structured overview about the dimensions of cyber security information sharing. First, we motivate the need in more detail and work out the requirements for an information sharing system. Second, we highlight legal aspects and efforts from standardization bodies such as ISO and the National Institute of Standards and Technology (NIST). Third, we survey implementations in terms of both organizational and technological matters. In this regard, we study the structures of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), and evaluate what we could learn from them in terms of applied processes, available protocols and implemented tools. We conclude with a critical review of the state of the art and highlight important considerations when building effective security information sharing platforms for the future.

1. Introduction

The smooth operation of critical infrastructures, such as telecommunications or electricity supply, is essential for our society. In recent years, however, operators of critical infrastructures have increasingly struggled with cyber security problems (Langner, 2011). Through the use of standard Information and Communications Technology (ICT) products and increasing network interdependencies (Rinaldi, 2004), the surfaces and channels of attacks have increased significantly. New approaches are required to tackle this serious security situation.

* *Corresponding author.*
E-mail address: florian.skopik@ait.ac.at (F. Skopik).
http://dx.doi.org/10.1016/j.cose.2016.04.003

One promising approach is the exchange of network monitoring data and status information (Hernandez-Ardieta et al., 2013) of critical services across organizational boundaries with strategic partners and national authorities. The main goal is to create an extensive situational awareness picture about potential threats and ongoing incidents, which is a prerequisite for effective preparation and assistance in large-scale incidents. Collaboration based on threat information sharing is believed to be effective in a multitude of cyber security scenarios including financially driven cyber crimes, cyber war, hacktivism, and terrorism (see Denise and James, 2015 and Dacey, 2003). The attack morphology can be different depending on the scenario, e.g., cyber crime might use stealthy advanced persistent threats (APTs) to steal intellectual property, while cyber war or terrorism uses botnets to run DDoS attacks. However, information sharing enables the victims to run coordinated and effective countermeasures, and provides preventive support to potential future targets on how to effectively protect their ICT infrastructures (see NIST, 2014b).

We argue that since attacks are becoming increasingly sophisticated, customized and coordinated, we also need to employ targeted and coordinated countermeasures. Typical commercial-off-the-shelf (COTS) virus scanner and firewall systems appear incapable of sufficiently protecting against APTs (Tankard, 2011). The rapidly growing complexity of today's networks, emergence of zero day exploit markets (Miller, 2007), and often underestimated vulnerabilities, e.g., due to outdated software or policies, lead to novel forms of attacks appearing daily. Thus, numerous information security platforms and knowledge bases have emerged on the Web. From there, people can retrieve valuable information about identified threats, new malware and spreading viruses, along with information about how to protect their infrastructure (e.g., see national Computer Emergence Response Teams).[1] However, this information is usually quite generic, not shaped to particular industries and often lacks in-depth knowledge.

In order to make such platforms more effective, sector-specific views along with rich information and experience reports are required to provide an added value to professional users. Many standardization bodies, including NIST (2014a), ITU-T (2012) and ISO (2012), have proposed the establishment of centrally coordinated national cyber security centers, which are currently emerging all over the world.

However, effective cyber security centers are hard to establish and often neither governmental bodies nor companies and customer organizations are well prepared to run and use them. The challenges are grounded in the fact that cyber security information sharing requires a great deal of multi-disciplinary research. Although the setup of such systems is often reduced to addressing technical aspects, it is a similarly significant challenge for legal experts, standardization committees and social as well as economic scientists. For example, questions dealing with the sharing process design, i.e., who is allowed to share what and when in a corporate environment, legal dependencies and regulatory compliance, as well as what can we learn from existing implementations of CERTs, are of equal importance.

[1] http://www.cert.org; April 2016.

Moreover, while there are many works that deal with information sharing among CERTs, such as ENISA (2011a) and ENISA (2013a), there is little experience so far with peer-to-peer sharing of such information among companies. This is for numerous reservations (ENISA, 2010), such as low quality information, reputational risks, and poor management. Raising awareness of these issues and providing an overview of potential solutions are two of the goals of this paper.

It is therefore critical to take a closer look into all of these aspects in a structured form – from the economic motivation (and requirements) on information sharing, over legal and regulatory aspects, to structural and technological matters. Therefore, the contributions of this survey article are as follows:

- *Holistic Picture of Cyber Security Information Sharing*. We shed light on the numerous economic, legal, and regulatory aspects that, besides the technical dimensions, are often neglected.
- *Survey on existing Methods, Technologies, Protocols and Tools*. We survey existing approaches and solutions as a prerequisite to identify open gaps.
- *Evaluation of the State-of-the-Art and Key Findings for Future Systems*. We critically evaluate the current situation and emphasize likely future developments regarding standards, norms and technologies.

The remainder of this paper is structured as follows: Section 2 provides an overview of related work. Since this is a survey paper, we mainly refer to other survey papers here, and omit works that is cited in the the other sections. Section 3 is about the various dimensions that need to be considered when it comes to cyber security information sharing. For that purpose, we group all relevant aspects into five distinct categories. After that, relevant regulations, standards, concepts, supporting tools, and protocols that are essential for setting up effective information sharing procedures are discussed. In particular, Section 4 outlines cooperation and coordination aspects and presents some sample sharing scenarios. Section 5 reviews existing regulatory directives and legal recommendations. Subsequently, Section 6 refers to well-recognized standards in this area, while Section 7 covers concrete implementations in terms of organizational structures. Section 8 deals with technologies, tools and applicable protocols. After this survey, we critically review the applicability of existing solutions in a large-scale national security information sharing network (as set up in the context of a number of projects together with national stakeholders) in Section 9. Finally, Section 10 concludes the paper.

2. Related work

Cyber-attacks are becoming increasingly sophisticated, targeted and coordinated, resulting in so-called advanced persistent threats (Farwell and Rohozinski, 2011; Tankard, 2011). Consequently, new paradigms are required for detecting and mitigating these kinds of attack (Virvilis and Gritzalis, 2013), and eventually to establish situational awareness (Jajodia et al., 2010; Sarter and Woods, 1991; Tadda et al., 2006). Many of these tasks are currently performed within individual

organizations only, and – apart from the important works that national CERTs[2] do – there is little cross-organizational security information sharing. However, information sharing is a crucial step to acquiring a thorough understanding of cyber-attack situations, and is necessary to warn others against (advanced) threats.

However, in practice, security information sharing is usually accomplished via ad-hoc and informal relationships (US Homeland Security Cyber Security R&D Center, 2009). Often, national CERTs assume the role of national contact points for coordinating and aggregating security incidence reports via communication channels such as email, instant messaging, file exchange/storage, VoIP, IRC and the Web (ENISA, 2011a). Internet forums, such as the Internet Storm Center from SANS,[3] collect and provide data about malicious activities on the Internet. Commercial service providers, such as Arbor Networks,[4] offer network-wide threat information updates and analysis services. Usually there is a crucial economic tradeoff to be considered between economic benefit of sharing (Agrawal et al., 2003; Skopik and Li, 2013) and potential disadvantages, such as harm of reputation and commitment of costly resources. The timing at which information is revealed and exchanged between the involved parties plays a crucial role in the mitigation phase, not only on an economic extent, but also with respect to the derived social costs (see Arora et al., 2008).

Cooperative cyber defense (Harrison and White, 2012; Hernandez-Ardieta et al., 2013; Zhao and White, 2012) has been studied in recent years, yet its broad adoption is still missing. In particular, sharing sensitive information among companies (Hausken, 2007) is still an unsolved issue as the risk for reputation damage is high. On the other side, a number of studies have shown that securing networks as a shared effort has clear economic advantages (Gal-Or and Ghose, 2005; Gordon et al., 2003). However, a major prerequisite to this is the creation of trust (Abrams et al., 2003; Golle et al., 2001; Skopik et al., 2010) among involved parties, specifically when it comes to the sharing of security-sensitive information (Fernandez Vazquez et al., 2012).

Standard bodies and the like have produced volumes about how to establish security information sharing networks – the canonical examples being the NIST guideline "Framework for Improving Critical Infrastructure Cybersecurity" (NIST, 2014a), the ENISA documents "Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches" (ENISA, 2015) and "Cybersecurity cooperation: Defending the digital frontline" (Helmbrecht et al., 2013) (just to name two of the many available guidelines from ENISA), or the ISO/IEC standard 27010 "Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications" (ISO, 2012). While representing important work, these recommendations are not the complete picture and important pieces are still missing. For instance, current recommendations largely take an architectural (and partly organizational) view on the problem, and omit guidance on the operational aspects of enabling security information sharing. Little attention is given to the technologies and processes that are needed to maintain situational awareness for these potentially complex cyber systems.

3. The dimensions of information sharing

A multitude of dimensions need to be considered in order to realize effective information sharing. In contrast to many others who primarily focus on the technical aspects, we argue that the biggest challenges are not entirely located in this area, but mainly span the different dimensions of technical, legal, regulatory and organizational means.[5]

In this paper we made an extensive literature survey to identify a large base corpora of literature and references; we then clustered the identified references according to their main subjects. Following this strategy we took into account all the significant dimensions that holistically capture the relevant State-of-the-Art in the domain of Cyber security information sharing only. However, other dimensions may emerge in the future or become more important.

Fig. 1 shows the dimensions of security information sharing, which need to be considered when setting up a large-scale organizational or even national cyber security center:

I *Efficient Cooperation and Coordination:* Real world experiences highlight the economic need for coordinated cyber defense (Gal-Or and Ghose, 2005; Gordon et al., 2003), e.g., due to increased system complexity and attack surfaces, as well as the sophistication of attacks. This coordinated cyber defense is mainly realized through information sharing. There exists a wide variety of information classes that are viable for a wide range of stakeholders: indicators of compromise, technical vulnerabilities, zero day exploits, social engineering attacks or critical service outages.

II *Legal and Regulatory Landscape:* However, in order to be adopted by a critical mass of stakeholders, information sharing requires a legal basis. Therefore, the European Union, as well as some of its Member States and the US, have recently begun to create a set of directives and regulations.

III *Standardization Efforts:* As a further step toward enabling information sharing, standards and specifications need to be developed that are compliant with legal requirements. NIST, ENISA, ETSI and ISO – just to name a few – have already released documents to start this effort, and will further develop existing guidelines in the near future.

IV *Regional and International Implementations:* Taking these standards and specifications, organizational measures

[2] http://www.cert.org; April 2016.
[3] http://isc.sans.org; April 2016.
[4] http://www.arbornetworks.com; April 2016.

[5] Notice that we intentionally left out social aspects here, such as personal incentive and motivation to share, as well as reward and trust. These issues have been extensively studied in the literature (cf. Abrams et al., 2003; Fernandez Vazquez et al., 2012; Golle et al., 2001; Parameswaran et al., 2001; Skopik and Li, 2013) and are thus omitted here for the sake of brevity. Moreover, incentive and motivation of individuals are comparatively neglectable here, where sharing is either legally enforced or performed due to compliance issues.

Fig. 1 – The primary dimensions of information sharing and their concerns.

and sharing structures need to be realized and integrated. Important work contributing to this step has been performed by CERTs and national cyber security centers so far.

V *Technology Integration into Organizations:* Eventually, a set of sharing protocols and management tools on the technical layer need to be selected and set into operation. Here it is essential that selected technical means are compatible to organizational processes and can be handled appropriately.

After the full implementation of information sharing procedures, a periodic re-evaluation of their effectiveness, e.g., in terms of detecting and combating new and emerging threats etc., needs to be performed and – if necessary – certain measures in the numerous dimensions reconsidered accordingly.

The next sections will deal with these dimensions and their concerns in detail.

