Deliverable 1.1

Report on Existing EU practices for cyber security

Tempus

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

Deliverable 1.1

Report on Existing EU practices for cyber security

European Commission Tempus Project:

544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES

This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of content

1. Introduction and preliminaries

The internet, together with the information communications technology (ICT) that underpins it, is a critical national resource for governments, a vital part of national infrastructures, and a key driver of socio-economic growth and development. Over the last forty years, and especially since the year 2000, governments and businesses have embraced the internet, and ICT's potential to generate income and employment, provide access to business and information, enable e-learning, and facilitate government activities. In some countries the internet contributes up to 8% of gross domestic product (GDP), and member countries of both the European Union (EU) and the G20 have established goals to increase the internet's contribution to GDP. This cyber environment's value and potential is nurtured by private and public sector investments in high-speed broadband networks and affordable mobile internet access, and break-through innovations in computing power, smart power grids, cloud computing, industrial automation networks, intelligent transport systems, electronic banking, and mobile e-commerce.

These document surveys and analyses current practices for cyber security at both, national and institutional levels. The analysis provides the necessary basis for understanding existing educational cyber security frameworks (which should be done in DEV 1.2) and further introducing a cyber-security framework and guidelines for establishing, assessing, accrediting, and running cyber security study programs at different levels, from informal education, higher education to life-long education; conducting cyber security projects, and providing firm and stable infrastructure for cyber security.

The analysis focuses primarily on cyber security practices in Europe, but also provides insight in such practices elsewhere in the world. It explores:

- the principles for cyber security presented in initiatives and projects of important European-level associations;
- developing strategies processes of assessment, experiences and good practices adopted by relevant national-level bodies and institutions.

1.1 Context

Information and communications technologies (ICT) have become indispensable to the modern lifestyle. We depend on information and communications infrastructure in governing our societies, conducting business, and exercising our rights and freedoms as citizens. In the same way, nations have become dependent on their information and communications infrastructure and threats against its availability, integrity and confidentiality can affect the very functioning of our societies.

The security of a nation's online environment is dependent on a number of stakeholders with differing needs and roles. From the user of public communications services to the Internet Service Provider supplying the infrastructure and handling everyday functioning of services, to the entities ensuring a nation's internal and external security interests – every user of an information system affects the level of resistance of the national information infrastructure to

cyber threats. Successful national cyber security strategies must take into consideration all the concerned stakeholders, the need for their awareness of their responsibilities and the need to provide them with the necessary means to carry out their tasks. Also, national cyber security cannot be viewed as merely a sectorial responsibility: it requires a coordinated effort of all stakeholders. Therefore, collaboration is a common thread that runs through most of the currently available national strategies and policies.

Moreover, the different national cyber security strategies represent another common understanding: while national policies are bound by the borders of national sovereignty, they address an environment based on both infrastructure and functioning logic that has no regard for national boundaries. Cyber security is an international challenge, which requires international cooperation in order to successfully attain an acceptable level of security on a global level.

National interests tend to have priority over common interests and this is an approach which may be difficult to change, if it needs changing at all. As long as we can find the common ground and discuss the problematic issues out in the open, national interests should not impede international cooperation.

The task of drafting a national cyber security strategy is a complex one. In addition to the versatile threat landscape and the various players involved, the measures to address cyber threats come from a number of different areas. They can be political, technological, legal, economic, managerial or military in nature, or can involve other disciplines appropriate for the particular risks. All of these competences need to come together to offer responses capable of strengthening security and resisting threats in unison, rather than in competition for a more prominent role or for resources. Also, any security measures foreseen must consistently be balanced against basic rights and freedoms and their effects on the economic environment must be considered. In the end, it is important to understand that cyber security is not an isolated objective, but rather a system of safeguards and responsibilities to ensure the functioning of open and modern societies.

1.1.1 Related concepts

Security, in general, is the protection of people and assets against threats and danger. Security in the scope of information technologies, in particular, can be defined as the protection of information technology tools and infrastructures against damage and loss. The Institute for Security and Open Methodologies[1] (ISECOM) defines security as »a form of protection where a separation is created between the assets and the threat«. The assets in general, are buildings, computers systems and devices, fiscal assets, information and data. On the other hand, the sources of damage and loss range from natural disasters such as earthquakes and storms to technological breakdowns such as equipment failures and information compromise.

The general concept security can be categorized into different branches of security as:

- Physical;
- Computer;
- Communications;
- Information;
- Human;
- National.

[1] http://www.isecom.org/

National security is protection or the safety of a country and its citizens. It requires the use economic, diplomatic and political power. National security covers economic security, public security, energy security, environmental security, etc. To ensure national security some measures must be taken:

- Sustaining competent armed forces;
- Rallying allies and isolating threats via diplomatic relations;
- Organizing economic resources in a way that promotes cooperation;
- Advancing emergency alertness and civil defence applications;
- Guaranteeing the redundancy and flexibility of important infrastructures;
- Utilizing intelligence and counterintelligence services to reveal and overthrow any internal or external throw or compromise of information.

1.1.2 Cyberspace

The term cyberspace can be best grasp as a metaphor that refers to the virtual world of information systems. Term »space« in cyberspace is best to be considered as more akin to an abstract mathematical sense of the term, rather than physical terrain. Cyberspace does not have a standard definition. Generally, the term is used to describe non-physical space that is composed of computer systems and information systems which can be accessed by computer networks. In contemporary terminology, the term »cyberspace« refers to world-wide network of computer systems, IT structures and communication networks.

Cyberspace is a medium that consists of many participants with the ability to affect and influence each other and is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modifies, and exchange data via networked systems and associated physical infrastructures.

Cyberspace is more than internet, includes not only hardware, software and information systems, but also people and social interaction within these networks. The ITU uses the term to describe the 'systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks. The International Organization for Standardization (ISO) uses a slightly different term, defining cyber as 'the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form. Separately, governments are defining what they mean by cyberspace in their national cyber security strategies (NCSS)

The global networks, along with its advantages, have also exposed us to security risks like cybercrimes. Cybercrime in general, can be defined as offences or illegal activities committed on the modern telecommunication networks such as Internet. Cybercrime covers such a broad scope of criminal activity but can be basically divided into three major categories:

- Cybercrimes committed against person: Any personal abuse by using computers; exchange broadcast or distribute inappropriate content.
- Cybercrimes against all forms of property: Distribution of malicious software, giving harm to the properties of individuals
- Cybercrime against Government: These action are considered as cyber terrorism if they are undertaken by cracking a governmental or military computer system

The Council of Europe (CoE) also adopted a Convention on Cybercrime in July 2004, the first international convention to address this issue. It contains a relatively high standard of international cooperation for investigating and prosecuting cybercrime. CoE is aware that criminals exploit the seams of cross-jurisdictional cooperation and coordination among nations. Other organisations have taken similar approaches, within their own frameworks. In July 2006, the ASEAN Regional Forum (ARF) issued a statement that its members should implement cyber-crime and cyber security laws 'in accordance with their national conditions and should collaborate in addressing criminal and terrorist misuse of the Internet. These commitments were later codified in the 2009 agreement within the Shanghai Cooperation Organization (ASEAN-China Framework Agreement) on information security.

Figure 1 shows relationship between Cyber Security and other Security Domains and has been adopted from ISO/IEC 27032:2012, '*Information technology – Security techniques – Guidelines for cyber security*'.

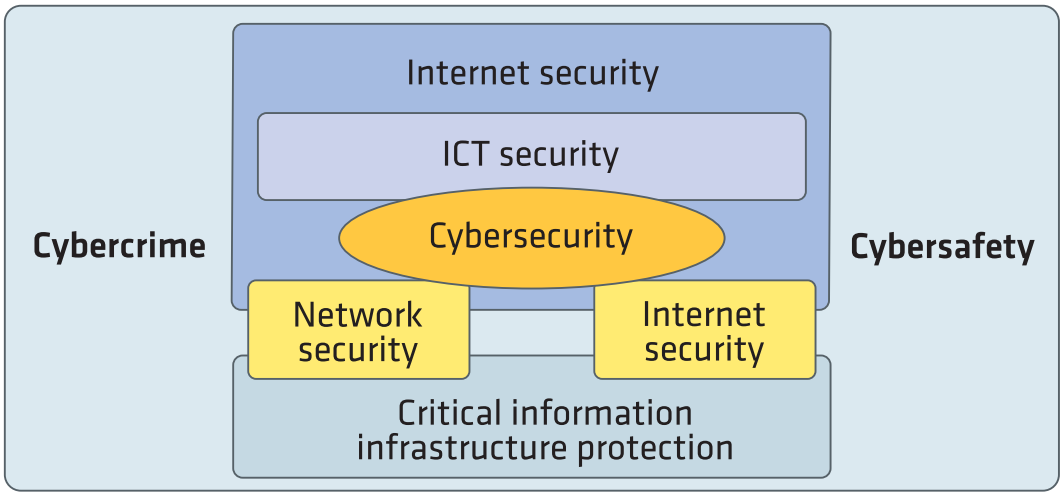

Figure 1: Relationship between cyber security and other security domains

Information Security 'is concerned with the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user' (ibid.).

Network Security 'is concerned with the design, implementation, and operation of networks for achieving the purposes of information security on networks within organizations, between organizations, and between organizations and users' (ibid.).

Internet Security 'is concerned with protecting internet-related services and related ICT systems and networks as an extension of network security in organizations and at home, to achieve the purpose of security. Internet Security also ensures the availability and reliability of Internet services' (ibid., 11.).

Critical information infrastructure protection (CIIP) 'is concerned with protecting the systems that are provided or operated by critical infrastructure providers, such as energy, telecommunication, and water departments. CIIP ensures that those systems and networks are protected and resilient against information security risks, network security risks, internet security risks, as well as Cyber security risks' (ibid.).

Cybercrime has been defined as the 'criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime' (ibid., 4.).

Cyber safety has been defined as the 'condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable' (ibid.).

Cyber security, or ***Cyberspace Security*** has been defined as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace' (ibid.). However, it has also been noted that in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved in cyber security. The term 'cyber security' was widely adopted during the year 2000 with the 'clean-up' of the millennium software bug. When the term 'cyber security' is used, it usually extends beyond information security and ICT security.

ISO defined cyber security as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace'.

The ITU also defined cyber security broadly as:

> '*The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality*'.

Many countries are defining what they mean by cyber security in their respective national strategy documents. More than 50 nations have published some form of a cyber-strategy defining what security means to their future national and economic security initiatives.