4. Dimension I: efficient cooperation and coordination

The increased presence of information technology in modern critical infrastructures has stimulated the proliferation of a significant number of new types of threats. These threats are global in nature and are shifting in focus and intensity, exploiting opportunities enabled by new technologies. Mitigation measures exist to respond to these evolving threats, but in most of the cases technological means need to be supported by cross-organizational (and even cross-border) collaboration to be effective.

4.1. *Cyber defense as a joint endeavor*

International collaboration is of the utmost importance for effective response mechanisms. Indeed, digital boundaries are not clearly defined and do not correspond to national frontiers. Moreover, recent publications show that threats such as malware (and botnets, in particular) are no longer an issue that people should deal with individually, but are increasingly a social and civic responsibility that affects all sectors of the digital society (Anonymous, 2012; ENISA, 2013b).

According to Helmbrecht et al. (2013), response mechanisms, containing numerous established policy initiatives, have been in place from the early days of ICT development. However, the deployment of ICT solutions used by citizens in their day-to-day lives is threatened by cyber attacks, targeting areas such as online payment, e-government services, and in general every critical infrastructure relying on computer networks. Finally, ICT is increasingly used in vandalism, terrorism, hacktivism, war and fraud that reduce the level of confidence citizens have in trustfully adopting such technology and exposes them to higher and higher danger.

Securing ICT systems within a confederation of countries needs to be coherent across geographical borders and consistently pursued over time.

The European Network and Information Security Agency (ENISA) is the main European body aiming at improving the convergence of efforts from the different Member States by encouraging the exchange of information, methods and results, and avoiding duplication of work. To this end, one of ENISA's tasks is to support European institutions and Member States by facilitating a coordinated approach to respond to network and information security threats.

The NIST supports the coordination of existing Computer Security Incident Response Teams (CSIRTs), when responding to computer security incidents, by identifying technical standards, methodologies, procedures, and processes related to Computer Security Incident Coordination (CSIC). NIST provides guidance on how multiple CSIRTs should cooperate while handling computer security incidents, and how CSIRTs should establish synergies with other organizations within a broader information sharing community.

4.2. *The threat landscape*

The cyber threat landscape evolves rapidly. Innovative methods to achieve malicious objectives are constantly taking shape in cyber space. Cyber-criminals and certain nation-states are aggressively pursuing valuable data assets, such as financial transaction information, product design blueprints, user credentials to sensitive systems, and other intellectual property. Attackers are armed with the latest zero-day vulnerabilities, high-quality toolkits, and social engineering techniques to perpetrate advanced targeted attacks. These threats use several stages and vectors to duck traditional defenses and find vulnerable systems and sensitive data (FireEye, 2013).

Attacks have changed in form, function, and sophistication from just a few years ago. The new generation of threats utilize both mass-market malware designed to infect multiple systems as well as sophisticated, zero-day malware to infect targeted systems. They leverage multiple attack vectors cutting across Web, email, and application-based attacks. Today's attacks are aimed at getting valuable data assets, sensitive financial information, intellectual property, authentication credentials, insider information, and each attack is often a multi-staged effort to infiltrate networks, spread, and ultimately exfiltrate the valuable data (FireEye, 2013).

Modern cyber attackers are not only motivated by economic reasons, but also their actions are more and more driven by impulses of social and political nature. International groups of associated activists and hacktivists, such as Anonymous, are nowadays well known for attacks on government, religious and corporate websites (Olson, 2012). In April 2007, Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial. Some government online services were temporarily disrupted and online banking was halted. The attacks were more like cyber riots than crippling attacks and provoked outages lasting several hours or days (Herzog, 2011). In October 2010, Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems (ICS), was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program (Farwell and Rohozinski, 2011). On November 24, 2014, data belonging to Sony Pictures Entertainment including personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of unreleased Sony films, and other information were released by hackers who called themselves the "Guardians of Peace" or "GOP" (State of California Department of Justice Office of the Attorney General, 2014). They demanded the cancellation of the planned release of the film *The Interview*, a comedy about a plot to assassinate North Korean leader.

In order to develop effective defense strategies, it is necessary to understand the cyber threats and the methodologies put in place to deploy them. The components of the evolving cyber threat landscape are becoming increasingly complex. A comprehensive analysis of the reported cyber incidents needs to be performed to characterize the multitude of aspects a cyber threat involves. Priority lists of cyber threats, threat agents, attack methods and threat trends are all elements that need to be taken into consideration. This information is useful for cyber security experts assessing risks to various systems and developing cyber security policies for defending valuable information. Nevertheless, care should always be taken when analyzing such data – the fact that an event has happened frequently in the past does not guarantee that it will continue to happen.

Given that the cyber threat landscape develops very dynamically, the main challenge is to capture the trends as early as possible (cf. ENISA report, Helmbrecht et al., 2013).

In 2014, for *Drive-by-exploits* there is a shift from botnets to malicious URLs as the preferred means to distribute malware, because URLs are a more difficult target for law enforcement take-downs. Regarding *Code Injection*, a notable issue is attacks against popular content management systems (CMSs). Due to their wide use, popular CMSs make up a considerable attack surface that has drawn the attention of cyber criminals. An interesting aspect is the increased use of *peer-to-peer (P2P) botnets* – more difficult to locate and take down. Also, the use of botnet infrastructures to mine the "virtual currency" bitcoins is an emerging trend.

After the 2013 Spamhaus attack (Arstechnica, 2013), Domain Name System *(DNS) reflection attacks* have gained popularity within the Denial of Service attacks. Further, there is an increase in *rogueware/scareware* reported. One reason for the growth is the expansion of ransomware and fake antivirus distribution to mobile platforms such as Android. *Cyber espionage* attacks reached a dimension that went far beyond expectations (ENISA, 2013c). Several mass surveillance campaigns run by nation states have been recently uncovered (see Clarke, 2011 and Hudson, 2014), generating the indignation of the population. *Identity theft* led to some of the most successful attacks by abusing SMS-forwarders to commit significant financial fraud. These attacks were based on known financial Trojans (e.g. Zeus, SpyEye, Citadel) that have been implemented on mobile platforms and attack two-factor authentication. *Search Engine Poisoning* has also moved to mobile devices. These developments led to the conclusion that attackers remain one step ahead; quite often it suffices to exploit simple and well known weaknesses to cause havoc.

Although information sharing might seem in contrast with the attitude of some nation states performing espionage on other countries, this should not void information sharing efforts among organizations (especially those with similar infrastructures, and thus suffering from similar vulnerabilities or being potentially similarly attractive to attackers) from these countries on another layer. The key message of ENISA is to transfer knowledge from the cyber security community to the user groups for the purpose of strengthening cyber defense. To this end, effective information sharing, not only between security

professionals, but also between all stakeholders dealing with critical ICT systems, needs to be enabled.

4.3. Incident taxonomies

In order to uniquely identify and compare events, incidents and revealed attacks, security communities have defined numerous taxonomies over the last years. Existing incident taxonomies are either specifically developed by individual CERTs (e.g., the one defined by the Latvian CERT[6] and the one by the Hungarian CERT[7]), or universal and internationally recognized. In this section we briefly describe two of the most commonly adopted taxonomies.

One of the oldest schemas, developed at the Sandia National Laboratories, is the so called "*Common Language*" (Howard and Longstaff, 1998). This taxonomy defines three main terms: *event*, *attack*, *incident*. An *event* comprises available information about a target of the *attack* and an action undertaken against it. When more information about it is available, such as a tool used to perform the attack, a vulnerability exploited and a result of the attack, then the *attack* can be fully described. According to this taxonomy, an *incident* is described only if, along with the information about the *attack*, the source of the *incident* and the objective of the *attack* are known. This taxonomy is quite extensive and allows to identify and classify incidents in detail according to several criteria. However, it can be time-consuming and ambiguous; often security experts are not able to collect all the information required to fully describe an incident. This taxonomy is therefore mostly used for research purposes, theoretical considerations and as a starting point for creating custom taxonomies.

Another taxonomy worth considering is the taxonomy developed within the *European CSIRT Network project*.[8] It is essentially based on the taxonomy by a Swedish CERT team (TS-CERT[9]) and it is currently adopted by many European CERTs. This taxonomy (see Kácha, 2014) groups incidents into eight main categories (*Incident Classes*) and twenty-five sub-categories (*Incident Types*). Several features make this taxonomy convenient to use. The main categories are actual and universal, while the subcategories became a part of the description rather than a concrete schema for classification.

4.4. Sharing scenarios

Facing the given threat landscape, there are a multitude of economic reasons for sharing (Gal-Or and Ghose, 2005; Gordon et al., 2003) in order to lower security expenses for all partners in an alliance (Phillips et al., 2002; Skopik and Li, 2013). Besides connecting organizations in a peer-2-peer manner, many national initiatives also foresee (national) cyber security centers, which provide help and support on request, specifically to critical infrastructure providers. In this article we identified four scenarios which in sum demonstrate the strong need for sharing and the high economic potential.

Notice that the applicability of the concepts proposed in this work is not limited to information sharing among (non-ICT) CI organizations; it rather spans a broader scope comprising ICT network service providers, cyber security providers, and other infrastructure providers.

4.4.1. Sharing information about recent or ongoing incidents

This scenario enables sharing of information on current incidents including the status of services, organizational impacts and consequences, as well as the attack vector (as far as known) or reasons for malfunction together with an estimation for the recovery time. This information is considered very sensitive and could possibly be used to harm the reputation of organizations; however, it is an important prerequisite to enable mutual aid and help, issue pre-warnings, or enable partner organizations to learn from recent incidents. In this scenario, we foresee three different use cases. First, organizations that are victims of a cyber incident report detailed information about the incident to a national cyber center. Second, a national cyber center informs organizations, which provide critical services, about incidents currently or recently affecting one or more of the federated organizations. And third, organizations within a confederation inform one another (especially business customers) about major service degradations due to current incidents they are affected by. Eventually, all these measures are suitable to increase cyber situational awareness.

4.4.2. Sharing information about service dependencies

This scenario deals with sharing static service dependencies to better predict the impact of a (potential) service degradation or outage. This is especially relevant for proper risk assessment if services from different companies depend on each other, e.g., the outage of a cloud provider has negative impact on services of other organizations that use the cloud as a back-end storage. In this scenario, the consumer of the service reports about the service dependencies in the following three cases: First, organizations report to a national cyber center about the services their activities depend on. Second, the national cyber center informs the federated organizations about other organizations' services dependencies. And third, the federated organizations inform one another on their services' dependencies.

4.4.3. Sharing information about the technical service status

In this scenario, dynamic information about the technical status of services, e.g., their availability, confidentiality and integrity, is shared. In case of outages, predictions for the required restore time is included. This information can be used for modeling or informing dependent organizations about the service status. In this scenario the consumer of the service reports about the service status in one of the following three cases: First, organizations inform the national cyber center about the status of the services they provide. Second, the national cyber center informs organizations about other organizations' services' status. Third, organizations inform one another about their services' status.

4.4.4. Request assistance of organizations

In case a cyber incident cannot be handled by an organization on its own, it might request help from external experts

[6] http://www.cert.lv/; April 2016.
[7] http://www.cert-hungary.hu/en; April 2016.
[8] http://www.ecsirt.net/; April 2016.
[9] http://www.teliasonera.com/; April 2016.

of the national cyber center. Furthermore, even a national cyber center could request help from external organizations or individuals, e.g., in case certain expertise is required but not available. Eventually, a cyber center could therefore act as a broker who connects the right people in time to tackle a cyber incident. We distinguish between two cases here: In the first case an organization asks for assistance from other organizations that might have been dealing with similar issues in the past. In the second case the cyber center asks for assistance from federated organizations in order to provide support to organizations facing a particular issue.

5. Dimension II: legal and regulatory landscape

Internationally, critical infrastructure (CI) cyber security has become a fundamental as well as delicate subject in the last years. The European Union and the United States are becoming increasingly sensitive to this topic, which has resulted in the release of indications, publishing strategies and the issuing of directives that regulate a secure digital environment for their Member States.

The European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, has published a Cyber security Strategy alongside a Commission Proposed Directive concerning measures to ensure a high common level of Network and Information Security (NIS) across the Union. In February 2013, the President of the United States signed Executive Order (EO) 13636, "Improving Critical Infrastructure Cyber security," and the Presidential Policy Directive (PPD)-21, "Critical Infrastructure Security and Resilience". The policies set forth in these directives will strengthen the security and resilience of critical infrastructure against evolving threats and hazards. These documents call for an updated and overarching national framework that reflects the increasing role of cyber security in securing physical assets.

Several smaller countries, outside the EU and the US, are currently discussing the essential aspects of Critical Information Infrastructure Protection (CIIP) to be regulated in their upcoming policies and directives. Due to resource limitations, the cyber security strategies being developed by Latin American countries such as Argentina, Colombia, Uruguay, Trinidad and Tobago, are mostly based on best practices and models adopted by more developed countries (see Micro and Organization of American States, 2015). According to BSA-The Software Alliance and Galexia (2015), a study which provides a comprehensive overview on cyber security policy environment in 10 Asia-Pacific markets, the markets included in the study have historically been slow to produce comprehensive national cyber security strategies, and to implement the necessary legal frameworks for security and critical infrastructure protection. However, in order to strengthen the protection of critical infrastructure from cyber threats, in the Asia-Pacific region public and private stakeholders are nowadays cooperating toward the establishment of proper policy, legal and operational frameworks; improve collaboration with various relevant stakeholders' communities; effectively share meaningful cyber security information; and prioritize the protection of critical infrastructures.

In the following we focus on the most prominent regulatory efforts and we report excerpts, related to cyber security in critical infrastructure and information sharing, collected from the aforementioned European and American bills.

5.1. *EU cyber security strategy: "An open, safe and secure cyberspace"*

This strategy (European Commission, 2013) clarifies the principles that the European Union intends to follow with regard to cyber security policy within the Union and internationally. Through this document, the European Commission (EC) aims to tackle crucial challenges such as protecting fundamental rights, freedom of expression, personal data and privacy, guaranteeing the Internet's integrity and security to allow safe access for all, supporting a multi-stakeholders governance approach, generate awareness on the shared responsibilities public authorities, private sector and individual citizens have to take action to protect themselves, and ensure a coordinated response to strengthen cyber security. Several strategic priorities and actions that can enhance the EU's overall performance are identified within the strategy.

Particularly relevant, for the scope of this article, is the request expressed in these priorities to establish common minimum requirements for NIS that would require each Member State to set up a well functioning CERT and adopt a national and international NIS cooperation plan. Sharing information and mutual assistance among the national NIS competent authorities is identified as a primary requirement in order to coordinate prevention, detection, mitigation and response to cyber attacks. Private and public players in different areas (i.e., energy, transport, banking, public administration, etc.) are requested to perform appropriate risk management and share identified information with the national NIS competent authorities. Incidents with a significant impact on the continuity of core services must be reported to the same authorities, that will in turn exchange this information, if necessary, with cooperating regulatory bodies and law enforcement authorities.

Another priority set in this strategy is the fight against cyber crime. For this purpose, the EC is asked to support the European Cybercrime Centre (EC3) in providing analysis, intelligence, investigations forensics, facilitating cooperation and creating channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders.

Moreover, the EC is aiming to develop a cyber defense policy framework to protect networks according to the Common Security and Defence Policy (CSDP) mission. Implementing dynamic risk management, threat analysis and information sharing are crucial objectives of this mission.

In order to face the complexity of managing cyber incidents within the interconnected networks of the Union, the strategy instructs all the different involved actors (NIS competent authorities, CERTs, law enforcement and industry) on roles and responsibilities they should take both on a national and EU level. National governments are most suitable for carrying out prevention and response to cyber incidents and attacks, and establish contacts and networks with the private

sector. At the same time, a national response requires EU-level involvement to be effective.

5.2. EU Network Information Security Directive

The Network Information Security Directive proposal (European Commission, 2015) is a key component of the overall strategy and requires all Member States, key Internet enablers and critical infrastructure operators, such as e-commerce platforms, social networks, and operators in energy, transport, banking and healthcare services, to ensure a secure and trustworthy digital environment throughout the EU.

The directive appoints the European Network and Information Security Agency (ENISA) to assist Member States and the Commission by providing expertise and advice. ENISA should ensure effective and timely information sharing between the Member States and the Commission through the establishment of a cooperation network. Within the cooperation network, a secure information-sharing infrastructure should be put in place, allowing the exchange of sensitive and confidential information. Only Member States proving that their technical, financial, and human resources and processes fulfill the high security requirements, will be eligible to get access to the sharing infrastructure.

According to the Directive, early warnings should be notified within the network only in the case of significantly severe incidents or risks that may affect more than one Member State and therefore require coordination of the response at Union level. In the notification process, particular attention should be paid to preserving informal and trusted channels of information-sharing between market operators and between the private and public sectors.

The Commission shall be empowered to adopt a Union NIS cooperation plan providing for: i) a definition of the format and procedures for the collection and sharing of compatible and comparable information on risks and incidents by competent authorities, ii) a definition of the procedures and the criteria for the assessment of the risk and incidents by the cooperation network. In case of incidents resulting in personal data breaches and in case the sharing of information on risk and incidents within the cooperation network should require the processing of personal data, the competent authorities shall work in close cooperation with personal data protection authorities in order to meet the objectives of public interest legitimate under Article 7 of Directive 95/46/EC.

5.3. US White House Executive Order (EO 13636) – improving CI cyber security

This Executive Order (EO) (White House, 2013a) published on February 12, 2013 strengthens the cyber security of critical infrastructures (CI) by increasing information sharing and by jointly developing and implementing a framework of cyber security practices with US industry partners. The EO strengthens the US government's partnerships with critical infrastructure owners and operators to address cyer threats through:

1. New information sharing programs to provide both classified and unclassified threat and attack information to US companies.
2. The development of a Cyber Security Framework. The EO directs the NIST to lead the development of a framework of cyber security practices to reduce cyber risks to critical infrastructure.

The EO requires federal agencies to produce high-informative unclassified reports of cyber threats and requires the reports to be shared with US private sector entities in a timely manner to enable these entities to protect themselves against potential cyber attacks. Moreover, classified reports should also be generated and disseminated only to critical infrastructure entities authorized to receive them. A system for tracking the production, the dissemination and the disposition of classified reports should be established. The EO also expands the Enhanced Cybersecurity Services program (Department of Homeland Security, 2013), enabling near real time sharing of cyber threat information to assist participating critical infrastructure companies in their cyber protection efforts.

The framework also assists the organizations in incorporating privacy and civil liberties as part of their cyber security program.

5.4. US Presidential Policy Directive (PPD-21) – critical infrastructure security and resilience

This Directive (White House, 2013b) updates the national approach on critical infrastructure security and resilience. According to this Directive, security and resilience of American critical infrastructures should be strengthened by embracing the following three strategic imperatives.

Imperative 1: Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience. Collaboration and information exchange between and among the Federal Government, critical infrastructure owners and operators should be facilitated. As part of a redefined structure, two national critical infrastructure centers operated by the Department of Homeland Security shall be established: one for physical infrastructures and another for cyber infrastructures. They shall serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information.

Imperative 2: Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government. Efficient exchange of information between governments and critical infrastructure owners and operators is essential for secure and resilient critical infrastructures. It should be enabled through timely exchange of threat and vulnerability information, as well as information allowing the development of a situational awareness capability during incidents. Requirements for data and information formats and accessibility, system interoperability, and redundant systems need to be therefore identified.

Imperative 3: Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructures. Operational and strategic analysis on incidents, threats, and emerging risks should be performed at the intersection of the two national centers (as identified in Strategic Imperative 1). It shall include the capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information to: aid in prioritizing

Table 1 – Subjects addressed in the different EU and US regulatory initiatives.

Regulated subject	EU CS strategy	EU NIS directive	US WH EO 13636	US PPD-21
Scope of the regulation	Cyberspace	CI NIS	CI Cyber Security	CI Cyber Security
Cooperation type	Public–private sector	Public–private sector	Public–private sector	Public–private sector
Coordination between entities	National and international NIS cooperation plan	ENISA coordinates and establishes cooperation network between Member States and the Commission	NIST leads the development of a framework of cyber security practices.	Department of Homeland Security shall establish and operate national critical infrastructure centers.
Information sharing infrastructure	National CERT in each Member State. Stakeholders shall share info with NIS competent authorities.	Info-sharing platform for exchange of sensitive information within the cooperation network	—	Two national CI centers: one for physical infrastructures and another for cyber infrastructures.
Cyber defense policy	Implement risk management, threat analysis, info sharing	Union NIS cooperation plan defines risk assessment procedures.	Federal agencies produce and share unclassified reports of cyber threats with CI operators in a timely manner.	Operational and strategic analysis on incidents, threats, and emerging risks performed at the intersection of the two national centers.
Format and procedure for collection and sharing information	—	Compatible and comparable information on risks and incidents shall be shared by member states.	Provide classified and unclassified threat and attack information to companies. Near real time sharing of cyber threat information.	Timely exchange of threat and vulnerability information. Identify data formats and accessibility, system interoperability, and redundant systems.
Privacy	Considered but only partly addressed	Personal data protection authorities shall be involved when required.	Considered but only partly addressed	—

assets and managing risks to critical infrastructure, anticipate interdependencies and cascading impacts, recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident, and to support incident management and restoration efforts related to critical infrastructure.

The legal initiatives reviewed in the previous sections are summarized in Table 1. The table provides an overview on the main subjects that the different documents analyze. It also highlights the different approaches the initiatives suggest, or demand to adopt, in order to address the various issues.

6. Dimension III: standardization efforts

A wide variety of official recommendations from standardization bodies, such as NIST or ENISA, exists, which are a valuable source of information when setting up information sharing procedures.

6.1. *ENISA: Proactive Detection Of Network Security Incidents*

ENISA carried out a study to investigate ways in which CERTs detect incidents, the tools and services they utilize for discovering malicious activities, identify good practices and recommend measures to other CERTs, and analyze the problems they face. The results of the study are presented in the report *Proactive Detection of Network Security Incidents* (ENISA, 2011b), which also offers recommendations to relevant stakeholders on what can be done to further push this process. The study has identified that CERTs are currently not fully utilizing all possible external sources at their disposal, some of them do not collect incident data about other constituencies or do not share these data with other CERTs. These and other shortcomings in the process of detection of incidents are examined in-depth in the report, both on a technical and legal/organizational level, and for each identified shortcoming, one or more recommendations are formulated. They are aimed at a) data providers, b) data consumers and c) organizations at the EU or national level.

For **data providers** key recommendations focus on suggestions on how to better reach out to CERTs, more suitable data formats and distribution approaches as well as data quality improvement and enrichment. In order to fulfill the high privacy constraints about shared information, data providers should screen potential data recipients for eligibility, establish contacts with security institutions and communities, and create an easy process of registration for clients.

To attract high-quality data sources and allow sharing of information in one of the commonly accepted ways and formats, data providers should adopt existing standards for sharing of incident information, use standard data transportation methods such as HTTPS, SCP or SFTP, include in the delivered data information that would allow correlation between various sources (e.g., timestamps of events, Autonomous System Number (ASN), affected IP addresses or domain names, type of incident/exploit/malware etc.), deliver the information to clients as soon as it becomes available, include

detailed description of the methods that are used for acquiring information about incidents, and, finally, adding context and classification.