1.2 Cybersecurity dimensions

Any approach to a National Cyber Security strategy needs to consider the following dimensions of activity:

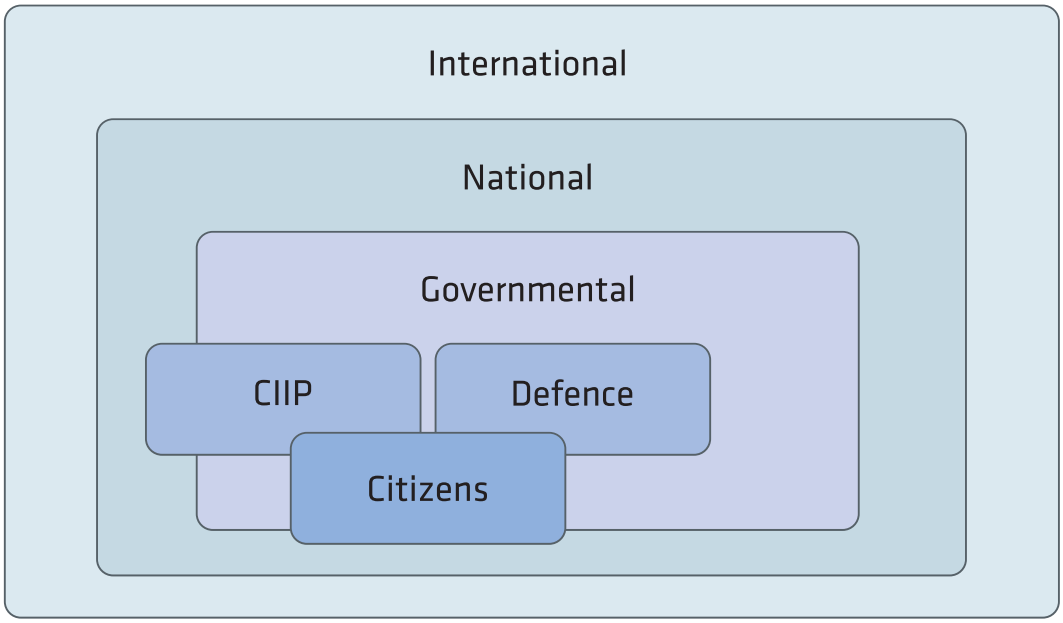

Figure 2: Relationship between cyber security and other security domains

Governmental

Within government alone, it is not unusual for up to a dozen different departments and agencies to claim responsibility for national cyber security in various forms, including military, law enforcement, judicial, commerce, infrastructure, interior, intelligence, telecommunications, and other governmental bodies. This is understandable due to breadth and depth of what constitutes NCS but leads to considerable difficulty in establishing coherent action. A major challenge for all NCS strategies is, therefore, improving the coordination between these governmental actors. This Whole of Government effort can be achieved by a number of different methods, ranging from appointing a lead agency or department to simply improving the inter-departmental process. Due to the esoteric nature of cyber security, however, it probably requires much more effort to achieve this Whole of Government synergy than practically any other security challenge.

International

Virtually no NCS document ignores the international dimension. The very basis of the internet, to say nothing of the myriad companies and organisations that effectively constitute the internet, is thoroughly globalised. For any nation state or interest group, to advance its interests requires collaboration with a wide range of international partners. This applies at any level: from internationally binding treaties (e.g., the Council of Europe Cybercrime Convention), to politically binding agreements (e.g., regarding Confidence Building Measures in Cyberspace), to non-governmental agreements between technical certification bodies (e.g., membership of FIRST and similar bodies). Many of the international collaborations will occur outside a specific national government. In fact, it can be necessary to work with non-state actors abroad. Therefore, the emphasis must be on relationships with all the relevant actors within specific systems (in particular, but not limited to the field of 'internet governance'). This Whole of System approach, therefore, emphasises the need for a government to agree on a single lead actor (which can be also outside of government itself), and to enable that actor to be flexible enough to engage with the entire range of actors globally.

National

Engagement with security contractors and critical infrastructure companies has always been seen as critical for national security. The steady expansion of the number of actors relevant to national cyber security within any particular nation has meant that some governments have decided to make their overall strategy 'comprehensive', including the entire society, or the Whole of Nation. A Whole of Nation approach tries to overcome the limitations of simply having special legally-defined relationships with a small number of specific security contractors. Often it tries to encourage a wide range of non-state actors (in particular private companies but also research establishments and civil society) to cooperate with the government on cyber security issues. While many governments are increasingly expanding their legal options, the general principle is that specific 'cooperation' is needed from such a great number of non-state actors that a pure legislative approach would be largely unworkable in most democracies. To encourage cooperation, Whole of Nation approaches usually include various incentives that directly support the security of these enterprises, and indirectly can be of other advantage as well (e.g., commercially).

Within the general context of discussing national cyber security, it is important to keep in mind that this is not one single subject area. Rather, it is possible to split the issue of NCS into five distinct perspectives or 'mandates', each of which could be addressed by different government departments. This split is not an ideal state but it is a reality due to the complexity and depth of cyber security as a whole. Each mandate has developed its own emphasis and even its own lexicon, despite the fact that they are all simply different facets of the same problem. Unfortunately, there is frequently a significant lack of coordination between these mandates, and this lack of coordination is perhaps one of the most serious organisational challenges within the domain of national cyber security.

Military Cyber

Many governments are building capabilities to wage cyber war, while some NATO reports have claimed that up to 120 countries are developing a military cyber capability. These capabilities can be interpreted as simply one more tool of warfare, similar to airpower, which would be used only within a clearly defined tactical military mission (for instance, for shutting down an air-defence system). Military cyber activities, therefore, encompass four different tasks: enabling protection of their own defence networks, enabling Network Centric Warfare (NCW) capabilities, battlefield or tactical cyber warfare, and strategic cyber warfare.

Counter Cyber Crime

Cyber-crime activities can include a wide swath of activities that impact both the individual citizen directly (e.g., identity theft) and corporations (e.g., theft of intellectual property). At least as significant for national security, however, is the logistical support capability cyber-crime can offer to anyone interested in conducting cyber-attacks. This is also where cyber-crime interacts not only with military cyber activities, but also with cyber terrorism. There have been a rising number of criminal acts, including attempts at mass disruption of communications, and this suggests cyber terrorism will be an issue for the future.

Intelligence and Counter-Intelligence

Distinguishing cyber espionage from cyber-crime and military cyber activities is controversial. In fact, both missions depend on similar vectors of attack and similar technology. In practice, however, serious espionage cases (regarding intellectual property as well as government secrets) are in a class of their own, while at the same time it can be very difficult to ascertain for sure if the perpetrator is a state or a criminal group operating on behalf of a state or indeed operating on its own. Whoever is actually behind the attack, cyber

espionage probably represents the most damaging part of cyber-crime (if included in the category).

Critical Infrastructure Protection and National Crisis Management

Critical infrastructure protection (CIP) has become the catch-all term that seeks to involve the providers of essential services of a country within a national security framework. As most of the service providers (such as public utilities, finance or telecommunications) are in the private sector, it is necessary to extend some sort of government support to help protect them and the essential services they provide from modern threats. While the original focus of these programmes post-September 11, 2001 was often on physical security, today the majority of all CIP activity is directly connected to cyber acts, usually cyber-crime and cyber espionage. In this context, National Crisis Management must be extended by an additional cyber component.

'Cyber Diplomacy' and Internet Governance

If diplomacy at its core is about how states exchange, deal with, gather, assess, present and represent information, cyber diplomacy is about 'how diplomacy is adapting to the new global information order.' Within this context, the promotion of aims such as 'norms and standards for cyber behaviour' (discussed primarily within the UN) and the aim for promoting 'confidence building measures between nations in cyberspace' needs to be understood as a mostly bilaterally-focused activity. Internet governance, in contrast, is largely a multilateral (or even multi-stakeholder) activity, and is probably the most international of all mandates. Internet governance is generally referred to as the process by which a number of state and non-state actors interact to manage what, in effect, is the programming (or code, or 'logical') layer of the internet.

The above segmentation is an attempt to provide for a more structured discussion on the scope of national cyber security. The reality of these different mandates is that they are each dealt with by different organisational groups not only within government, but also within the non-state sector. Normatively speaking, all of these mandates should be holistically engaged if a comprehensive NCS perspective is to be developed.

2. Relevant Organizations and Institutions

Throughout the early years of Internet development, security was not established or maintained via a formal or planned institutional framework. Instead, the critical roles of threat detection and mitigation were largely left to the private sector. Companies were expected to handle security for their own products, and users accepted some inherent risk or liability. However, this approach was never suited to handle significant growth in vulnerabilities. Individual corporations lacked incentives to share information, and more importantly, lacked the legal authority to deal with emerging national threats or to prosecute criminal networks. As a result, response to cyber incidents remained closeted and uncoordinated, with private entities adopting a largely reactive approach.

Observing this situation, several non-profit organizations attempted to fill the organizational gap by providing volunteer response teams, information sharing networks, and security guidelines. By focusing on issues that spanned the corporate barrier, these non-profit organizations established a foundation for coordinated community response to emerging cyber threats. However, although they were often successful at mitigating localized security issues, non-profit organizations lacked the requisite authority and resources to effectively respond to crises of global or national scope.

Over the better part of a decade, the convergence of four distinct but interconnected trends created demands for formal interventions involving governments and international coordination. First, internet usage continued to rise, coupled with an expansion in forms of use. Second, many governments recognized that cyber vulnerabilities continued to threaten not only the security of their own networks but also those of their citizens involved in routine activities on a daily basis. Third, there was a noted absence of coordinated industry responses or of efforts to develop cooperative threat reduction strategies, thereby reinforcing an unambiguous gap-in-governance. Finally, a growing set of cyber incidents, large and small, signaled to governments the potential impact of their failure to address the emerging threat. In response, governments, in various ways, national and international resources towards the creation of a broad cyber security framework; the resulting institutional responses serve as the focus of this paper.

Table 1 identifies the organizations and entities referred to cyber security. A cursory look at this table indicates that the cyber security system is a complex assortment of national, international, and private organizations. Parallel to the organic fashion in which cyberspace itself developed, these organizations often have unclear mandates or possess overlapping spheres of influence. At this stage we seek only to highlight the major entities and, to the extent possible, to signal their relationships and interconnections.

We used two criteria to select organizations for analysis. First, we focused on entities that provide public information relevant to cyber security issues. Second, within each of our three areas of focus (International, Intergovernmental, and National) we selected institutions with coordinating responsibility or formal mandates issued by recognized international or national bodies. For the national level, we shortly present cyber security organization in the United States as a representative model. Detailed analysis of other national efforts is shown in the next chapter of this report.

Table 1: International Institutional Cyber Security System

Institution	Role
CERTs	
AP-CERT: Asia Pacific Computer Emergency Response Team	Asian regional coordination
CERT-CC: Computer Emergency Response Team - Coordination Centre	Coordination of global CERTs, especially national CERTs.
FIRST: Forum for Incident Response and Security Teams	Forum and information sharing for CERTs
TF-CSIRT: Collaboration of Security Incident Response Teams	European regional coordination
International Entities	
CCDCOE: Cooperative Cyber Defence Centre of Excellence	Enhancing NATO's cyber defence capability
European Union	Sponsors working parties, action plans, guidelines
ENISA: European Network and Information Security Agency	Awareness raising, cooperation between the public and private sectors, advising the EU on cyber security issues, data collection
G8: Subgroup on High Tech Crime	Sponsored 24/7 INTERPOL hotline, various policy guidelines
IMPACT: International Multilateral Partnership Against Cyber Threats	Global threat response centre, data analysis, real-time early warning system
INTERPOL: International Criminal Police Organization	Manages 24/7 hotline, trains law enforcement agencies, participates in investigations.
ITU: International Telecommunications Union	Sponsors IMPACT. Organizes conferences, releases guidelines and toolkits, facilitates information exchange and cooperation.
NATO: North Atlantic Treaty Organization	Responding to military attacks on NATO member states
OECD: Organisation for Economic Co-operation and Development	Develops policy options, organizes conferences, publishes guidelines and best-practices.
UNODC: United Nations Office on Drugs & Crime	Promotion of legislation, training programs, awareness, enforcement

Institution	Role
WSIS: World Summit on the Information Society	Global summit on information security; publishes resolutions and monitors implementation through stocktaking efforts.
National Entities	
NSA/CSS: The National Security Agency/Central Security Service	NSA/CSS leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.
CIA: Central Intelligence Agency	Defence of intelligence networks, information gathering
DHS: Department of Homeland Security	Protection of federal civil networks & critical infrastructure; information sharing and awareness; coordinating federal response and alerts.
DoD: Department of Defence	Defence of military networks, counterattack capability
DOJ: US Department of Justice	Federal Prosecution
FBI: Federal Bureau of Investigation	Federal Investigation
US-CERT: United States Computer Emergency Response Team	Defence of federal civil networks (.gov), information sharing and collaboration with private sector.
National CERTs	National coordination; national defence & response

2.1 International Institutional Response

First, we consider two sets of institutions that are international but not intergovernmental in scope. We begin with a brief overview of *Computer Emergency Response Teams* (CERTS), and then examine a subset of collaborative organizations that coordinate CERT policy.