For the purpose of increasing the quality of delivered data, ENISA (2011b) recommends data providers to enrich incident information with additional meta data and thus provide insights into observed events. In order to decrease the number of false positive classifications, strict filtering, consequent verification and correlation of data are also suggested. According to the report, it would be moreover necessary to keep data stored for historical reference and research purposes and offline analysis while implementing data aging mechanisms to remove data from blacklists.

For **data consumers** a guide on how to acquire access to datasets is given in ENISA (2011b). The report puts forward suggestions on better integration of external feeds with internal monitoring systems; additional activities that can be performed by a CERT to verify the quality of data feeds, along with specific deployments of new technologies, are also enumerated.

According to this report, organizations which apply access to a data source should first select the most appropriate sources for their situation; they should then develop their own monitoring capabilities or install sensors in their networks to allow the providers to gather data for the use of the service. Moreover, it is recommended that they establish relationships with security communities (e.g., with FIRST, TF-CSIRT, APCERT, etc.) to gain trust and speed up the process of verifying eligibility to access restricted data feeds. Finally, data consumers are asked to be aware of potential legal issues concerning data sharing when applying for services that require setting up a sensor or sharing data.

With respect to best practices, data consumers should implement automation systems that allow the processing of incident data. These systems should therefore be able to handle data in many different formats, storing it in a database which allows offline analysis, correlation and visualization, and integrate their own data with data from external sources. Incoming data feeds need constant verification. Therefore, data receivers should develop methods and criteria for assessing the quality of the data sources, verifying incident information before submitting it to database or incident handling software. Data correlation with external services is recommended in order to enrich it with additional data and filter duplicate events. If a feedback mechanism is in place, a data consumer should eventually use it to give data providers information to improve the quality of the service they offer.

Since a data consuming CERT may become a data provider, data consumer CERTs are encouraged to deploy their own monitoring mechanisms, such as sensor networks, client honeypot technologies, sandbox technologies, and passive DNS monitoring.

Finally, at the **EU or national level**, activities are pointed out that are aimed at achieving a balance between privacy protection and the security provision needs, the encouragement of the adoption of common formats and underused technologies, and the integration of statistical incident data on a wider scale. Research is also suggested into the area of data leakage reporting.

6.2. *ISO/IEC27010: information technology – security techniques – information security management for inter-sector and inter-organizational communications*

This international standard (ISO, 2012) provides guidelines and general principles on how to share confidential information regarding IT security threats, vulnerabilities and/or incidents between or within a community of organizations, for example when private companies, governments, law enforcement and CERT-type bodies are collaborating on the investigation, assessment and resolution of serious pan-organizational and often international or pan-jurisdictional cyber attacks. The standard is designed to support the creation of trust when exchanging and sharing sensitive information, thereby encouraging the international growth of information sharing communities.

Among the general recommendations, the standard demands the establishment of information sharing communities. To be effective, these communities should have common interests which define the scope of the shared sensitive information. Moreover, organizational structures and management functions applying to community information security management should be clearly defined. Information exchanged within the community needs to be classified in terms of its value, legal requirements, sensitivity, credibility and criticality to the organization. Adequate protection of shared information has to be guaranteed in a consistent manner. Where anonymity is requested, any information identifying the source of the information exchange should be removed.

To securely exchange sensitive information among the information-sharing community parties, designing, implementing and monitoring processes to provide a secured flow of information on a timely basis is required. Information should, through this process, be disseminated to the appropriate persons, providing reasonable assurance that the information will not be used for malicious purposes or inappropriately redistributed. Secure and resilient communications between community members should also include risk knowledge and management, monitoring and dissemination.

The greatest benefits in sharing information can be experienced by organizations operating within the same sector or with the same corporate objectives, sharing sector-specific categories of information security risk. Nevertheless, sharing information across sectors can be fruitful either if communities are defined by geographical location or if a hierarchical structure of communities is in place.

Information sharing communities should moreover define rules and conditions governing their operations, including: objectives of the community, procedures for joining and leaving the community, obligations of community members, disciplinary and expulsion processes and criteria, rules for usage of shared information, legal and financial obligations.

An information exchange agreement should specify the types of information (e.g., *announcements*, *alerts and warnings*, *incident handling*, *information requests*, *quality of service predictions* etc.) that may be exchanged between members of the community in order to allow the members to design and implement appropriate security measures for the sensitivity level of the shared information. Sharing too much information could

be as bad as sharing too little, unless a suitable method of data filtering is utilized.

6.3. NIST: framework for improving critical infrastructure cybersecurity

As mentioned in Section 5.3, the Executive Order calls for the development of a voluntary risk-based Cyber Security Framework. The resulting Framework (NIST, 2014a), created through collaboration between government and the private sector, was published on February 12, 2014, and addresses and manages cyber security risk in a cost-effective way based on business needs.

The Framework focuses on using business drivers to guide cyber security activities and considering cyber security risks as part of the organization's risk management processes. It consists of three parts: the *Framework Core*, the *Framework Profile*, and the *Framework Implementation Tiers*.

The ***Framework Core*** is a set of cyber security activities, outcomes, and informative references that are common across critical infrastructure sectors. It provides detailed guidance for developing individual organizational Profiles. It presents industry standards, guidelines, and practices in a manner that allows for communication of cyber security activities and outcomes across the organization, from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions: *Identify*, *Protect*, *Detect*, *Respond* and *Recover*. When considered together, these functions provide a high-level, strategic view of the life-cycle of an organization's management of cyber security risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

Profiles are defined to help organizations in aligning their cyber security activities with their business requirements, risk tolerances, and resources. A Framework Profile represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cyber security posture by comparing a "Current" profile with a "Target" profile. To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

The ***Tiers*** support organizations in understanding the characteristics of their approach to managing cyber security risk. Framework Tiers provide context on how an organization views cyber security risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cyber security risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses, to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

The Framework also includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cyber security activities. While processes and existing needs will differ, the Framework can assist organizations in incorporating privacy and civil liberties as part of a comprehensive cyber security program. Moreover, the Framework enables organizations to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework finally provides organization and structure to today's multiple approaches to cyber security by assembling standards, guidelines, and practices that are working effectively in the industry today.

6.4. Recommendation ITU-T X.1500 cyber security information exchange techniques

Recommendation ITU-T X.1500 (ITU-T, 2012) was approved in April 2011 and describes techniques to enhance cyber security through coherent, comprehensive, global, timely and assured information exchange. It presents a cyber security information exchange (CYBEX) model and discusses techniques that can be used to facilitate the exchange of cyber security information. The techniques include the structured global discovery and interoperability of cyber security information in such a way as to allow for continual evolution to accommodate the significant activities and specification evolution occurring in numerous cyber security forums. The general cyber security information exchange model used in this Recommendation consists of basic functions, listed in the following, that can be used separately or together as appropriate, and extended as needed in order to facilitate assured cyber security information exchanges.

- Structuring cyber security information for exchange purposes;
- Identifying and discovering cyber security information and entities;
- Establishment of trust and information exchange policy agreements between exchanging entities;
- Requesting and responding with cyber security information;
- Assuring the integrity of the cyber security information exchange.

For the exchange of cyber security information to occur between any two entities, the exchange must be structured and described in some consistent manner that is understood by both of those entities. For the purposes of accomplishing these exchanges, cyber security information includes structured information or knowledge concerning the following characteristics: the state of equipment, software, or network-based systems as related to cyber security, especially

Table 2 – Cyber security information exchange groups and corresponding relevant techniques, standards and protocols.

Group	Techniques/Standards/Protocols
Weakness, vulnerability and state	CVE, CVSS, CWE, CWSS, OVAL, XCCDF, CPE, CCE, ARF
Event, incident, and heuristics	CEE, IODEF, CAPEC
Information exchange policy	TLP
Identification, discovery, and query	OID arc, CYIQL
Identity assurance	TPM, TNC, entity authentication assurance, and extended validation certificate framework
Exchange protocol	RID, HTTPS, BEEP, SOAP

Table 3 – Aspect addressed by the different standardization efforts.

Recommended matter	ENISA report	ISO/IEC 27010	NIST framework	ITU-T X.1500
Protection of shared information	✓	✓		✓
Cyber security risk management		✓	✓	
Privacy preservation in information sharing	✓	✓	✓	
Data format, protocols and standards	✓			✓
Data quality improvement	✓			
Incident handling process	✓	✓		✓

vulnerabilities; forensics related to incidents or events; heuristics and signatures gained from experienced events; cyber security entities involved; specifications for the exchange of cyber security information (including modules, schemas, terms and conditions) and assigned numbers; the identities and assurance attributes of all cyber security information; and implementation requirements, guidelines and practices.

As a means of describing at a general level the desired attributes of cyber security information exchange, the structured information capabilities are organized into six *clusters* of techniques for distinct cyber security information exchange groups. The clusters along with the corresponding relevant techniques, standards and protocols are reported in Table 2.

6.5. *Overview on information sharing standardization efforts*

The standardization efforts described in the previous sections are summarized in Table 3. The table provides an overview on the principle matters the different documents aim to address with their recommendations.

While the ENISA report provides generic recommendations covering a wide set of matters regarding cyber security information sharing, the NIST framework targets American (and non) organizations, focusing mostly on risk management procedures and privacy preservation aspects. The guidelines included in the ISO/IEC27010 standard and in the ITU-T X.1500 are oriented toward the the protection of the data exchanged in the information sharing process, as well as to the collection, analysis and correlation of cyber incidents in order to obtain an effective mitigation strategy. Techniques standards and protocols for systems monitoring, threat detection, vulnerability inventory and incident exchange are analyzed in deep detail in the ITU-T X.1500 document, but are also taken into account by the ENISA report and the NIST framework.

7. Dimension IV: regional and international implementations

CERTs are a vital part of every regional cyber security ecosystem. They collect information on new threats, maintain mailing lists to issue early warnings and, in certain cases, provide help on request. CERT cooperation has proved to be the most effective within regions. This can be easily explained, as short travel times and overall relatively low costs stimulate more frequent personal meetings. Another important aspect is the similarity of the cultural backgrounds of the participating teams which make social networking easier and facilitates common projects.

However, the global nature of cyber threats also calls for international collaborations. Therefore, CERTs are also internationally well connected with each other, and additionally to them, well-connected (national) cyber centers are emerging. These initiatives and their background are studied in this section.

7.1. *Computer emergency response teams*

Asia: APCERT[10]: Formed during the first *Asia-Pacific Security Incident Response Coordination (APSIRC)* meeting in Japan in March 2002, with the aim of improving working relationships between CERT neighbors across national borders, APCERT is the vehicle for regional cross border cooperation and information sharing. In February 2003, 15 CERT teams from the 12 Asia Pacific economies accepted the APCERT agreement. APCERT aims at maintaining a trusted contact network of computer security experts in the Asia Pacific region to improve the region's awareness and competency in relation to computer security incidents, enhance Asia Pacific regional and international cooperation on information security, jointly develop measures to deal with large-scale or regional network security incidents, promote

[10] http://www.apcert.org; April 2016.

collaborative research and development on subjects of interest to its members, assist other CERTs in the region to conduct efficient and effective computer emergency response, and provide input and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries.

Europe: TERENAs TF-CSIRT[11]: Due to different interests and needs of various networks in Europe, CERT teams agreed that establishing a permanent operational European CERT coordination center would not be possible. Nevertheless, cooperation and development in certain areas are still a common interest for some teams. Sharing statistical data about incidents in order to observe common trends, developing an European accreditation scheme, establishing education and training and assisting new teams are some of the main common objectives of this cooperation that led the Euro-CERT group, in May 2000, to form a task force of TERENA called *TF-CSIRT*.

Europe: NORDUnet CERT[12]: One of the regional CERT initiatives that aims to better coordinate incident handling and cooperation among Northern European countries is *NORDUnet CERT*. NORDUnet CERT performs security incident handling in cooperation with the Nordic national research networks. As NORDUnet is the Nordic Internet highway to research and education networks in Denmark, Finland, Iceland, Norway and Sweden, NORDUnet CERT fulfills the coordination role for all the national CERTs in these countries. Each CERT operates in its own country and is independent in operation, and can be a member of international organizations (TERENA TF-CSIRT, FIRST). Nevertheless, those teams have established a network of peers which is also a "Web of Trust". NORDUnet CERT also plays a role in international contacts since it is a member of FIRST and TF-CSIRT.

South America: CLARA (Cooperation of Advanced Networks in Latin America) has established a working group, among CERTs in the region of South America and the Caribbean, to address two major security issues. First, the group is focusing on the protection of the critical infrastructure of *REDClara*.[13] Second, it deals with the creation of security working groups in the NRENs called CLARA WG-CSIRT. With regard to this, the goals of CLARA WG-CSIRT are: (i) to establish a work framework, in terms of security, for each NREN; (ii) to promote the development of new working groups dealing with security in Latin America and the region through training programs aimed at working group members; (iii) to promote the exchange of data and information on related problems, incident management, etc.; (iv) to promote coordinated and prompt reactions for security incidents occurring on REDClaras infrastructure and that of each NREN; (v) to build a data base of contact points responsible for security in each NREN; and (vi) to cooperate with similar initiatives, such as TF-CSIRT and APCERT.

North America: In the United States, *USCERT (United States Computer Emergency Readiness Team)*,[14] with the support of the CERT/CC team, has organized several CSIRT meetings, which brought together product vendors, security vendors, service providers, industry, academia, and government. The United States government also cooperates with the sector *Information Sharing and Analysis Centers (ISACs)*, hosting meetings limited to organizations dealing with the protection of critical national infrastructure. Specifically, the *Information Technology Information Sharing and Analysis Center (IT-ISAC)* is established as a trusted community of security specialists, from companies across the Information Technology industry, dedicated to protecting the Information Technology infrastructure by identifying threats and vulnerabilities to the infrastructure, and sharing best practices on how to quickly and properly address them. The IT-ISAC also communicates with other sector specific ISACs, enabling members to understand physical threats, in addition to cyber threats. Taken together, these services provide members a current and coherent picture of the security of the IT infrastructure.

7.2. *International cooperations*

A crucial factor for successful incident handling is a well established cooperation among countries (Herzog, 2011) and/or CERTs respectively. These collaborations aim to better address the global character of Internet security threat propagation. Moreover, many CERT services are strongly dependent on collaborations with other teams located in different parts of the world. Here, we briefly review the role of the *Forum for Incident Response and Security Teams (FIRST)* in building the international community of CERTs. Furthermore, we show some examples of sector cooperation initiatives; finally, we report two cross-regional cooperation cases: region to region cooperation and cooperation among member states from two different regions in the same organization.

7.2.1. *FIRST – Forum for Incident Response and Security Teams*

FIRST is an organization formed in 1990 with the goal of establishing better communication and coordination between incident response teams. Today the FIRST membership consists of 286 teams across 61 countries from a variety of organizations including educational, commercial, vendor, government and military. Membership in FIRST enables incident response teams to respond to security incidents by providing access to best practices, tools, and trusted communication with member teams. FIRST members develop and share technical information, tools, methodologies, processes and best practices. It encourages and promotes the development of quality security products, policies and services, develops and publishes best practices, promotes the creation and expansion of incident response teams and memberships from organizations from around the world.

7.2.2. *Sector cooperation*

A sector specific CERT is mainly characterized by the type of constituency and the responsibilities it has. Common constituency and similar responsibilities represent incentives to cooperate; some teams, being in private or public sector, affiliate and start cooperations because of their common area of interest.

[11] http://www.terena.org/activities/tf-csirt/; April 2016.
[12] http://www.nordu.net/; April 2016.
[13] REDClara is the network connecting Latin America National Research and Education Networks (NRENs) with each other and Europe. More at http://www.redclara.net; April 2016.
[14] https://www.us-cert.gov; April 2016.

The *European Government CSIRTs* group (EGC) is an informal group of governmental CERTs. Given the similarity in constituencies and problem sets between its members, this group aims at developing methods for incident response, taking advantage of the cooperation between its members. EGC members carry out different activities in order to reach this objective. They develop measures to deal with network security incidents, enable information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities, identify areas of specialist knowledge and expertise to share within the group, identify areas of collaborative research and development, and communicate common views with other initiatives and organizations. Moreover, EGC members cooperate with other international CERT initiatives dealing with vulnerabilities and incident management on a global scale (e.g., many EGC teams are members of FIRST and TFCSIRT).

7.2.3. *Cross-regional cooperation*

Cross-regional cooperation between different teams and organizations exists and is usually based on the exchange of knowledge and experience at physical meetings.

One example is the *Central and Eastern European Networking Association (CEENet)*,[15] which is an association of 23 national academic, research and educational organizations from Europe and Asia regions. CEENet's mission is to coordinate the international aspects of the academic, research and education networks in Central and Eastern Europe and in adjacent countries. Since there are substantial differences in ICT developments among members of this organization, sharing of information between those countries is a key element to achieve acceptable average level of ICT security across the whole region.

Another example of cross-regional cooperation is the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). It is one of NATO Centres of Excellence, located in Tallinn, Estonia. The Centre was established on May 14, 2008; it received full accreditation by NATO and attained the status of International Military Organization. NATO CCD COE, is an international military organization with a mission to enhance the capability, cooperation and information sharing among NATO, its member nations and partners in cyber defense by virtue of education, research and development, lessons learned and consultation. Among others, NATO CCD COE develops recommendations, manuals and guidelines for national and international cyber security (see NATO Cooperative Cyber Defence Centre of Excellence, 2012, NATO Cooperative Cyber Defence Centre of Excellence, 2011, and NATO Cooperative Cyber Defence Centre of Excellence, 2010).

7.3. *IT crisis management*

Some of the (mainly) Western countries have recently started to establish IT crisis management centers with the purpose of addressing cyber security issues and generate cyber situational awareness (D'Amico et al., 2005; Jajodia et al., 2010). These centers are the main sources of information with regard to national cyber security for critical infrastructures. They offer expertise and advice through services available on a 24/7 basis. Besides providing information, a crisis management center must always have a reliable picture of the current IT security situation in the country. For this reason, monitoring procedures are put in place on the governmental and critical infrastructure networks. A tight cooperation with the national CERT is usually also established in order to keep a close contact with national and international partners. Germany and the Netherlands have been among the first European countries deploying national IT crisis management centers, and are described here.

In the German case a clear separation of tasks between 4 different entities is foreseen.[16] The *CERT-Bund* performs the computer emergency response operations; the *BSI IT Situation Center* carries out monitoring functions, informs about alerts and early warnings, and reacts to IT security incidents; the *BSI IR Crisis Reaction Center* is in charge of national crisis management by resolving disruptions of the information infrastructure; finally, the *Cyber Response Center* cooperates with other federal agencies when necessary.

The Dutch IT crisis management operations are, instead, concentrated in a single entity called *National Cyber Security Center (NCSC)*.[17] The services delivered by this center are very similar to the ones provided by the German centers. Moreover, the NCSC plays a key role in operational coordination during an ICT crisis. It provides support in (large-scale) cyber exercises and scenarios, contributing to the development of a high level preparedness. Finally, it facilitates the ICT RESPONSE Board (IRB), allowing public–private partnerships to take place; meeting and cooperation processes are organized by the IRB while an ICT crisis is occurring or is threatening the security of the country.

An example of a non-European IT crisis management center is the *Canadian Cyber Incident Response Centre (CCIRC)*.[18]

8. Dimension V: technology integration into organizations

As described in the previous section, much progress has been made recently in establishing national/governmental cyber security centers worldwide. All these entities are at different maturity levels and face the challenge of coordinating responses to global cyber attacks not only within national boundaries, but also at a cross-border level. Cooperation between many of these centers has led to visible results (TF-CSIRT, CEENET, North America CSIRT meeting, FIRST SIGs, and E-COAT are examples of development of best practices, code of conduct, recommendations for legislation, etc. obtained by effective collaboration of international teams; ENISA, 2006), but there are still obstacles left that make seamless security information exchange and sharing a less cumbersome task. Among the main problems, which hinder effective information sharing, are technical barriers. This section therefore

[15] http://www.ceenet.org; April 2016.

[16] https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/itcrisismanagement_node.html; April 2016.

[17] https://www.ncsc.nl/english/; April 2016.

[18] http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx; April 2016.

highlights the state of the art[19] in terms of technical platforms, tools, standards, and open protocols regarding security information exchange and management.

8.1. Open web-platforms and open source tools

As reported in the survey ENISA (2013a), a number of initiatives exist that aim to make data sharing effective among CERTs. These initiatives are developed by CERTs, NATO, or by private companies and are driven by "cyber community" interests. Some initiatives have already attracted solid user communities, and they tend to be user-friendly and flexible, as they are mostly open source. On the other hand, as pointed out in ENISA (2011b), CERTs are still often focused on detecting and remedying a single incident rather than identifying and understanding larger events that encompass small individual attacks.

Even in the case of simple cyber incidents, correlation has been proven useful to gain better insight, eliminate false positives, or detect duplicates. Incident correlation is the process of comparing different events, coming from multiple sensors and data sources, in order to identify patterns and relationships, enabling the identification of events belonging to one attack or indicator of broader malicious activity. It allows to better understand the nature of an event, to reduce the workload needed to handle incidents, and to automate the classification and forwarding of incidents that are only relevant to a particular constituency. Correlation is useful for both in the case of processing data from multiple tools on a monitored network and in the case of using multiple different external services that supply incident data.

SIEM (Security Information and Event Management) tools are used to perform correlation on the enterprise level, by analyzing information derived from very varying datasets, and are already available on the market. However, commercial solutions often come at high costs, while the open-source solutions are usually harder to manage. There is still no standard framework that defines how to get to the root cause of an incident by fully utilizing all data feeds available to a CERT/CSIRT team. Emerging solutions that enable correlation of external services that provide incident data, such as Megatron[20] or AbuseHelper,[21] are becoming available now, but are still not mature. The need for such tools is recognized by many CERTs, but they remain underemployed.

In the following section, we provide a short comparison between some of the open web-platform and open source tools that are currently employed by CERTs and cyber security centers, for information sharing and data correlation.

8.1.1. Threat intelligence sharing

The reliable detection of security breaches has become hard by using traditional signature-based methods only, because today's highly-sophisticated attacks aim to circumvent known signatures and exploit multiple vulnerabilities on different systems at the same time (FireEye, 2013). Therefore, organizations need to share higher-level threat intelligence data to be able to quickly adapt their systems to new threats using machine-digestible formats that remove human delay from intelligence sharing. Some of the most popular intelligence sharing tools are here revisited and compared.

OpenIOC (Open Indicators of Compromise)[22] is an open framework for sharing threat intelligence and consists of an extensible XML schema describing the technical characteristics that define a known threat, an attack methodology or other artifacts left by an intrusion. Organizations that join the OpenIOC community get access to threat intelligence shared within a network of more then 1000 entities. In order to enable an organization to document and categorize forensics artifacts of an intrusion identified on a host or network, a simple XML schema needs to be filled in with the related information about the indicators of compromise. Simplicity is indeed one of the biggest advantages of using OpenIOC. Further usage of OpenIOCs is straightforward, given that utilities to parse and convert XML into other formats are easy to implement. On the other hand, OpenIOC is not largely adopted outside of Mandiant products, and has a limited support for network-based IoCs, focusing more on file-based IoCs.