As defined by the CERT Coordination Centre (CERT/CC), these teams organize responses to security emergencies, promote the use of valid security technology, and ensure network continuity. In principle, this means that CERTs focus on identifying vulnerabilities and fostering communication between security vendors, users, and private organizations. Although the majority of CERTs were founded as non-profit organizations, many have transitioned towards public-private partnerships in recent years. This increasing level of integration with national governments represents an attempt to build upon the successes of

non-profit CERTs by providing a level of structure and resources hitherto unavailable. At present, there are over 200 recognized CERTs, with widely different levels of organization, funding, and expertise.

At least three products are expected to result from CERT activities and interactions:

1. a reduction in unaddressed security vulnerabilities;
2. improved understanding of the nature and frequency of cyber threats;
3. improved methods of communicating and reporting these threats to other security teams and the general public.

Figure 3 shows a subset of these structured relationships at different levels of analysis of organization [1].

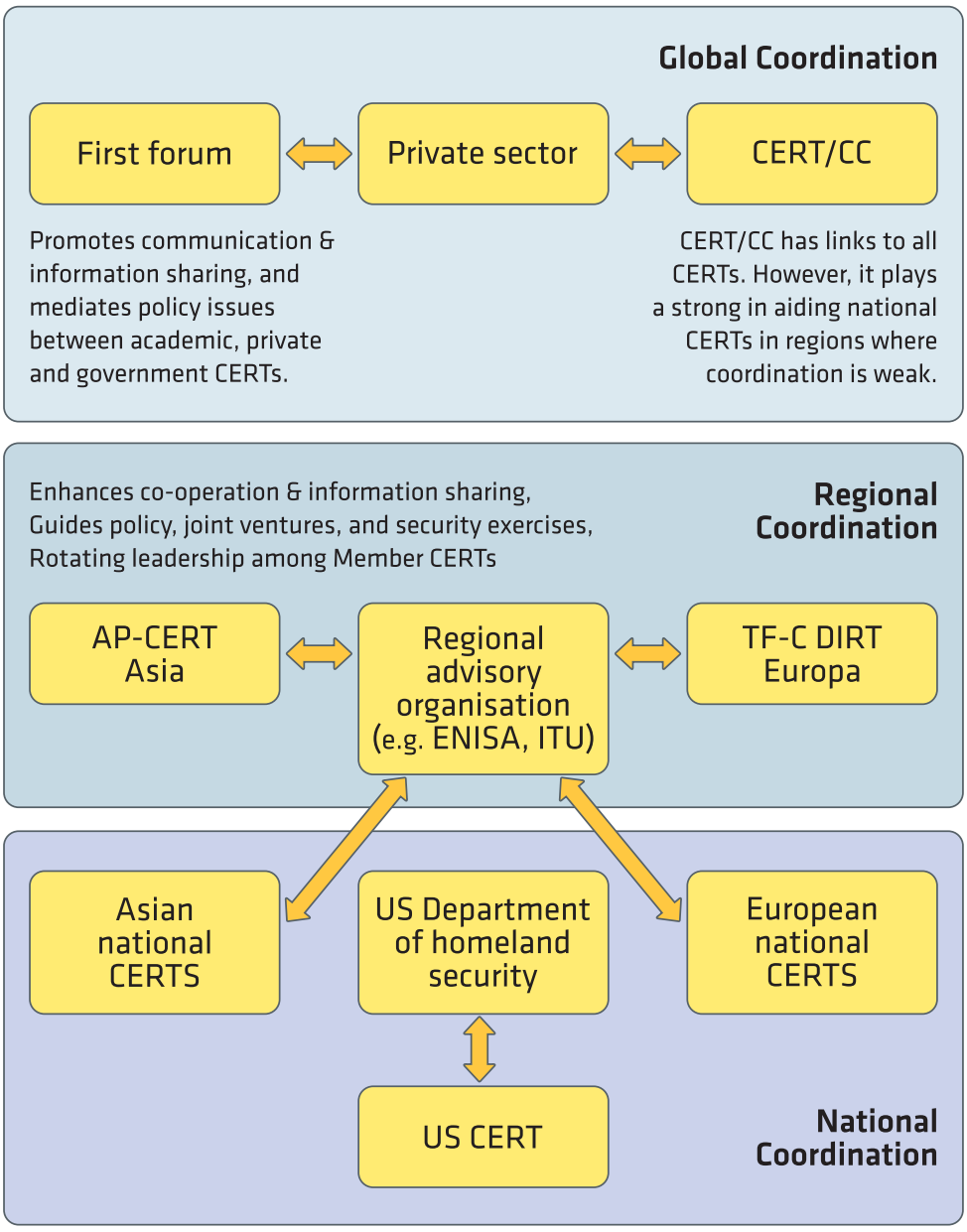

Figure 3: International CERTs

In general, CERTs share a common structure and backbone. The majority of CERT teams are defined according to guidelines originally published by CERT/CC, and many use common toolkits to establish their organizations [2]. As a result, CERTs tend to differ from each other mainly in their area of focus (academic, private, national, regional), or their respective area of expertise (phishing, viruses, information security). These roles are largely self-defined according to each team's level of funding (which can vary widely), technical expertise, and the presence of perceived gaps within the CERT collaborative network. One expected advantage of this underlying flexibility is that it greatly improves the possibility of coordination between CERTs.

However, as cyberspace expanded, a single organization proved insufficient to handle the increasing volume of security incidents, and CERT/CC was forced to reframe its activities and priorities. Rather than responding directly to emerging incidents, CERT/CC chose to utilize the lessons it had learned to provide guidelines, coordination, and standards for other CERTs. By relinquishing operational control in favour of a collaborative structure, CERT/CC laid the foundation for the establishment of regional, focused organizations. Today, the CERT network has expanded beyond the scope and control of CERT/CC, although the organization continues to play an influential role in establishing national CERTs in developing countries and fostering CERT communication.

In addition to CERT/CC, many CERTS also interact with parallel coordination networks, such as the *Forum of Incident Response and Security Teams* (FIRST). This body was established to enhance information sharing between disparate security groups. Now composed of more than 200 organizations, FIRST is notable for its influential annual conferences and its extensive integration of national, academic, and private CERT teams.

The collaborative structure maintained by coordinating agencies such as FIRST and CERT/CC clearly aids in enhancing information flow between security teams. However, if CERTs were only organized in this fashion, it would be unclear which organizations possessed regional authority to coordinate the actions of other CERTs; for instance, in the event of a national attack on civilian networks. This problem was addressed by transitioning the CERT structure to a national level. One valuable side effect of this shift to national-level jurisdiction was the creation of public/private partnerships between national CERTs and national agencies.

However, a solution to one problem can often give rise to additional complications. Given the diversity of national political systems and bureaucratic practices, the transition to national CERTs exacerbated the realities of legal and jurisdictional diversity. National CERTs occupy a first-line responder role in the event of attacks on national civilian networks, but lack the jurisdictional authority to shut down criminal networks and prosecute perpetrators. As a result, national CERTs focus primarily on responding to and preventing *technical* cyber threats. In order to effectively deal with legal issues, clear lines of communication between national CERTs and government agencies are essential. Although this link has been formalized in some countries such as the United States, other nations are still developing the requisite connections between national CERTs and legal authority.

2.2 Inter-Governmental Organizations

Although CERTs occupy an important role in the international cyber security system, their core competencies or self-defined responsibilities do not extend to consensus building, legislation, or awareness-raising. While this set of functions remained largely unclaimed in the nascent years of internet development, they have recently been embraced by a variety of

inter-governmental organizations. Unlike the CERTS, which are based on collaborative and hierarchical principles, intergovernmental organizations are composed of equal actors defined by their status as sovereign entities. All of these organizations are driven first and foremost by their own formal mandates and priorities.

If we focus on organizations that, in principle, have some clear interest or focus on cyberspace, we can identify the major actors and their zones of activity or interest. Unsurprisingly, this leads to a diffuse network of organizations and a wide array of cross-cutting linkages. By way of orientation, we show in Figure 4 several well-known international organizations (such as the UN) and new cyber-focused entities that do not have the status of 'organization' but are likely to retain a long standing institutional presence on the international arena (such as the World Summit on the Information Society).

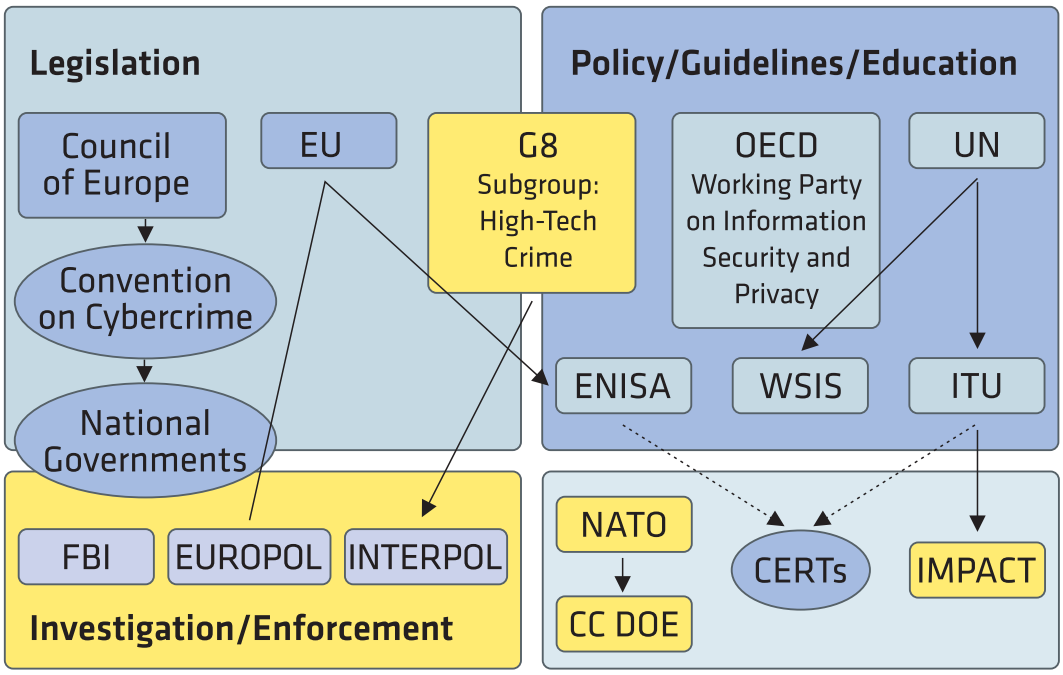

Figure 4: Key Intergovernmental Institutions

The involvement of international organizations in internet security issues can be traced to early meetings of the G8 Subgroup on Hi-Tech Crime. In 1997, the G8, comprised of the world's most developed economies, in cooperation with the International Criminal Police Organization (INTERPOL), established a 24/7 'Network of Contacts' in order to help national governments »identify the source of terrorist communications, investigate threats and prevent future attacks« [3].

In most cases, international organizations cede direct action to national governments, and instead focus on organizing conferences that bring together security professionals, academics, law enforcement agencies, and government representatives. The white papers that they publish serve a key role in building international consensus and developing standard practices and guidelines. In many ways this process is an important milestone in the emerging response to cyber threats and the quest for cyber security.

A closer look at two such conferences: The *Working Party on Information Security and Privacy* (WPISP) and *The World Summit on the Information Society (WSIS)*, helps to clarify the nature

of the intergovernmental cyber security system by illustrating the broad differences in institutional and statutory status that characterize current inter-governmental initiatives.

The OECD has been actively involved in the internet security landscape since 2002 [4]. The *Working Party on Information Security and Privacy* (WPISP) is supported by the OECD-Secretariat within the Directorate for Science, Technology and Industry. The WPISP develops public policy analysis and high level recommendations to help governments and other stakeholders ensure that security and privacy protection foster the development of the Internet economy. WPISP delegates come from various government bodies with an interest in the economic and social aspects of information security and privacy. Non-governmental stakeholders participate actively in the dialogue through the Business and Industry Advisory Committee to the OECD (BIAC), the Civil Society Information Society Advisory Council (CSISAC) and the Internet Technical Advisory Committee (ITAC). The WPISP has also established relationships with other international and regional organisations such as Council of Europe, Asia-Pacific Economic Co-operation, ENISA, the International Conference of Data Protection and Privacy Commissioners, and the Global Privacy Enforcement Network.