The *Malware Information Sharing Platform (MISP)*[23] is another open-source software developed by the Belgian Defense CERT and the NATO Computer Incident Response Capability (NCIRC). MISP provides a central IoC database where technical and non-technical information about malware and attacks are stored in a structured format. It automatically creates relations between malware, events and attributes. It allows the integration with other systems by generating IDS, OpenIOC, plain text and XML outputs. Automatic sharing of information is enabled between trust groups, but also sub-communities can be created in order to selectively share certain data with certain parties. Finally, an automatic notification system, using PGP, is foreseen.

8.1.2. Data correlation tools

As pointed out in ENISA (2013a), data providers are recommended to employ correlation methods to remove false positives and duplication of data. The data consumers, on the other hand, are strongly recommended to implement their own solutions for verifying datasets to help improve quality of data before forwarding them to their constituencies. Some organizations try to implement event correlation mechanisms both on received datasets and on the output generated from their own monitoring solutions. Extracting common behavior patterns and relations between incidents is no trivial task.

We reviewed the main open-source solutions for data correlation and categorized them in three different groups: generic correlation tools, SIEM tools and tools for incident handling providing information correlation features. The main characteristics of each tool along with the input and output data type are reported in Table 4.

[19] Notice that we left commercial products out intentionally, as it is not our goal to advertise certain products here, and thus rather survey tool/solution categories with open-source alternatives.

[20] https://www.cert.se/; April 2016.

[21] http://www.abusehelper.be; April 2016.

[22] http://www.openioc.org; April 2016.

[23] https://github.com/MISP/MISP; April 2016.

Table 4 – Comparison between the main open-source correlation tools.

Tool	Developer	Type	Input format	Output format	Description
SEC	Risto Vaarandi, Tallin Univeristy of Technology	Generic	Files, named pipes, standard input	Files, mails, TCP and UDP packets, etc.	Text lines are processed in order to detect certain event groups occurring in a predifined time window, according to rules defined in a configuration file.
LogHound	Risto Vaarandi, Tallin Univeristy of Technology	Generic	Log files	Files	Finding frequent patterns from event log data sets with the help of a breadth-first frequent item set mining algorithm
iView	Cyberoam	SIEM	Logs and reports related to intrusions, attacks, spam and blocked attempts	Reports based on the user identity	Centralized reporting from multiple devices across geographical locations; it allows to view information across hundreds of users, applications and protocols; it correlates the information, giving the user a comprehensive view of network activity
OSSIM	AlienVault	SIEM	Logs and information from security controls and detection systems	Summary and statistical reports related to the operation of the system threat reports provided by the community	Combines log management and asset management and discovery with information from dedicated information security controls and detection systems. This information is then correlated together to create contexts to the information not visible from one piece alone.
Abuse Helper	CERT.FI (Finland) and CERT.EE (Estonia)	Incident handling	Incidents notifications and Internet abuse handling related information	Reports in different formats, via different transports	Aggregates internet abuse handling related information, retrieved via several sources, based on different keys, such as AS numbers or country codes
BGPrank	Computer Incident Response Centre Luxemburg (CIRCL)	Incident handling	Dshield, Shadowserver, Arbor ATLAS	BGP Ranking	Ranks autonomous system (AS) numbers based on malicious activities. A trust ranking scheme is implemented based on existing dataset of compromised systems, malware C&C IP and existing datasets of the ISPs.
CIF	Wes Young at REN-ISAC	Incident handling	IP addresses, domains and URLs that are observed to be related to malicious activity	Series of messages "over time" (e.g., reputation)	Combines known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route).

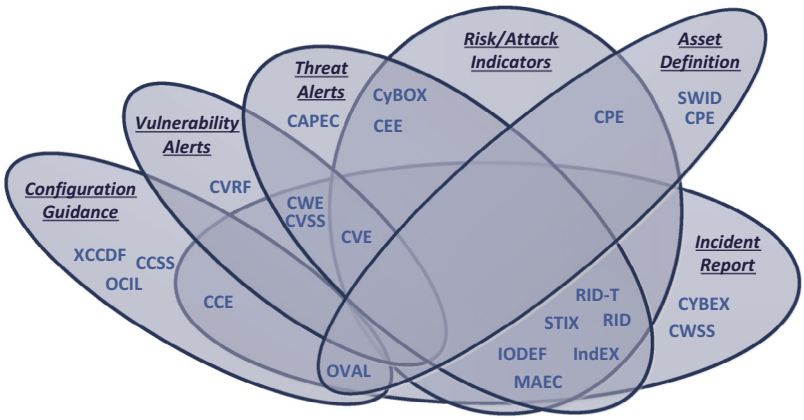

Fig. 2 – Knowledge areas covered by the different existing standards. For further information on the abbreviations, see Hernandez-Ardieta et al. (2013).

8.2. *Technical standards and protocols*

In order to achieve effective defensive actions while performing incident analysis, automated systems that assist operators need to be put in place. To cope with the growing complexity of the threat landscape, the increasing frequency at which cyber events occur, and the growing amount of data that need to be handled in cyber threat intelligence and threat information sharing, human analysis alone is not sufficient anymore. Automation is therefore becoming a fundamental asset to build defensive capabilities. Moreover, given the heterogeneous architectures, products and systems being used as source of data for the information sharing systems, standardized, structured threat information representations are required to allow a satisfying level of interoperability across organizations.

The exchange of information in both a human readable and machine-parsable form has clear advantages: while basic data collection, categorization and correlation are best performed by machines, the intelligence information generation itself is largely driven by human analysts, who perform types of analysis that are most of the time unsuitable for automation.

Performing a 2-stage process where incident data are first automatically collected, parsed, filtered and subsequently thoroughly analyzed by human experts to generate intelligence, is essential in incident handling for critical infrastructure. This approach leverages the benefits of machine learning methods to preliminarily process large amounts of raw data, and dramatically reduces the chance of overlooking critical security information (lowering therefore the false positive rate) by employing human experts able to identify, highlight, and analyze the most relevant data.

In addition, because of the different quality of shared threat information, the intelligence analyst has to also assess the fidelity based on the sources and methods adopted to generate the threat information. All these issues underline the need for structured representations of threat information that are expressive, flexible, extensible, automatable and human-readable.

An overview of the existing efforts is given in Fig. 2 where concurrent standards are grouped into six different knowledge areas: **Asset Definition** (inventory); **Configuration Guidance** (analysis); **Vulnerability Alerts** (analysis); **Threat Alerts** (analysis); **Risk/Attack Indicators** (intrusion detection); and **Incident Report** (management). The figure depicts how some standards cover different knowledge areas providing a more exhaustive service, while others are developed for being employed in a specific area. For further details on the standards analyzed in the figure, see Hernandez-Ardieta et al. (2013).

Some of the aforementioned standards define the way cyber threat information should be described; they are mostly based on the exchange of Indicators of Compromise (IoCs). After IoCs have been identified in a process of incident response and computer forensics, they can be shared for early detection of future attack attempts. In order to obtain a more efficient automated processing of these indicators, there are initiatives to standardize formats for IoC descriptions. In the following, we briefly describe the two most prominent initiatives from OASIS (formerly developed by MITRE) and the IETF.

8.2.1. *OASIS standards – STIX, TAXII and others*

OASIS Cyber Threat Intelligence (CTI)[24] is a technical committee of a US standardization organization, which supports a number of (community-driven) efforts to design standards for security information sharing, including non-commercial solutions for threat modeling and transport protocols. These efforts have been started by the MITRE Corporation but transitioned to OASIS in June 2015.

Structured Threat Information eXpression (STIX)[25] is a standardized language for structured cyber threat information representation. The STIX language aims at providing comprehensive cyber threat information as well as flexible mechanisms for addressing such information in a wide range of use cases. STIX's architecture comprises a large set of cyber threat information classes, including indicators, incidents, adversary tactics techniques and procedures, exploit targets, courses of action, cyber attack campaigns, and cyber threat actors. Existing structured languages, such as Cyber Observable Expression (CybOX), Malware Attribute Enumeration and Characterization (MAEC), Common Attack Pattern Enumeration and Classification (CAPEC), can be leveraged to provide an aggre-

[24] https://www.oasis-open.org/committees/cti; April 2016.
[25] http://stix.mitre.org; April 2016.

gate solution for any single use case. Furthermore, numerous flexibility mechanisms are designed into the language so that portions of the available features are independently usable, accounting for the relevance of a specific use case.

Trusted Automated eXchange of Indicator Information (TAXII)[26] defines a set of services and message exchange mechanisms for the detection, prevention, mitigation and sharing of cyber threat information across organization and service boundaries. It allows organizations to achieve improved situational awareness about emerging threats, enabling them to share subsets of information with a selected list of partners they choose. TAXII is the preferred method to securely and automatically exchange information represented in the STIX language. TAXII use cases include public alerts or warnings, private alerts and reports, push and pull content dissemination, set-up and management of data sharing between parties. It uses a modular design that can accommodate a wide array of optional sharing models. Sharing models supported by TAXII include (but are not limited to): *Source-Subscriber*: A single entity publishes information for a group of consumers. *Peer-to-Peer*: A group of data producers and data consumers establish direct relationships with each other. All sharing exchanges are between individuals. *Hub-and-Spoke*: A group of data producers and consumers share information with each other. The information is sent to a central hub, which then handles dissemination to all the other spokes as appropriate. *Push or Pull Sharing*: Data consumers are automatically provided with new data (push), or the consumer can request updates at times of their choosing (pull).

8.2.2. *IETF standards – IODEF and RID*

The Managed Incident Lightweight Exchange (MILE) IETF Working Group defined two main standards for describing (IODEF) and exchanging (RID) incident information. Although the current implementations of IODEF and RID are mostly limited to the technical description and local exchange of IoCs, the standards are designed to allow large-scale sharing of complex incidents.

The *Incident Object Description Exchange Format* (IODEF) specification described in RFC 5070 (Danyliw et al., 2007) provides an XML representation for conveying incident information across administrative domains. The data model comprises information about hosts, networks, services running on the systems, attack methodology and associated forensic evidence, the impact of the activity, and approaches for documenting the workflow.

The *Real-time Inter-network Defense (RID)* protocol described in RFC 6545 (Moriarty, 2012) was designed to transport IODEF cyber security information. RID is flexible enough to exchange other schemas or data models either embedded in IODEF or independent of IODEF, with a transport binding using HTTP/TLS. RID is preferred for peer-to-peer models with higher levels of security and privacy.

8.3. *Organizational aspects of tools application*

One should notice that with respect to tools, there is no "one fits all" solution. Usually powerful solutions also need considerable resources to be operated, which small or medium sized enterprise often cannot afford. On the other side, there is the strong need to secure critical infrastructures by all means. Eventually, every organization needs to perform a careful consideration of the cost–benefit ratio individually.

However, in general we can conclude that some open source solutions with a quite large user community (cf. Table 4) can be installed rather quickly and operated with manageable costs – even for SMEs. Regarding standards, the ones from IETF seem to be easier to learn and apply, whereas the OASIS standards are more complex, but also more powerful – and have a large community.

9. Review of cyber incident information sharing aspects

Incident information sharing is a vital effort for future infrastructures. However, a multitude of quite diverse aspects need to be considered in order to implement and run effective systems, which have been addressed in this paper. The following section sums up the most important findings, of both technical and non-technical nature, derived from our survey, and provides recommendations for future developments.

9.1. *Public and private sector cooperation*

Both the European and the American regulations aim at achieving cyber resilience enhancing cooperation between public and private sectors in order to improve capacities, resources and processes to address cyber threats in critical infrastructures.

The US effort (White House, 2013a) points to expand the Enhanced Cybersecurity Services (ECS) (Department of Homeland Security, 2013) information sharing program, in order to enable near real time sharing of cyber threat information between critical infrastructure companies and governmental entities (Senate of The United States, 2014).

The European strategy (European Commission, 2013) intends to increase the international cooperation, (including exchanging best practices, sharing early warnings, enable joint incident management exercises and so on), intensifying the ongoing efforts to strengthen Critical Information Infrastructure Protection (CIIP) cooperation networks involving governments and private stakeholders. Moreover, the EU incentivizes the enhancement and subsequent exploitation of the synergies between civilian and military approaches in protecting critical cyber assets by the means of establishing research and development programs and closer cooperation between governments, private sector and academia in the EU.

No particular focus is reserved in these documents on sharing of information about vulnerabilities affecting the ICT "supply chain" itself. Legal frameworks regulating the discovery of traces of possible threats, such as the presence of hardware *back doors* (see Waksman and Sethumadhavan, 2011), "built-in" by IT systems manufacturers, are strongly required.

9.2. *International cooperation*

Currently cooperation between incident handling teams across the world occurs only in the form of sporadic physical

[26] http://taxii.mitre.org; April 2016.

meetings, conferences, mailing lists subscriptions and the like (ENISA, 2006). However, more structured collaboration means are required to achieve a tighter and more extensive cooperation. There are barriers which limit the possibilities to cooperate or even make cooperation impossible. Confidence between cooperating teams while handling sensitive information is most of the time prevented by international regulations that limit the exchange and usage of such information. Building a valuable level of cooperation is also a monetary issue: real life contacts between interested people are necessary, but the costs for achieving that is not always negligible. Team–Team cooperation is in many cases slowed down by the lack of service level agreements (SLAs) between cooperating entities; the incident handing process, for instance, relies on tight request/response times that need to be strictly regulated by common rules. Teams working in different countries have to comply to different legal environments. This issue influences the way the teams provide their services and therefore the way they treat particular kinds of attacks (ENISA, 2003). This especially concerns international cooperation. Moreover, although CERT team was established more than 20 years ago, there is still no developed and adopted standard for CERT operation. This hugely impedes international cooperation, making the exchange of information barely possible.

Although cooperation between international stakeholders is hampered by many obstacles, it is beneficial for all sides. Cooperating international cyber incident response teams get most benefit in terms of joint incident handling, project conducting, resource and information sharing, and (social) networking.

Having an ecosystem of (international) interconnected sharing entities (critical infrastructure providers, governments, security organizations, etc.), like the one proposed in Kaufmann et al. (2014), would indeed ease the gain of situational awareness, allowing consciousness on the current cyber security situation of all the monitored infrastructures. This is the initial step required to effectively perform cyber defense and incident response. Being part of such ecosystem enables the participating organizations to get access to a large amount of relevant security information that can be essential while defending against ongoing cyber threats. Best practices, resolved security issues, newly discovered vulnerabilities and any other relevant information included in this shared knowledge are fundamental for protecting the organizations' infrastructures and prevent future incidents. Eventually, coordinated incident response methods can produce more effective results, thanks to the diversity of available resources and skills within the sharing community.

9.3. *Incident information sharing architecture*

From an architectural standpoint, the European directive (European Commission, 2015) indicates the necessity for each Member State to create national CERTs that are responsible for handling incidents and risks, interconnected with each other through a common interoperable secure information sharing infrastructure.

The US strategy (White House, 2013a), instead, foresees two national critical infrastructure centers operated by the Department of Homeland Security (DHS) – one for physical infrastructures and another for cyber infrastructures. They are intended to work in a complementary way to serve as focal points for critical infrastructure stakeholders, in order to obtain situational awareness and integrated information to protect the physical and the cyber aspects of critical infrastructure.

Even though the aforementioned approaches both suggest a centralized architecture, a different option should also be taken into account when designing incident information sharing architectures: *peer-to-peer sharing models*. From previous information sharing-related research and studies (Golle et al., 2001; Parameswaran et al., 2001) emerge the strong need – from the perspective of the sharing organization – for a more reactive infrastructure layout capable of guaranteeing high responsiveness, availability, resilience and trustworthiness. Moreover, establishing a peer-to-peer sharing infrastructure would enable ad-hoc incident response. In emergency situations (such as the case described by Shin and Gu, 2010), affected peers would be able to request tailored and anonymous security support approaching the most trusted and qualified peers in the sharing network. Having a centralized entity in charge of collecting data from the sharing parties, analyzing it, generating information about incidents, threats and attacks, and distributing indicators back to the sharing nodes, could lead to a slow reacting architecture; moreover, the centrally collecting node would inevitably be a single point of failure.

Furthermore, private companies and organizations appear to be more willing to share sensitive information with trusted parties (Fernandez Vazquez et al., 2012; Skopik and Li, 2013), rather than with a centralized common entity. This is clearly inferred from the analysis on the cooperation between CERT teams. Although regional and international collaboration initiatives between CERTs exist and work effectively, more and more sector cooperation groups have recently been put in place (see Section 7). Teams tend to establish peer-to-peer collaboration infrastructures and exchange information with centers they can mutually trust (Abrams et al., 2003; Gibson and Cohen, 2003). This type of approach, on the other hand, leads to an increased value and sensitivity of the information shared, and therefore requires a more secure and reliable communication infrastructure.

9.4. *Data collection, information analysis and intelligence disclosure*

The analysis reported in this paper points out the necessity for cyber defense centers to consider different data collection points when deploying their architecture. Interfaces that enable the collection of open source intelligence information and unstructured data should be defined and employed. Situational awareness can be more readily achieved by correlating information gathered from "classic" data sources (e.g., CERTs providing reports and indicators of compromise) with OSINT information. Both the German and the Dutch cyber security centers examined in this paper already adopt this approach and analyze both confidential and open source information in order to always get an insight into current threats. Collecting large amounts of data requires, as already mentioned, more complex analysis methods and capabilities. For this reason, big data analytics techniques (Maltby, 2011) should be considered in facilitating the generation of situational awareness.

A crucial aspect to be considered, once data are collected and ready to be analyzed, is the sharing procedure. Automated sharing guarantees high data transfer rate, but implies unsupervised transmission of information. This might raise serious liability concerns and might also be limited by regulation in international cooperative frameworks. Moreover, purely automated sharing is not favorable in certain situations, as security information might be too complex, ambiguous or simply not fitting to any pre-existing model to be shared automated (see Dandurand and Serrano, 2013). In these cases, free text reports written and read/interpreted by humans should be used. Nevertheless, to perform a comprehensive incident analysis, where possible, a combination of automated and manual information sharing should be established (see Settanni et al., 2015).

One of the main objectives of security information sharing is to selectively warn targeted organizations about discovered bugs, vulnerabilities and threats. The process of disclosing such insights is critical and needs to be suitably designed. Reporting publicly a discovered vulnerability might expose organizations if no hot-fix or patch has been released yet. Information sharing requires trust among sharing partners and it will not be effective if performed in a completely public manner. Complete public disclosure of sensitive security information should therefore not be applied as the first step in the sharing procedure, but a *responsible disclosure* should be put in place (Shepherd, 2003). As regulated by the EU NIS Directive (European Commission, 2015), sensitive and critical information on bugs and vulnerabilities (as well as available exploits) can be disclosed to the public; however, the vendor needs to be contacted upfront to also provide a solution (bugfix, update, configuration change) together with the disclosure. Similarly, the Enhanced Cyber Security Program, extended by the US Executive Order (White House, 2013a), imposes the sharing of sensitive and classified government vetted cyber threat information with qualified commercial service providers (CSPs) and operational implementers (OIs). The Department of Homeland Security, therefore, does not share threat indicators with CI entities directly but rather with participating CSPs.

9.5. *Data format and exchange protocols*

The quality and the timeliness of the information and intelligence exchanged are of primary importance within the incident-sharing architecture between the expert centers, the organizations, the agencies as well as the critical infrastructure owners and operators. Currently, sharing communities use a combination of standard and proprietary mechanisms to exchange indicators; as described in this article, numerous data types are exchanged using different protocols depending on the scope of the sharing-system.

The European directive (European Commission, 2015) asks the Union NIS cooperation plan to provide a definition of the format and procedures for the collection and sharing of compatible and comparable information on risk and incidents by the competent authorities. To this regard, one of the PPD's goals is to enable efficient information exchange through the identification of baseline data and systems requirements, data formats, availability and accessibility, and ability to exchange various classifications of information.

Moreover, the US cyber security framework (NIST, 2014a) encourages the development of standard approaches in the data exchange mechanism to incorporate successful practices to enable sharing within and among sectors. When organizations share indicators, security automated technologies should be able to detect past attacks in operational data archives, identify compromised systems and support detection of future attacks.

9.6. *Future research and development*

A common point highlighted in all the analyzed regulations, strategies and international initiatives reported in the previous sections is the need for investment in innovation, research and development. According to the EU strategy (European Commission, 2013), R&D will support a strong industrial policy, promote a trustworthy ICT industry, boost the internal market and reduce European dependence on foreign technologies.

The US PPD (White House, 2013b) directs the competent authorities to develop a comprehensive research and development plan that shall provide input to align the Federal and Federally-funded R&D activities that seek to strengthen the security and resilience of US critical infrastructures.

An exemplary implementation of this requirement is the Tallinn Manual Process (NATO Cooperative Cyber Defence Centre of Excellence, 2013). It was launched in 2009, and is a leading effort in international cyber law research and education. In collaboration with distinguished international law scholars and practitioners, the center develops programs based on two pillars: i) a comprehensive research agenda and ii) practitioner-oriented training opportunities.

The aim of this survey article includes identifying the shortcomings and providing some general recommendations on cyber security information sharing. However, proposing solutions to address them in detail goes far beyond the scope of the paper.

10. Conclusion

In practice, security information sharing is usually accomplished via ad-hoc and informal relationships. Often, national CERTs assume the role of a contact point for coordinating and aggregating security incidence reports. However, the information that is provided is usually not targeted to particular vertical industry sectors. We suggest that sector-oriented views, along with rich information and experience reports, are required to make such platforms more effective. Furthermore, there is a crucial trade-off to be considered: existing platforms require information to be verified centrally (in order to avoid hoaxes); therefore, the speed of information distribution suffers. Timeliness of information is very important when protecting against aggressive attackers and zero-day exploits. Consequently, there is a need for new standards that employ suitable direct sharing models, which allow the targeted exchange of specific information about discovered vulnerabilities of ICT systems utilized in critical infrastructure control systems, as well as current threats (such as new SCADA (supervisory control and data acquisition)-targeted malware) and recent incidents. The application of these standards further implies the existence

of a federated trust and reputation model to address the reservations of users, and to attract a critical mass of users. This is also in-line with the objectives of the recently introduced European NIS directive and its US pendant. Both explicitly recommend the implementation of national cyber security centers, which are not only informed about the security status of the national critical infrastructure providers, but also play a coordinating role in the prevention of, or protection from attacks.

Acknowledgments

This study was partly funded by the Austrian FFG research program KIRAS in course of the projects CIIS (840842) and CISA (850199) as well as the European Union FP7 project ECOSSIAN (607577).

REFERENCES

Abrams LC, Cross R, Lesser E, Levin DZ. Nurturing interpersonal trust in knowledge-sharing networks. Acad Manage Exec 2003;17(4):64–77.

Agrawal R, Evfimievski A, Srikant R. Information sharing across private databases. In: Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data. ACM; 2003. p. 86–97.

Anonymous. Port scanning/0 using insecure embedded devices. <http://internetcensus2012.bitbucket.org/paper.html>; 2012 [accessed 04.16].

Arora A, Telang R, Xu H. Optimal policy for software vulnerability disclosure. Manage Sci 2008;54(4):642–56.

Arstechnica. Spamhaus ddos grows to internet-threatening size. <http://arstechnica.com/security/2013/03/spamhaus-ddos-grows-to-internet-threatening-size/>; 2013 [accessed 04.16].