The World Summit on the Information Society (WSIS) represents the opposite end of the spectrum. Rather than focusing narrowly on security issues, the summit was convened under the auspices of the United Nations as the first comprehensive response to the emergent 'virtual' global society. Interestingly, the WSIS objectives that dealt with cyber security were broadly consistent with the goals and orientation of the WPSIP. Given differences in impetus, legal status, and participation, this alignment of concerns can be seen as another instance of consensus building within the international community. As an UN-based initiative, WSIS decisions were made at the state-level, and only sovereign states served as 'decision-makers.'

For the most part, the foregoing efforts can be seen as 'self-initiated,' whereby private or public entities voluntarily take on a particular function in the emergent cyber security domain. However, more recently the international community has issued operational mandates to specific organizations.

The International Telecommunications Union (ITU)

ITU was given the primary responsibility for coordinating the implementation of WSIS' Action Plan C5 [5]. Utilizing a group of high-level experts, ITU provides a variety of resources and toolkits addressing legislation, awareness, self-assessment, botnets, and CERTs [6]. Additionally, ITU publishes guides that educate developing nations on cybercrime and promote best practices and approaches. One of ITU's core missions is to standardize telecommunication technology and release statistics that can be used to track the internet connectivity of nations [7]. Its efforts to promote cyber security arose as a function of the increasing threat rather than as part of its original mission. Thus the international community chose to build upon existing organizational strengths rather than establishing a new institution.

Although the ITU's core competencies are mission specific, they have recently acted in a direct fashion by establishing an arm that will provide international threat response. Envisioned as a global response centre focused on combating cyber terrorism and protecting critical infrastructure networks, the *International Multilateral Partnership against Cyber Threats* (IMPACT) is a public/private venture headquartered in Malaysia [8]. Among other services, IMPACT offers a real-time warning network to 191 member countries, 24/7 response centres, and software that allows security organizations across the globe to pool resources and coordinate their defence efforts [9]. Additionally, IMPACT maintains a research division, hosts educational workshops, and conducts high-level security briefings with representatives of

member states. These efforts are intended to make IMPACT the »the foremost cyber threat resource centre in the world« [10].

NATO

In a similar vein to IMPACT, a second major adaptive case is demonstrated by NATO. This intergovernmental organization established a technical response arm in the aftermath of the coordinated attacks on Estonia in 2007. Designated the Cooperative Cyber Defence Centre of Excellence (CCD COE), the entity is responsible for training NATO member states, conducting attack exercises, and supporting NATO in the event of an international cyber-attack [11]. Interestingly, not all NATO states have joined the CCDCOE program, with many countries opting to rely on their own traditional military cyber defence networks. There is no strong evidence that all members of NATO are willing to engage in a common approach to a shared problem, presumably because many states are developing their own strategies for cyber warfare. At the same time, however, the CCDCOE fills an important void for several European states, notably those whose own cyber security capabilities are yet to be developed.

ENISA

Although the European Union has published numerous resolutions on cybercrime, and EUROPOL is actively engaged in investigation, the most important action which performed by EU's was the creation of the European Network and Information Security Agency (ENISA). The Agency's Mission is essential to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union.

ENISA is helping the European Commission, the Member States and the business community to address, respond and especially to prevent Network and Information Security problems.

2.3 National Organizations

The United States has been at the forefront of institutional response to the new realities formed by cyberspace. It is the leading world power, the state that originally encouraged and supported the creation of cyberspace, and the country that remains renowned for its innovative spirit. By default, the United States has been thrust in a leadership position and has acted as a model for other governmental response to cyber issues, notably in Europe and Asia [1].

The Federal government is not organized to address this growing problem effectively now or in the future. Responsibilities for cyber security are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions.

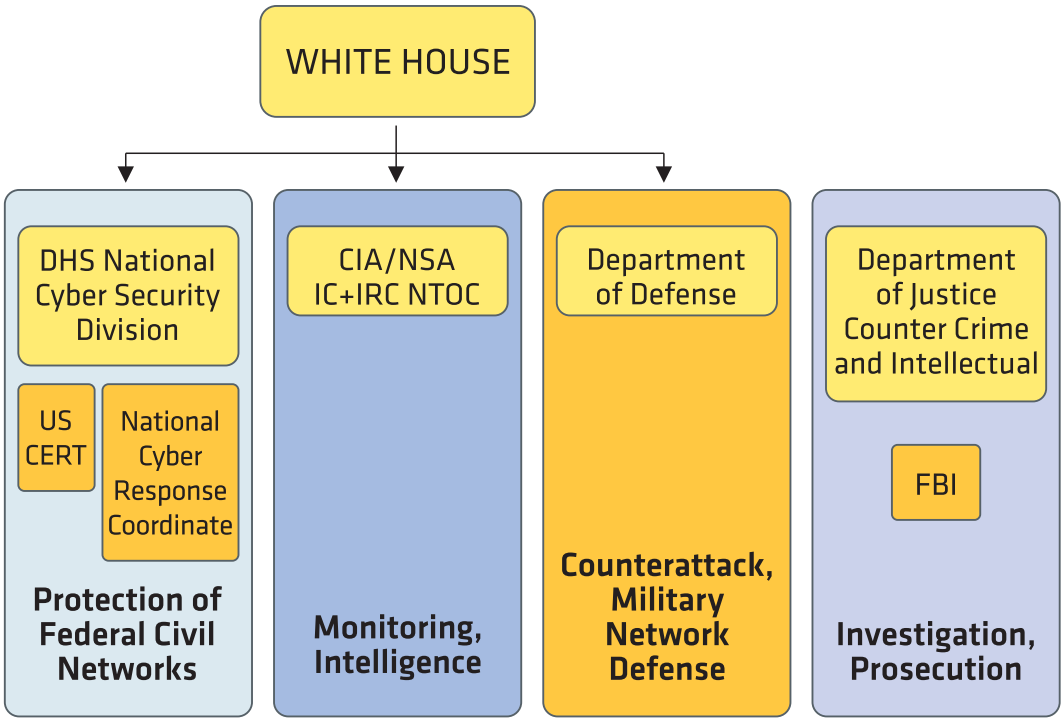

Figure 5: Proposed Cyber security organization in US [1]

Detailed information about Cyber security organization in US will be presented in the next chapter.

3 Cybersecurity standards and frameworks

The issue of managing cybersecurity risk is recognized as essentially to be addressed by global cooperation and joint work on establishing approaches for »prioritized, flexible, repeatable, performance-based, and cost-effective activities« for assisting organizations to manage cybersecurity risk [12]. It is not expected to define exhaustive model applicable to any organization or government, it is rather to provide a model covering all phases (e.g. establishing, implementing, operating, monitoring, reviewing, maintaining, and improving) which adoption should be a strategic decision for an organization [13].

The general methodological approach which is used is leveraged on »Plan-Do-Check-Act« (PDCA) model [14], which is commonly used in cases when new approaches are implementing and when improvements of existing models are needed. The four phases in the Plan-Do-Check-Act Cycle involve:

- Plan: Identifying and analysing the problem.
- Do: Developing and testing a potential solution.
- Check: Measuring how effective the test solution was, and analysing whether it could be improved in any way.
- Act: Implementing the improved solution fully.

The application of PDCA model is essential since cybersecurity framework should support both, (I) an organization without an existing cybersecurity program in order to create new cybersecurity program, and (II) organizations that can improve existing cybersecurity risk management. Each activity in the framework should be referenced and mapped to a subset of commonly used standards and guidelines. These standards provide advice and guidelines on best practice in support of activities in both, establishing and managing, and implementation of cybersecurity systems in accordance with existing normative references[2] and standards[3].

This section is divided into three sub-sections: Sub-section 3.1 is presenting International Standard ISO/IES 27001 at conceptual level of establishing and/or improving Information Security Management System (ISMS); sub-section 3.2 presents framework for implementation of defined standards; and finally, sub-section 3.3 is presenting practical guidance to administrators trying to secure their information and services.

3.1 International Standard ISO/IEC 27001

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. In the field of information technology, ISO and IEC have established a joint technical committee,

[2] ISO/IEC 17799:2005 Information technology- Security techniques- Code of practice for information security management, recently updated to: ISO/IEC 27002:2005 (http://www.iso.org/iso/catalogue_detail?csnumber=50297)

[3] If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of International Standard ISO/IEC 27001 within existing management system

ISO/IEC JTC 1. They established the International Standard [13] that has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the ISMS. The adoption of ISMS should be a strategic decision for an organisation, i.e. it is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.

In accordance with PDCA model, the ISMS processes are established on the Figure 6.

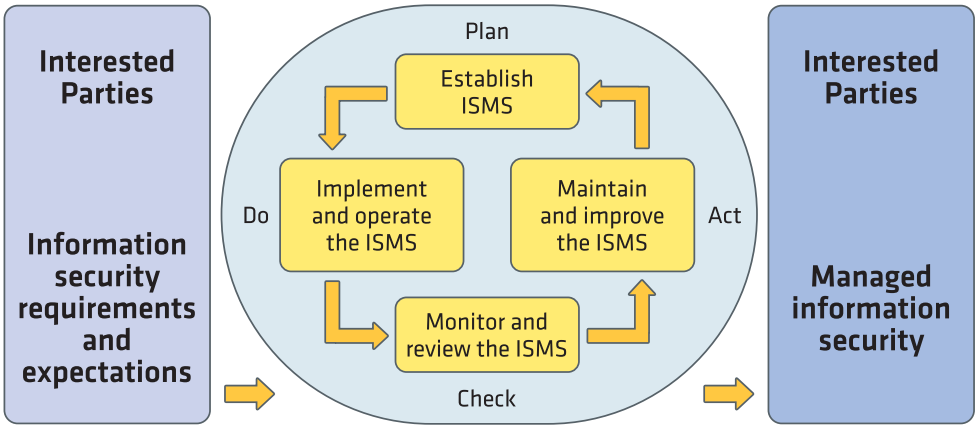

Figure 6: PDCA model applied to ISMS processes [13]

The International Standard identifies specific sub-activities related to each activity in ISMS processes (Table 2 summarizes all activities) with control objectives and controls that shall be selected as part of the ISMS processes. Controls specified in ISO/IEC 27001:2005 (A.5 to A.15) are not exhaustive and an organization may consider that additional control objectives and controls are necessary. Furthermore, ISO/IEC 17799:2005 [15] Clauses 5 to 15 provide implementation advice and guidelines to best practice in support to those controls.

Due to space limitation of the report, control objectives and implementation advice and guidance are not listed since online available at specified URLs.

Table 2: ISMS activities and sub-activities

Activity	Sub-activities	
Establish the ISMS	a.	Define the scope and boundaries of the ISMS
	b.	Define the ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology
	c.	Define the risk assessment approach of the organisation
	d.	Identify the risks
	e.	Analyse and evaluate the risks
	f.	Identify and evaluate options for the treatment of risks

Activity	Sub-activities	
	g.	Select control objectives and controls for the treatment of risks
	h.	Obtain management approval of the proposed residual risks
	i.	Obtain management authorization to implement and operate the ISMS
	j.	Prepare a Statement of Applicability (providing a summary of decisions concerning risk treatment)
Implement and operate the ISMS	a.	Formulate a risk treatment plan
	b.	Implement the risk treatment plan in order to achieve the identified control objectives
	c.	Implement control objectives
	d.	Define how to measure the effectiveness of the selected controls and specify how these measurements to be used
	e.	Implement training and awareness programmes
	f.	Manage operations of the ISMS
	g.	Manage resources of the ISMS
	h.	Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents
Monitor and review the ISMS	a.	Execute monitoring and reviewing procedures and other controls
	b.	Undertake regular reviews of the effectiveness of the ISMS
	c.	Measure the effectiveness of controls to verify that security requirements have been met
	d.	Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks
	e.	Conduct internal ISMS audits at planned intervals
	f.	Undertake a management review of the ISMS on a regular basis
	g.	Undertake security plans
	h.	Record actions and events that could have an impact on the effectiveness or performance of the ISMS

The International Standards put special importance on documentation requirements and management issues. Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and ensure that the recorded results are reproducible [13]. Furthermore, management responsibilities are divided in two categories concerning:

1. Management commitment (providing evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS);
2. Resource management (aimed on providing needed resources and ensuring that personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks).

Additionally, the following requirement and responsibilities are defined:

1. Internal ISMS audits (the organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS are effectively implemented, confirmed to requirements and performed as expected);
2. Management review of the ISMS;
3. ISMS improvement (aimed on providing continual improvement, taking actions to eliminate the cause of nonconformities with the ISMS requirements and taking preventive actions).

3.2 Cybersecurity framework

Whereas standards are accepted as best practices, frameworks are practices that are generally employed and should be developed in accordance with established standards. Critical infrastructure defined as »systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters« [16] is recognized as a key factor of the national and economic security. To this end, cybersecurity framework is relied on existing standards, guidance, and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk.
The Cybersecurity Framework (»Framework«) [12] established by NIST (National Institute of Standards and Technology- USA) is initiated by Executive Order 13636 (EO), »Improving Critical Infrastructure Cybersecurity« on February 12, 2013 by USA President Obama. Prior to this order, in May, 2009 President of USA, Barack Obama [16] gave the speech about international cyberspace policy as the belief that networked technologies hold immense potential for the whole nation, and for the world. The 'Strategy for Cyberspace'[4] [16] established in May, 2011 defines the issues of prosperity, security, and openness in a networked world as a strategic framework. The Framework [12] is developed in collaboration with industry and provides guidelines to an organization on managing cybersecurity risk, in a

[4] The 'Strategy for Cyberspace' identifies seven areas of activity, each demanding collaboration within government, with international partners, and with the private sectors. This strategic framework outlined call for and guide specific actions in the following areas: (I) Economy: Promoting International Standards and Innovative, Open Markets; (II)Protecting Networks: Enhancing Security, Reliability, and Resiliency; (III) Law Enforcement: Extending Collaboration and the Rule of Law; (IV) Military: Preparing for 21st Century Security Challenges; (V) Internet Governance: Promoting Effective and Inclusive Structures; (VI) International Development: Building Capacity, Security, and Prosperity; (VII) Internet Freedom: Supporting Fundamental Freedoms and Privacy.

manner similar to financial, safety, and operational risk. To this end, the Framework provides a common language and mechanism for organizations to:

1. Describe current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within context of risk management;
4. Assess progress toward the target state;
5. Foster communications among internal and external stakeholders.

Generally, the Framework can be divided in two parts, the first one representing conceptual framework for managing risk issues with demonstrated implementation, while the second part is focused on identification of areas for improvement and further development.

3.1.1 Risk Managements and Cybersecurity Framework

The framework structure is designed to support existing aspects of business operations, and can be used as the basis for creating a new cybersecurity program for an organisation that does not already have one. Also, the Framework is appropriate for identifying gaps in existing cybersecurity program and activities for their improvement.

The Framework is composed of three parts:

- *Framework Core* – presents standards and best practices in a manner that allows for communication and risk management across the organization from the senior executive level to the implementation/operations level;
- *Framework Implementation Tires* – demonstrate the implementation of the Framework Core;
- *Framework Profile* – conveys how an organization manages cybersecurity risk and identifies the appropriate goals for an organization or for a critical infrastructure sector and to access progress against meeting those goals.

Methodologically, the Framework is focused on creation of a Profile (Figure 7) that can be used to describe both the current state and the desired target state of specific cybersecurity activities, thus revealing gaps that should be addressed to meet cybersecurity risk management objectives. Identifying the gaps between the Current Profile and the Target profile allows the creation of a roadmap that organisations should implement to reduce cybersecurity risk.

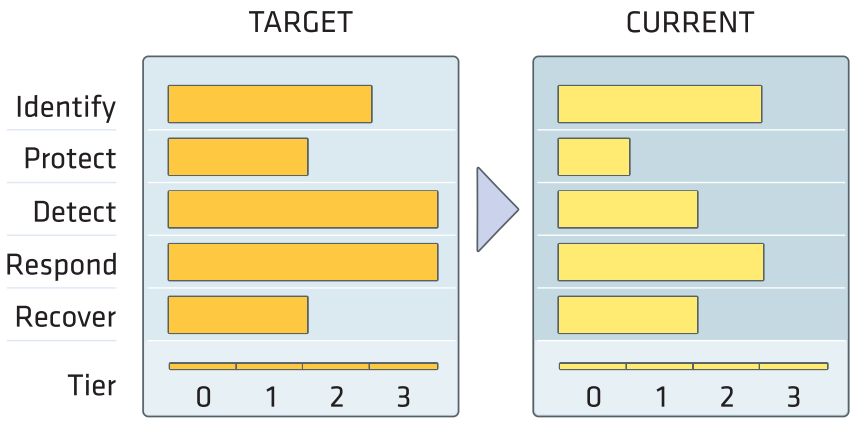

Figure 7: Framework Profile [12]

The Profile is the selection of the Functions, Categories, and Subcategories that are aligned with the business requirements, risk tolerance, and resources of the organization.

Functions provide the highest level of structure, for organizing cybersecurity activities into Categories and Subcategories. These Functions are: Identify, Protect, Detect, Respond, and Recover.

Categories are the subdivisions of a Function into groups of cybersecurity activities, more closely tied to programmatic needs. Examples of Categories include »Asset Management«, »Access Control«, and »Detection Processes.«

Subcategories further subdivide a Category into high-level tactical activities to support technical implementation. Examples of subcategories include »Inventory and track physical devices and systems within the organization«, »Protect network integrity by segregating networks/implementing enclaves (where appropriate)«, and »Assess the impact of detected cybersecurity events to inform response and recovery activity

Informative References are specific sections of standards and practices common among critical infrastructure sectors and illustrate a method to accomplish the activities within each Subcategory. The Subcategories are derived from the Informative References. The Informative References presented in the Framework Core are not exhaustive, and organizations are free to implement other standards, guidelines, and practices. List of all categories and references are given in Appendix.

Finally, Implementation of the Profile is communicated by the implementation/operations level to the business/process level, where an impact assessment is made. The outcomes of that impact assessment are reported to the senior executive level to inform the organization's overall risk management process.

3.1.2 Areas of Improvement for the Cybersecurity Framework

Collaboration and cooperation must increase for these areas to further understanding and/or the development of new or revised standards. The initial Areas for Improvement are as follows:

- Authentication;
- Automated Indicator Sharing;
- Conformity Assessment;
- Data Analytics;
- International Aspects, Impacts, and Alignment;
- Privacy;
- Supply Chains and Interdependencies.

This is not intended to be an exhaustive list, but these are highlighted as important areas that should be addressed in future versions of the Framework.

3.3 Cybersecurity and practice for information security management

A guide to developing computer security policies and procedures is usually published in the form of handbooks and practical publications. The RFC 2196 published by Network Working Group in 1997 [17] defines practical guidance to administrators trying to secure their information and services. The subjects covered include policy content and formation, a broad range of technical system and network security topics, and security incident response.

Firstly, the Handbook introduce the need of establishing a security policy as a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide. One of the most important reasons for creating a computer security policy is to ensure that efforts spent on security yield cost effective benefits. The policy includes references to standards and framework and then identifies technical elements of policy implementation.

Practical issues covered by this Handbook, recognized of the importance for setting computer security procedures for sites that have systems on the Internet. This guide lists the following issues and factors that a site must consider when setting their own policies:

1. Architecture;
2. Network and Service Configuration (Protecting the Infrastructure, Protecting the Services, Name Servers (DNS and NIS (+)), Authentication/Proxy Servers (SOCKS, FWTK), Electronic Mail, File Transfer (FTP, TFTP), NFS, etc.);
3. Security Services and Procedures (Authentication, Confidentiality, Integrity, Authorization, Access, Auditing, Securing Backups);
4. Security Incident Handling (Preparing and Planning for Incident Handling, Notification and Points of Contact, Identifying an Incident, Handling an Incident, Aftermath of an Incident, Responsibilities).

Similar to Handbook RFC 2196 [17], different areas in cyberspace such as banking sector, finances, governments, etc. impose creation of detailed recommendations and issues specific to domains of applications and identified issues for cyber protection. Table 3 gives an overview of existing practical guidelines and handbooks for implementation.

Table 3: Existing practical guidelines and handbooks in different cyber domains and areas

Cyberspace Domain	Publication
Banking and finance sector	[18] [19]
Health care system	http://www.igi-global.com/book/handbook-research-advances-health-informatics/441
Cloud computing	http://www.cyber-cloud.com/

Cyberspace Domain	Publication
Computer crime laws	http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1258&context=chtlj
Web 2.0, 3.0	http://www.igi-global.com/book/handbook-research-web/518&f=e-book

4 International cybersecurity strategies, best practices, frameworks

4.1 ITU

The International Telecommunication Union (ITU) is the specialized agency of the United Nations which is responsible for Information and Communication Technologies. Cybersecurity is considered in the »C5« World Summit on Information Society (WSIS)[5] Action Line of the Geneva Action Plan on building confidence and security in the use of ICT. ITU deals also with adopting international standards to ensure seamless global communications and interoperability for next generation networks; building confidence and security in the use of ICTs; emergency communications to develop early warning systems and to provide access to communications during and after disasters, etc.

In the following, ITU activities are grouped into two subsections: Section 4.1.1. is focused on **holistic** framework established by ITU aimed on coordinating, developing and implementing global culture of cybersecurity, while Section 4.1.2. gives recommendations and methodological solutions for their adoptions at national levels due to national heterogeneity and diversity among nations.

4.1.1 ITU Global Cybersecurity Agenda (GCA)

In May 2007, the ITU launched the Global Cybersecurity Agenda (GCA) [20] to provide a framework within which an international response to the growing challenges to cybersecurity can be coordinated and addressed. The GCA is based on international cooperation and strives to engage all relevant stakeholders in a concerted effort to build confidence and security in the information society. The GCA is built upon five strategic pillars, also known as work areas, and made up of the following seven main strategic goals:
1. *Legal Measures* - The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cybersecurity.

The ITU cybercrime legislation resources currently consist of two main deliverables, the ITU publication titled ITU Toolkit for Cybercrime Legislation and »Understanding Cybercrime: A Guide for Developing Countries« [21] aims to help developing countries better understand the national and international implications of growing cyber-threats, assess the requirements of existing national regional and international instruments, and assist countries in establishing a sound legal foundation.

The ITU Toolkit for Cybercrime Legislation [22] aims to provide countries with sample legislative language and reference material that can assist in the establishment of harmonized

[5] http://www.itu.int/wsis/index.html

cybercrime laws and procedural rules. The Toolkit is a practical instrument that countries can use for the elaboration of a cybersecurity legal framework and related laws.

2. *Technical and Procedural Measures*- ICTs is a vital tool in information societies. The mail goal in the field of standardization is defined as: brings together the private sector and governments to coordinate work and promote the harmonization of security policy and security standards on an international scale.

Standards development bodies have a vital role to play in addressing security [6] and due to constant improvement in ICTs, all standards are changing simultaneously.

3. *Organizational Structures*- Individuals, organizations and governments are increasingly dependent on globally interconnected networks. In order to protect network infrastructures and address threats, coordinated national action is required to prevent, respond to and recover from incidents. It is proposed to establish national cybersecurity response centres, such as computer incident response teams (CIRTs) [23], noting that there is still a low level of computer emergency preparedness within many countries, particularly developing countries and that a high level of interconnectivity of ICT networks could be affected by the launch of an attack from networks of the less-prepared nations.