BSA-The Software Alliance and Galexia. Asia-pacific cybersecurity dashboard – a path to a secure global cyberspace. <http://www.bsa.org/APACcybersecurity>; 2015 [accessed 04.16].

Clarke R. China cyberassault on America. Wall Street J 2011;15.

Dacey R. Homeland security: information sharing responsibilities, challenges, and key management issues. US General Accounting Office. <https://books.google.at/books?id=R2n-PQAACAAJ>; 2003 [accessed 04.16].

Dandurand L, Serrano O. Towards improved cyber security information sharing. In: Proceedings of 5th International Conference on Cyber Conflict. 2013. p. 1–16.

Danyliw R, Meijer J, Demchenko Y. Rfc 5070: the incident object description exchange format (IODEF). <http://www.ietf.org/rfc/rfc5070.txt>; 2007 [accessed 04.16].

D'Amico A, Whitley K, Tesone D, O'Brien B, Roth E. Achieving cyber defense situational awareness: a cognitive task analysis of information assurance analysts. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 49. SAGE Publications; 2005. p. 229–33.

Denise Z, James L. Cyber threat information sharing. 2015.

Department of Homeland Security. Enhanced cybersecurity services program. <http://www.dhs.gov/sites/default/files/publications/ecs_final_factsheet_08182014.pdf>; 2013 [accessed 04.16].

ENISA. CSIRT legal handbook. <https://www.enisa.europa.eu>; 2003 [accessed 04.16].

ENISA. CERT cooperation and its further facilitation by relevant stakeholders. <https://www.enisa.europa.eu>; 2006 [accessed 04.16].

ENISA. Incentives and challenges to information sharing. <https://www.enisa.europa.eu/news/enisa-news/incentives-challenges-for-cyber-security-information-sharing-in-europe-identified>; 2010 [accessed 04.16].

ENISA. Practical guide/roadmap for a suitable channel for secure communication: secure communication with the CERTs & other stakeholders. 2011a.

ENISA. Proactive detection of network security incidents. <https://www.enisa.europa.eu/activities/cert/support/proactive-detection/survey-analysis>; 2011b [accessed 04.16].

ENISA. Detect, share, protect – solutions for improving threat data exchange among CERTs. <https://www.enisa.europa.eu/activities/cert/support/data-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs/at_download/fullReport>; 2013a [accessed 04.16].

ENISA. Enisa threat landscape mid year 2013. 2013b.

ENISA. Flash note: can recent attacks really threaten internet availability? 2013c.

ENISA, Cyber security information sharing: an overview of regulatory and non-regulatory approaches. <https://www.enisa.europa.eu/publications/cybersecurity-information-sharing>; 2015 [accessed 04.16].

European Commission. Cybersecurity strategy of the European Union: an open, safe and secure cyberspace. <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf>; 2013 [accessed 04.16].

European Commission. Proposal for a directive of the european parliament and of the council concerning measures for a high common level of security of network and information systems across the union. <http://www.consilium.europa.eu/en/press/press-releases/2015/12/pdf/st15229-re02_en15_pdf>; 2015 [accessed 04.16].

Farwell JP, Rohozinski R. Stuxnet and the future of cyber war. Survival (Lond) 2011;53(1):23–40.

Fernandez Vazquez D, Pastor Acosta O, Brown S, Reid E, Spirito C. Conceptual framework for cyber defense information sharing within trust relationships. In: 2012 4th International Conference on Cyber Conflict (CYCON). IEEE; 2012. p. 1–17.

FireEye. Advanced targeted attacks. How to protect against the next generation of cyber attacks. White Paper. <http://www.exebridge.com/landing%20pages/FireEye/docs/Exebridge-Advanced-Targeted-Attacks-White-Paper.pdf>; 2013 [accessed 04.16].

Gal-Or E, Ghose A. The economic incentives for sharing security information. Inform Syst Res 2005;16(2):186–208.

Gibson CB, Cohen SG. Virtual teams that work: creating conditions for virtual team effectiveness. John Wiley & Sons; 2003.

Golle P, Leyton-Brown K, Mironov I, Lillibridge M. Incentives for sharing in peer-to-peer networks. In: Electronic commerce. Springer; 2001. p. 75–87.

Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: an economic analysis. J Account Public Policy 2003;22(6):461–85.

Harrison K, White G. Information sharing requirements and framework needed for community cyber incident detection and response. In: 2012 IEEE Conference on Technologies for Homeland Security (HST). IEEE; 2012. p. 463–9.

Hausken K. Information sharing among firms and cyber attacks. J Account Public Policy 2007;26(6):639–88.

Helmbrecht U, Purser S, Cooper G, Ikonomou D, Marinos L, Ouzounis E, et al. ENISA: cybersecurity cooperation: defending the digital frontline. 2013.

Hernandez-Ardieta JL, Tapiador JE, Suarez-Tangil G. Information sharing models for cooperative cyber defence. In: 2013 5th International Conference on Cyber Conflict (CyCon). IEEE; 2013. p. 1–28.
Herzog S. Revisiting the Estonian cyber attacks: digital threats and multinational responses. J Strateg Secur 2011;4(2):4.
Howard JD, Longstaff TA. A common language for computer security incidents. Sandia National Laboratories; 1998.
Hudson A. Top German spy says Berlin under cyber attack from other states. Reuters 2014;11.
ISO. Iso/iec27010: information technology – security techniques – information security management for inter-sector and inter-organizational communications. 2012. 2012-03-20.
ITU-T. Recommendation ITU-T x.1500 cybersecurity information exchange techniques. 2012.
Jajodia S, Liu P, Swarup V, Wang C. Cyber situational awareness: issues and research, vol. 14. Springer; 2010.
Kácha P. Idea: security event taxonomy mapping. In: 18th International Conference on Circuits, Systems, Communications and Computers. 2014.
Kaufmann H, Hutter R, Skopik F, Mantere M. A structural design for a Pan-European early warning system for critical infrastructures. In: Elektrotechnik und informationstechnik. Springer; 2014.
Langner R. Stuxnet: dissecting a cyberwarfare weapon. Secur Privacy 2011;9(3):49–51. IEEE.
Maltby D. Big data analytics. In: Communication and information in society, technology and work, vol. 48. ASIST; 2011. Proceedings of the 74th ASIS&T Annual Meeting.
Micro T, Organization of American States. Report on cybersecurity and critical infrastructure in the americas. 2015.
Miller C. The legitimate vulnerability market: the secretive world of 0-day exploit sales. In: Proceedings of the Workshop on the Economics of Information Security (WEIS). 2007. p. 1–10.
Moriarty K. Rfc 6545: real-time inter-network defense (RID). <http://www.ietf.org/rfc/rfc6545.txt>; 2012 [accessed 04.16].
NATO Cooperative Cyber Defence Centre of Excellence. International cyber incidents – legal consideration. 2010.
NATO Cooperative Cyber Defence Centre of Excellence. Strategic cyber security. 2011.
NATO Cooperative Cyber Defence Centre of Excellence. National cyber security – framework manual. 2012.
NATO Cooperative Cyber Defence Centre of Excellence. Tallin manual on the international law applicable to cyber warfare. 2013.
NIST. Framework for improving critical infrastructure cybersecurity, 2014a. 2014-02-12.
NIST. Guide to cyber threat information sharing. NIST special publication 800-150 (Draft). 2014b. 2014-October.
Olson P. We are anonymous: inside the hacker world of LulzSec, anonymous, and the global cyber insurgency. Little, Brown 2012;528. Back Bay Books, ISBN-10: 0316213527; ISBN-13: 978-0316213523, <https://books.google.at/books?id=ncGVPtoZPHcC> [accessed 04.16].
Parameswaran M, Susarla A, Whinston AB. P2p networking: an information-sharing alternative. Computer 2001;34(7):31–8.
Phillips CE Jr, Ting T, Demurjian SA. Information sharing and security in dynamic coalitions. In: Proceedings of the seventh ACM symposium on access control models and technologies. ACM; 2002. p. 87–96.
Rinaldi SM. Modeling and simulating critical infrastructures and their interdependencies. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences. IEEE; 2004. p. 8.
Sarter NB, Woods DD. Situation awareness: a critical but ill-defined phenomenon. Int J Aviat Psychol 1991;1(1):45–57.
Settanni G, Skopik F, Fiedler R, Shovgenya Y. A blueprint for a pan-european cyber incident analysis system. In: Proceedings of 3rd International Symposium for ICS and SCADA Cyber Security Research. 2015. p. 84–8.
Shepherd S. Vulnerability disclosure: how do we define responsible disclosure? GIAC SEC practical repository. SANS Inst 2003;9.
Shin S, Gu G. Conficker and beyond: a large-scale empirical study. In: Proceedings of the 26th Annual Computer Security Applications Conference. ACM; 2010. p. 151–60.
Skopik F, Li Q. Trustworthy incident information sharing in social cyber defense alliances. In: 2013 IEEE Symposium on Computers and Communications. ISCC; 2013. p. 233–9.
Skopik F, Schall D, Dustdar S. Modeling and mining of dynamic trust in complex service-oriented systems. Inform Syst 2010;35(7):735–57.
State of California Department of Justice Office of the Attorney General. Sony pictures entertainment notice letter. 2014.
Tadda G, Salerno JJ, Boulware D, Hinman M, Gorton S. Realizing situation awareness within a cyber environment. In: Defense and security symposium. International Society for Optics and Photonics. 2006. p. 624204.
Tankard C. Advanced persistent threats and how to monitor and deter them. Netw Secur 2011;(8):16–19.
The Senate of The United States. Cybersecurity Information Sharing Act. <https://www.congress.gov/bill/113th-congress/senate-bill/2588/text>; 2014.
US Homeland Security Cyber Security R&D Center. A roadmap for cybersecurity research. 2009.
Virvilis N, Gritzalis D. The big four-what we did wrong in advanced persistent threat detection? In: 2013 Eighth International Conference on Availability, Reliability and Security (ARES). IEEE; 2013. p. 248–54.
Waksman A, Sethumadhavan S. Silencing hardware backdoors. In: 2011 IEEE Symposium on Security and Privacy (SP). 2011. p. 49–63.
White House. Executive order (EO13636): improving critical infrastructure cybersecurity. <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>; 2013a [accessed 04.16].
White House. Presidential policy directive – critical infrastructure security and resilience. <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>; 2013b [accessed 04.16].
Zhao W, White G. A collaborative information sharing framework for community cyber security. In: 2012 IEEE Conference on Technologies for Homeland Security (HST). IEEE; 2012. p. 457–62.

Florian Skopik Senior Scientist of the research program "IT Security". Current research interests include the security of critical infrastructures, especially in course of national cyber defense. Before joining AIT, Florian was with the Distributed Systems Group at the Vienna University of Technology as a research assistant and post-doctoral research scientist where he finished his PhD studies. Florian further spent a sabbatical at IBM Research India in Bangalore for several months. He published around 80 scientific conference papers and journal articles, and is a member of various conference program committees and editorial boards. Florian is IEEE Senior Member.

Giuseppe Settanni joined AIT in 2013 as scientist and is currently working on national and European applied research projects regarding security in communication and information systems. Before joining AIT, Giuseppe Settanni worked for 2 years at FTW (Telecommunication Research Center in Vienna), as a communication

network researcher, on the development of a network-based anomaly detection tool in the context of DEMONS European Project. His current research interests include security of critical infrastructures, information sharing and anomaly detection in national cyber defense.

Roman Fiedler is Scientist at the AIT Austrian Insititute of Technology and runs projects in the areas of telehealth and ICT security. Roman has got a decade of experience in network security and operations. He finished his Master studies in the domain of biochemistry at the University of Technology Graz.