4. *Capacity Building*- Several regional initiatives are already recommending that Member States establish national cybersecurity response centres, such as computer incident response teams (CIRTs), and also to invite Member States to promote the development of educational and training programmes to enhance user awareness of risks in cyberspace.

Furthermore, ITU developed several tools aimed on assisting member countries to develop their own cyber security elements, such as:

- ITU National Cybersecurity/CIIP Self-Assessment Tool [24] aims to assist ITU Member States in developing their national strategy by examining their existing capacities for addressing challenges to cybersecurity and CIIP, identifying their requirements and outlining a national response plan.
- ITU Toolkit for Promoting a Culture of Cybersecurity [25]aims to provide guidelines on how to raise awareness on cybersecurity issues for SMEs, consumers and end-users in developing countries
- ITU is working with experts on developing a practical Botnet Mitigation Toolkit[7] to assist developing countries in particular to deal with the growing problem of botnets. The Botnet Mitigation Toolkit is a multi-stakeholder, multi-pronged approach to track botnets and mitigate their impact, with a particular emphasis on the problems specific to emerging internet economies.

5. *International Cooperation* - Cybersecurity is as global and far-reaching as the Internet. Therefore solutions need to be harmonized across all borders. This necessarily entails international cooperation, not only at government level, but also with industry, non-governmental and international organizations.

[6] As well as many key security Recommendations, ITU has developed overview security requirements, security guidelines for protocol authors, security specifications for IP-based systems it defines (NGN, H.323, IPCableCom, etc), guidance on how to identify cyber threats and countermeasures to mitigate risks. ITU also provides the international platform for the development of the protocols that protect current and Next-Generation Networks (NGN).

[7] *Information about the ITU Botnet Mitigation, Toolkit is available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html*

4.1.2 ITU National Strategy Guide

At the national level, enhancing cybersecurity and protecting critical information infrastructures is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens.

In September 2011, ITU established 'ITU National Cybersecurity Strategy Guide' [26]which is focused on the issues that countries should consider when elaborating or reviewing national cybersecurity strategies. Since national capabilities, needs and threats vary, national values are recommended as the basis for strategies which is derived from GCA. Methodologically, this approach is rooted in the Ends-Ways-Means strategy[8] paradigm due to its popularity with national policy makers.

This Guide aims to assist States as they build capacity to identify goals, constraints and stakeholders of a national cybersecurity strategy. Graphical presentation of the National Model is given on the Figure 8.

In this context, the term of »***Cybersecurity ends***« means the objectives that a national cybersecurity strategy seeks to accomplish. Cybersecurity ends describe what a nation has to do to support national interests in cyberspace. As strategies are often written by technical experts, ITU suggests to that countries assign CS ends the same titles as the core national interest categories, so all misunderstanding will be avoid. Also, losing focus on national values must be avoided.

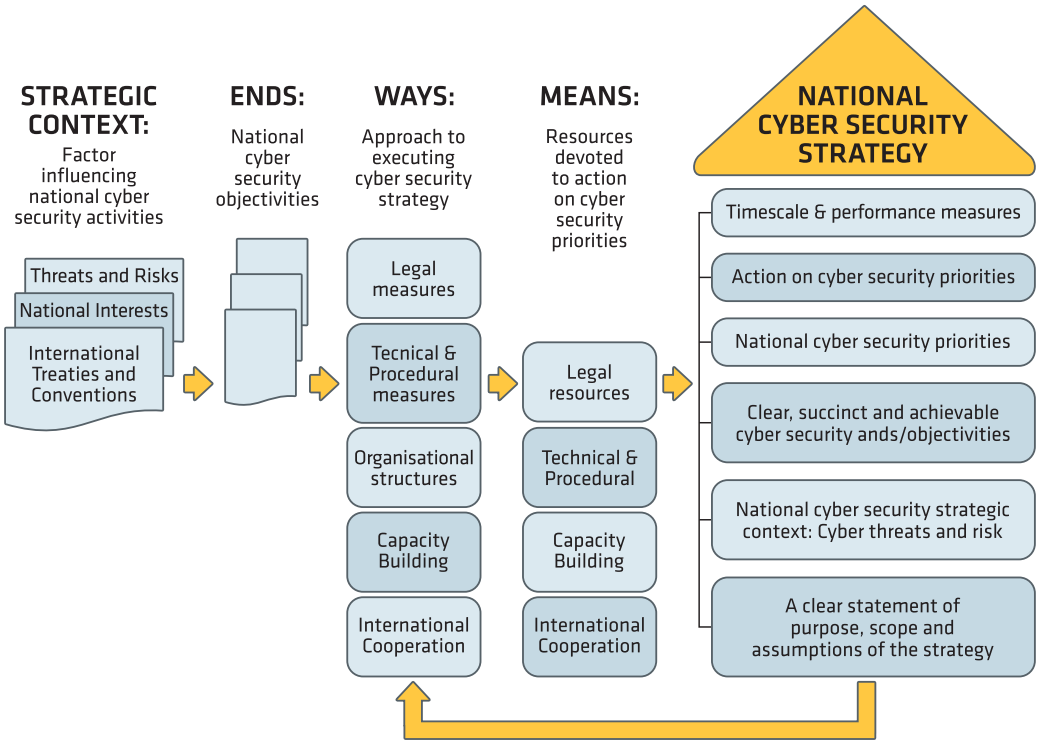

Figure 8: National Cyber security Strategy Model

[8] The model is known as »ends, ways, and means," where ENDS = WAYS + MEANS. Ends are defined as the strategic outcomes or end states desired. Ways are defined as the methods, tactics, and procedures, practices, and strategies to achieve the ends. Means are defined as the resources required achieving the ends, such as troops, weapons systems, money, political will, and time. The model is really an equation that balances what you want with what you are willing and able to pay for it or what you can get for what you are willing and able to pay.

This national cyber security strategy model chose the five pillars of the GCA as the forms through which States may pursue national cyber security strategies, as follows:

Pillar 1 – Legal Measures

This Pillar seeks to elaborate strategies for the development of model globally applicable and interoperable cybercrime legislation. The overall goal of the Pillar is to develop advice and internationally compatible processes for handling crime committed over ICTs.

Pillar 2 – Technical and Procedural Measures

This Pillar focuses on measures for addressing vulnerabilities in software products. The pillar aims to devise globally acceptable accreditation schemes, protocols and standards.

Pillar 3 – Organizational Structures

The Pillar aims to create organisational structures and strategies to help prevent, detect and respond to attacks against critical information infrastructures.

Pillar 4 – Capacity Building

This Pillar seeks to elaborate strategies for enhancing knowledge and expertise to boost cyber security on the national policy agenda.

Pillar 5 – International Cooperation

The Pillar focuses on strategies for international cooperation, dialogue and coordination.

Furthermore, the GCA contains ten cyber security programme elements. These are:

1. *Top Government Cybersecurity Accountability;*
   Top government leaders are accountable for devising a national strategy and fostering local, national and global cross-sector cooperation.
2. *National Cybersecurity Coordinator;*
   An office or individual oversees cybersecurity activities across the country.
3. *National Cybersecurity Focal Point;*
   A multi-agency body serves as a focal point for all activities dealing with the protection of a nation's cyberspace against all types of cyber threats.
4. *Legal Measures;*
   Typically, a country reviews and, if necessary, drafts new criminal law, procedures, and policy to deter, respond to and prosecute cybercrime.
5. *National Cybersecurity Framework;*
   Countries typically adopt a Framework that defines minimum or mandatory security requirements on issues such as risk management and compliance.
6. *Computer Incident Response Team (CIRT);*
   A strategy-led programme contains incident management capabilities with national responsibility. The role analyses cyber threat trends, coordinates response and disseminates information to all relevant stakeholders.
7. *Cybersecurity Awareness and Education;*
   A national programme should exist to raise awareness about cyber threats.

8. *Public-Private Sector Cybersecurity partnership;*
   Governments should form meaningful partnership with the private sector.
9. *Cybersecurity Skills and Training Programme;*
   A programme should help train cybersecurity professionals.
10. *International Cooperation;*
    Global cooperation is vital due to the transnational nature of cyber threats.

In the proposed model, '***Cybersecurity Ways'*** identify the strategic activities to help countries govern the pillars. Governance defines how nations may use the resources in the five pillars to attain the outcomes that the ends envisage. In the multi-stakeholder domain of cybersecurity, the ways define how nations may allocate resources, coordinate and control the activities of all relevant stakeholders.

Clear governance structures further confer legitimacy on stakeholders including government. Importantly, the ways define expectations for activities and thus are a basis for verifying performance.

The '***Cybersecurity Means'*** flow from the Ways. The means describe the resources available to achieve the stated ends. Local conditions should determine the type and order of actions appropriate to be chosen from this list. The only condition, of course, is that one does not lose track of the GCA association.

The Table 4 below gives an overview of priorities of all Cyber Ends, Cyber Ways and Cyber Means Actions.

Table 4: Overview of priorities and related GCA goals

End Cyber-Security Priorities	Ways- Priorities (5 pillars)	Means Actions
National security	**Legal measures** • Legal measures strategy • Government Legal Authority • Parliamentary Cybersecurity Process • Law Enforcement Governance Framework • Global Fight against Cybercrime	**Legal Actions** • Legal measured Strategy • Review Adequacy of Legislation • Government Legal Authority
Economic well-being	**Technical and procedural measures** (i) PROCEDURAL MEASURES • Cybersecurity Goals • National Cybersecurity Framework (ii)TECHNICAL MEASURES • Network Protection Strategy Principles	**Technical and procedural Actions** (i)PROCEDURAL MEASURES • National Cybersecurity Framework (Cybersecurity Accountability, Risk management, Security Policies, Compliance and Assurance)

End Cyber-Security Priorities	Ways- Priorities (5 pillars)	Means Actions
	• Global Cooperation on Technical Measures	(ii) TECHNICAL MEASURES • Deploy Technical Solutions • Secure Applications • Secure Government Infrastructure • Technical Measures Actions (Business Objectives, Cyber Threats, Risk Management, Technical Measures, Accreditation Maintenance)
Promotion of values	**Organizational structures** • Governmental organizational structures • National Cybersecurity Focal Point • National Computer Incident Response Team (CIRT) • Cybersecurity partnership • National cybercrime units	**Organizational structures** • Role of Government • National Focal Point • National CIRT
Favourable world order **(seen as macro-national interest category)**	**Capacity Building** • Cybersecurity skills and trainings • Judicial capacity • National culture of cybersecurity • Cybersecurity innovation	**Capacity Building** • Cybersecurity skills and trainings (Cybersecurity Framework Assumptions, etc.) • Culture of Cybersecurity (National Awareness Program, Cybersecurity Culture in Government, Cybersecurity in Business Enterprises, Children and Vulnerable individuals) • Cybersecurity innovation

End Cyber-Security Priorities	Ways- Priorities (5 pillars)	Means Actions
Governance **(i.e. Cybersecurity Ends Consideration: (i) Role in ICTs, (ii) Stakeholders and Roles – lead institutions for each sector, (iii) International Cooperation)**	**International Cooperation**	**International Cooperation** • International Cybersecurity Strategy

Finally, Assurance and Monitoring activities are aimed to monitor cybersecurity programmes to ensure that they meet business requirements. The ITU strategy recommends re-using the ISO/IEC 27001-based Plan-Do-Check-Act (PDCA) model (which is described above in Section II). The model helps structure Information Security Management Systems (ISMSs). The PDCA model also reflects the OECD guidelines towards building a culture of security [27]. Therefore, the use of the PDCA model supports the GCA notably international cooperation.

4.2 EU-level

The cyber security strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, outlines the EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world. This vision can only be realised through a true partnership, between many actors, to take responsibility and meet the challenges ahead.

This strategy clarifies the next principles that should guide cyber security policy in the EU and internationally [28]:

- **The EU's core values apply as much in the digital as in the physical world.** The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain.
- **Protecting fundamental rights, freedom of expression, personal data and privacy.** Cyber security can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field.
- **Access for all.** Limited or no access to the Internet and digital illiteracy constitute a disadvantage to citizens, given how much the digital world pervades activity within society. Everyone should be able to access the Internet and to an unhindered flow of information. The Internet's integrity and security must be guaranteed to allow safe access for all.

- **Democratic and efficient multi-stakeholder governance.** The digital world is not controlled by a single entity. There are currently several stakeholders, of which many are commercial and non-governmental entities, involved in the day-to-day management of Internet resources, protocols and standards and in the future development of the Internet. The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach.
- **A shared responsibility to ensure security.** The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities which need to be properly defined, thoroughly analysed, remedied or reduced. All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect them and if necessary ensure a coordinated response to strengthen cyber security.

The EU vision presented in the strategy is articulated in five strategic priorities [29]:

1. Achieving cyber resilience;
2. Drastically reducing cybercrime;
3. Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
4. Develop the industrial and technological resources for cyber security;
5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.

a) Achieving cyber resilience

To promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and cooperate effectively. Building on the positive results achieved via the activities carried out to date, further EU action can help in particular to counter cyber risks and threats having a cross-border dimension, and contribute to a coordinated response in emergency situations. This will strongly support the good functioning of the internal market and boost the internal security of the EU.

Main actions which will be taken are [29]:

- The Commission will continue its activities, carried out by the Joint Research Centre in close coordination with Member States authorities and critical infrastructure owners and operators, on identifying NIS vulnerabilities of European critical infrastructure and encouraging the development of resilient systems.
- ENISA will assist the Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure.
- ENISA will continue supporting the Member States and the EU institutions in carrying out regular pan-European cyber incident exercises which will also constitute the operational basis for the EU participation in international cyber incident exercises.
- ENISA has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships. Europol, Eurojust and national data protection authorities are also active in raising awareness.

b) Drastically reducing cybercrime

Cybercriminals and cybercrime networks are becoming increasingly sophisticated and we need to have the right operational tools and capabilities to tackle them. Cybercrimes are high-

profit and low-risk, and criminals often exploit the anonymity of website domains. Cybercrime knows no borders - the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative cross border approach to respond to this growing threat.

The EU and the Member States need strong and effective legislation to tackle cybercrime. The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, is a binding international treaty that provides an effective framework for the adoption of national legislation. The Commission will urge those Member States that have not yet ratified the Convention to ratify and implement its provisions as early as possible.

Currently, not all EU Member States have the operational capability they need to effectively respond to cybercrime. All Member States need effective national cybercrime units, in accordance with that the Commission will support the Member States to identify gaps and strengthen their capability to investigate and combat cybercrime, through its funding programmes. The Commission will furthermore support bodies that make the link between research/academia, law enforcement practitioners and the private sector, similar to the on-going work carried out by the Commission-funded Cybercrime Centres of Excellence already set up in some Member States. Also, the Commission together with the Member States will coordinate efforts to identify best practices and best available techniques including with the support of JRC to fight cybercrime.

In accordance to improve coordination at EU level, the EU can complement the work of Member States by facilitating a coordinated and collaborative approach, bringing together law enforcement and judicial authorities and public and private stakeholders from the EU and beyond. The Commission will support the recently launched European Cybercrime Centre (EC3) as the European focal point in the fight against cybercrime. The EC3 will provide analysis and intelligence, support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders and gradually serve as a voice for the law enforcement community [29].

c) Developing cyber defence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)

Cyber security efforts in the EU also involve the cyber defence dimension. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyber defence capability development should concentrate on detection, response and recovery from sophisticated cyber threats. Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, private sector and academia in the EU.

The High Representative will focus on the following key activities and invite the Member States and the European Defence Agency to collaborate [29]:

- Assess operational EU cyber defence requirements and promote the development of EU cyber defence capabilities and technologies to address all aspects of capability development - including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability;
- Develop the EU cyber defence policy framework to protect networks within CSDP missions and operations, including dynamic risk management, improved threat analysis and information sharing. Improve Cyber Defence Training & Exercise

Opportunities for the military in the European and multinational context including the integration of Cyber Defence elements in existing exercise catalogues;

- Promote dialogue and coordination between civilian and military actors in the EU – with particular emphasis on the exchange of good practices, information exchange and early warning, incident response, risk assessment, awareness raising and establishing cyber security as a priority
- Ensure dialogue with international partners, including NATO, other international organisations and multinational Centres of Excellence, to ensure effective defence capabilities, identify areas for cooperation and avoid duplication of efforts.

d) Develop industrial and technological resources for cyber security

Europe has excellent research and development capacities, but many of the global leaders providing innovative ICT products and services are located outside the EU. There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers. It is vital to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data.

A Europe-wide market demand for highly secure products should also be stimulated. First, this strategy aims to increase cooperation and transparency about security in ICT products. It calls for the establishment of a platform, bringing together relevant European public and private stakeholders, to identify good cyber security practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions. A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally. The Commission will promote the adoption of coherent approaches among the Member States to avoid disparities causing locational disadvantages for businesses. Second, the Commission will support the development of security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing, while taking in due account the need to ensure data protection. Work should focus on the security of the supply chain, in particular in critical economic sectors (Industrial Control Systems, energy and transport infrastructure) [29].

The Commission will use Horizon 2020 to address a range of areas in ICT privacy and security, from R&D to innovation and deployment. Horizon 2020 will also develop tools and instruments to fight criminal and terrorist activities targeting the cyber environment.

e) Establish a coherent international cyberspace policy for the European Union and promote EU core values

Preserving open, free and secure cyberspace is a global challenge, which the EU should address together with the relevant international partners and organisations, the private sector and civil society.

The Commission, the High Representative and the Member States should articulate a coherent EU international cyberspace policy, which will be aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and private sector.

To address global challenges in cyberspace, the EU will seek closer cooperation with organisations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS. At bilateral level, cooperation with the United States is particularly important and will be further developed, notably in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime.

Cyber incidents do not stop at borders in the interconnected digital economy and society. All actors, from NIS competent authorities, CERTs and law enforcement to industry, must take responsibility both nationally and at EU-level and work together to strengthen cyber security. As different legal frameworks and jurisdictions may be involved, a key challenge for the EU is to clarify the roles and responsibilities of the many actors involved.

To address cyber security in a comprehensive fashion, activities should span across three key pillars—NIS, law enforcement, and defence—which also operate within different legal frameworks:

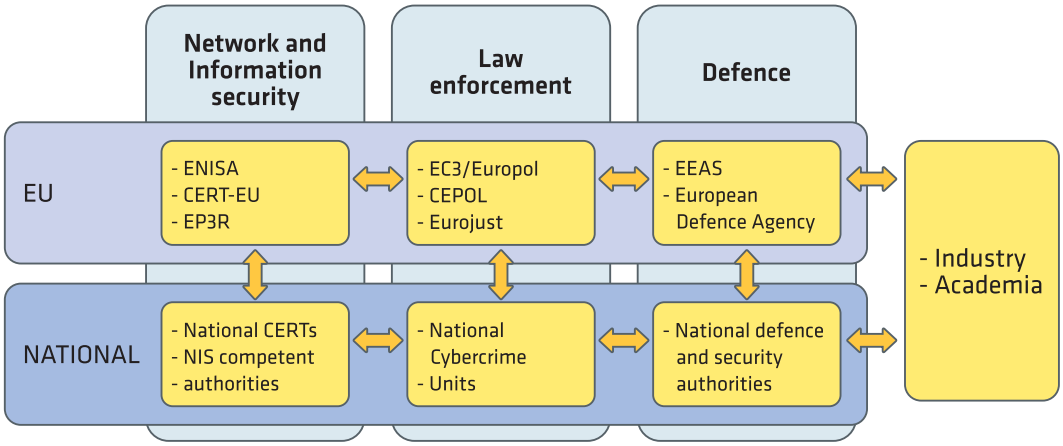

Figure 9: Roles and responsibility [29]

On national level Member States should have, either already today or as a result of this strategy, structures to deal with cyber resilience, cybercrime and defence; and they should reach the required level of capability to deal with cyber incidents.

On EU level coordination and collaboration will be encouraged among ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, risk assessment, training and sharing of best practices. They should collaborate while preserving their specificities. These agencies together with CERT-EU, the Commission and the Member States should support the development of a trusted community of technical and policy experts in this field.

The Commission, the High Representative and the Member States engage in policy dialogue with international partners and with international organisations such as Council of Europe, OECD, OSCE, NATO and UN.

4.3 Other international level cybersecurity strategies, best practices, frameworks

Table 5 identifies the organizations and entities referred to cyber security. A cursory look at this table indicates that the cyber security system is a complex assortment of national, international, and private organizations. Parallel to the organic fashion in which cyberspace itself developed, these organizations often have unclear mandates or possess overlapping spheres of influence. At this stage we seek only to highlight the major entities and, to the extent possible, to signal their relationships and interconnections.

Table 5: International Institutional Cyber Security System

Institution	Role
CERTs	
AP-CERT: Asia Pacific Computer Emergency Response Team	Asian regional coordination
CERT-CC: Computer Emergency Response Team - Coordination Centre	Coordination of global CERTs, especially national CERTs.
FIRST: Forum for Incident Response and Security Teams	Forum and information sharing for CERTs
National CERTs	National coordination; national defence & response
TF-CSIRT: Collaboration of Security Incident Response Teams	European regional coordination
International Entities	
CCDCOE: Cooperative Cyber Defence Centre of Excellence	Enhancing NATO's cyber defence capability
Council of Europe	International Legislation
European Union	Sponsors working parties, action plans, guidelines
ENISA: European Network and Information Security Agency	Awareness raising, cooperation between the public and private sectors, advising the EU on cyber security issues, data collection
G8: Subgroup on High Tech Crime	Sponsored 24/7 INTERPOL hotline, various policy guidelines
IMPACT: International Multilateral Partnership Against Cyber Threats	Global threat response centre, data analysis, real-time early warning system
INTERPOL: International Criminal Police Organization	Manages 24/7 hotline, trains law enforcement agencies, participates in investigations.

Institution	Role
ITU: International Telecommunications Union	Sponsors IMPACT. Organizes conferences, releases guidelines and toolkits, facilitates information exchange and cooperation.
NATO: North Atlantic Treaty Organization	Responding to military attacks on NATO member states
OECD: Organisation for Economic Co-operation and Development	Develops policy options, organizes conferences, publishes guidelines and best-practices.
UNODC: United Nations Office on Drugs & Crime	Promotion of legislation, training programs, awareness, enforcement
WSIS: World Summit on the Information Society	Global summit on information security; publishes resolutions and monitors implementation through stocktaking efforts.
National Entities	
CIA: Central Intelligence Agency	Defence of intelligence networks, information gathering
DHS: Department of Homeland Security	Protection of federal civil networks & critical infrastructure; information sharing and awareness; coordinating federal response and alerts.
DoD: Department of Defence	Defence of military networks, counterattack capability
DOJ: US Department of Justice	Federal Prosecution
FBI: Federal Bureau of Investigation	Federal Investigation
US-CERT: United States Computer Emergency Response Team	Defence of federal civil networks (.gov), information sharing and collaboration with private sector.

International Institutional Response

As defined by the CERT Coordination Centre (CERT/CC), these teams organize responses to security emergencies, promote the use of valid security technology, and ensure network continuity. In principle, this means that CERTs focus on identifying vulnerabilities and fostering communication between security vendors, users, and private organizations. Although the majority of CERTs were founded as non-profit organizations, many have transitioned towards public-private partnerships in recent years. This increasing level of integration with national governments represents an attempt to build upon the successes of non-profit CERTs by providing a level of structure and resources hitherto unavailable. At present, there are over 200 recognized CERTs, with widely different levels of organization, funding, and expertise.

At least three products are expected to result from CERT activities and interactions:

1. a reduction in unaddressed security vulnerabilities;
2. improved understanding of the nature and frequency of cyber threats; and
3. improved methods of communicating and reporting these threats to other security teams and the general public.

In addition to CERT/CC, many CERTS also interact with parallel coordination networks, such as the Forum of Incident Response and Security Teams (FIRST). This body was established to enhance information sharing between disparate security groups. Now composed of more than 200 organizations, FIRST is notable for its influential annual conferences and its extensive integration of national, academic, and private CERT teams.

Inter-Governmental Organizations

NATO. In a similar vein to IMPACT (IMPACT, 2009), a second major adaptive case is demonstrated by NATO. This intergovernmental organization established a technical response arm in the aftermath of the coordinated attacks on Estonia in 2007. Designated the Cooperative Cyber Defence Centre of Excellence (CCDCOE, 2009), the entity is responsible for training NATO member states, conducting attack exercises, and supporting NATO in the event of an international cyber-attack (CCDCOE, 2009). Interestingly, not all NATO states have joined the CCDCOE program, with many countries opting to rely on their own traditional military cyber defence networks. There is no strong evidence that all members of NATO are willing to engage in a common approach to a shared problem, presumably because many states are developing their own strategies for cyber warfare. At the same time, however, the CCDCOE fills an important void for several European states, notably those whose own cyber security capabilities are yet to be developed.

ENISA. Although the European Union has published numerous resolutions on cybercrime, and EUROPOL is actively engaged in investigation, the most important action which performed by EU's was the creation of the European Network and Information Security Agency (ENISA). The Agency's Mission is essential to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union.

ENISA is helping the European Commission, the Member States and the business community to address, respond and especially to prevent Network and Information Security problems.

5 Cybersecurity related practices of EU Countries

5.1 Austria

The ICT Security Strategy of Federal Republic of Austria was approved in 2013 in Vienna. The core objectives of ICT Security Strategy are critical information infrastructures (CII) and their protection. The strategy addresses a wide range of issues – from different aspects of creating ICT security knowledge and ICT security awareness to proactive and reactive cyber incident management. Strategic objectives and measures for implementation of the Austrian concept may be divided into five key areas: Stakeholders and Structures, Critical Infrastructures, Risk management and status quo, Education and research and Awareness [30].

Compared to previous strategies the new one has few differences [31]:

- traditional threats and challenges to security are becoming less imminent; new and more complex threats/challenges are becoming more important;
- the role of international organizations is growing, the role of state actors relatively declining;
- a comprehensive approach according to the principle of comparative advantages of the respective actors is needed on the international and regional levels;
- a more interactive and integrated approach (civilian/military) is needed on the domestic level (the so-called »whole of government approach«);
- Security increasingly also comprises economic, social, development and interior security aspects.

The National Security Strategy is a commitment to apply EU recommendation in crisis management, including the clause which requires Member States to improve their capabilities and make them available to the EU. It welcomes NATO's Strategic Concept of 2010, including NATO's increased ambitions in international crisis management, in cooperative security, in tackling new security challenges, and in the upgrading of its partnerships. According to the National Security Strategy, Austria is crafted its security policy mainly in the frameworks of the UN, the EU, the OSCE and NATO partnerships. It pledges continued Austrian cooperation within and with these organizations, and Austrian contributions to their respective endeavours. Participation in international crisis management missions/operations is understood as an essential element of this policy. Crisis prevention, mediation and the support of disarmament measures are further important elements [30].

Defence policy is defined as an integral part of the Comprehensive Security Provision, as being required to cooperate with internal security and foreign policies, and as comprising: the defence of sovereignty and territorial integrity; the protection of constitutional institutions and critical infrastructure; the protection of the population, including in case of natural disasters; a contribution to ensuring the functioning of the state institutions; the participation in international crisis management; and a contribution to the EU's security policy. Emerging security challenges can lead to new tasks for the Austrian armed forces and other official institutions and bodies [30].

The changes and advances in technology, in particular in IT technology, are not happening at a »bureaucratic« pace, but exponentially faster. One has only to mention inventions like Twitter, Facebook, Cloud Computing, and others. Risks and dangers involved are growing by the same speed as the innovations themselves. This puts Austrian government in a very difficult situation. Not only because state administrations are, more or less by definition, slower than innovative industries. But also because state action must (a) be based on a broad political consensus of, at least, the parliamentary majority, preferably though on that of a much wider societal majority; and (b) must – both in the process of its elaboration and in its contents – respect the fundamental principles of Austrian society, such as the rule of law, the separation of powers, the individual freedoms, etc.

It is obvious that no single ministry or even single government agency can fulfil these tasks alone. A »whole-of-government« approach or, indeed, a »whole-of-nation« approach involving also private stakeholders is required. Furthermore, no single country can successfully act just by itself. International cooperation becomes more and more pivotal, including with relevant international organizations that play an ever increasing role. This fact, by the way, is underlined in practically all recent doctrinal documents of states and international organizations.

The brief description of engagement of Austrian government in the cyber security area is given in the next few sentences. The well-developed national crisis response mechanisms and structures are being utilized to meet also new challenges such as cyber security. The coordination competence rests with the Federal Chancellery, which has established a government Computer Emergency Response Team (CERT) in 2008 in order to integrate cyber security efforts of the public and private sectors. The Federal Chancellery coordinates cyber crisis management with other government, CERT stakeholders and in consultation with experts from the Ministries of Interior and Defence. In 2010, the »Internet Offensive Austria« – a joint initiative of the ICT stakeholders of Austria (leading local ICT companies, research institutions and interest groups) – developed a national ICT strategy, the »Austria Internet Declaration«. Moreover, government has set up a Centre of Excellence for the Internet Society, which uses this Declaration as a comprehensive guideline for the future »whole-of-government« approach.

Austria has set up a Private Public Partnership Program for Critical Infrastructure Protection (APCIP) with the objective to develop a comprehensive strategy and detailed measures and to bring all relevant public and private organizations and infrastructure operators under one common conceptual roof.

The Defence Ministry is further developing its cyber defence capabilities by setting up a military CERT. The Interior Ministry has started to elaborate a Cyber Risk Matrix and Analysis, involving the academic, business, administration and political communities. The individual activities carried out by various ministries and agencies are consolidated by a national cyber security concept.

By this strategy it is planned to establish new bodies in order to enhance CS situation in Austria. The central contact for public cyber security matters will be created by establishing the position of a Chief Cyber Security Officer, who will be in close cooperation with the Chief Information Officer of the Federal Republic. *A Cyber Security Crisis Management* will consist of state representatives. Rules and procedures will have to be agreed upon to facilitate cooperation between public and private crisis centre. Crises management plans are adopted by Cyber Security Steering Group and define how crisis management bodies must deal with the most important cyber threats. *The Cyber Security Steering Group* is set up as the federal government's central advisory body for all matters involving Austria's CS. This body focuses on integrated approaches, strategies, crisis management, inter-governmental cooperation and

Austria's active participation in matters involving CS. It adopts Austria's comprehensive CS Strategy, monitors its implementation and takes corrective action if necessary. Organisational underpinning will be provided by the Board of Liaison Officers. *Information exchange centre of CS* will be institutionalised by launching CS Platform and serve as a central point of contact for all issues relating to ICT security and the key IC base concerning all awareness-raising measures for all target groups. A number of expert groups have already been established for various sectors, such as finance and health care. A number of research projects on cyber threats have been identified and started.

Establishment of a *Cyber Situation Centre* which will be responsible for tracking major cyber incidents in public administration, as well as for special crisis and disaster situations at national level. Services of the Austrian Federal Army will round off the activities of this body. In normal situation this body analyse network security in Austria and is responsible for simulations and reporting. Early warning is one of major tasks.

Austria has also been promoting the issue of cyber security in different international organizations. In OSCE, Austria is among a group of Participating States promoting cyber security issues within that organization. In particular, it advocates the development of Confidence and Security Building Measures (CSBMs) and training activities in field missions. In the Council of Europe, Austria holds the position of Thematic Coordinator on Information Policy Internet Governance, playing an important role in drafting the new Council of Europe Strategy on Internet Governance 2012.

5.2 Estonia

Estonia has embraced the concept of e-governance and built a fairly extensive national information infrastructure – the X-road data exchange solution, national ID-card, etc. On the one hand, this has given Estonian scientists, engineers and IT companies plenty of experience in researching and developing such solutions. For example, the X-road development by Cybernetica, or the time stamping solution developed by GuardTime. On the other hand, there are numerous services available for the citizen and the entrepreneur, including on-line tax-declaration, accessing national registries and even on-line voting. While this arguably gives Estonia a significant competitive advantage, it also creates a critical dependency from information systems. As a result, cyber security is considered a key component in protecting the Estonian way of life.

The Estonian Cyber Security Strategy was developed in the wake of the cyber-attacks against Estonian public and private entities in the spring of 2007. The Strategy was approved in 2008 with a scheduled update after five years. The updated version of the Strategy is expected to be published later in 2014. Since there is no public draft available of the latter, this section covers only the 2008 Strategy and the changes in the Estonian cyber security landscape that have occurred since the Strategy was adopted [32].

In Estonia, cyber security addresses the entire society. Although the lead actor for the 2008 Strategy drafting process was the Ministry of Defence, the document was prepared in a wider public-private working group with representatives from the Ministry of Economic Affairs and Communications, Ministry of Justice, Ministry of Education and Research, Ministry of Interior, the banking sector, the Internet Service Provider community, etc. While the drafting lead for the updated version has passed to Ministry of Communications and Economic Affairs, it is still prepared in close cooperation with relevant public and private actors. As a result, both

Strategies consider cyber security as something that covers the entire spectrum from citizen safety to Critical Information Infrastructure Protection (CIIP) [32].

The 2008 Strategy gives a brief overview of the drafting process and other Estonian policy documents that are related to the issue, such as the Estonian Information Society Strategy 2013. It then follows with two chapters that provide a general overview of threats in cyberspace and the current state of affairs in the fields that support cyber security in Estonia and in the international community. Chapter four outlines the goals and measures to improve the Estonian cyber security situation. The first focuses on developing a system of security measures that would address CIIP and organizational co-operation at the state level. The second addresses cyber security training, education and research, followed by goals on improving the legal framework, international co-operation and raising cyber security awareness throughout the society. While most of the goals are set for government entities, they address aspects of cyber security on the international, national, organizational and even personal level. For example, increasing awareness of all computer users and providing cyber security classes at all levels of education. The Strategy closes with a short note on implementation issues and an annex detailing the categories of critical infrastructure in Estonia [32].

Since 2008 there have been numerous changes in cyber security policy, law and organizational roles in Estonia. For example, the cyber security topic was included in the updated National Security Concept in 2010, the Penal Code was revised to address cyber-attacks against critical infrastructure, and the Emergency Act of 2009 – while general in nature – is also suitable to handle cyber emergencies [33].

One of the key actors in Estonian cyber security is the Estonian Information System Authority (EISA), which operates under the Ministry of Economic Affairs and Communications. EISA is tasked to handle most operational cyber security concerns of national relevance. It includes CERT Estonia, which manages cyber security incidents, as well as the CIIP department, which carries out risk assessments and develops security measures for vital service providers [34].

Estonia also hosts the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), an international military organization focusing on cyber defence consulting, research, education and lessons learned in support of NATO and NATO nations. While the preparation for establishing the Centre started as early as 2004, it was formally established in 2008. By February of 2014 the NATO CCD COE had eleven Sponsoring Nations. Examples of the NATO CCD COE products include the Tallinn Manual on the International Law Applicable to Cyber Warfare [35], the annual Conference on Cyber Conflict (CyCon) and the Locked Shields series of international cyber defence exercises [36].

Since the writing of the 2008 Strategy, there has been progress in cyber security education provided in Estonia. Most notably, an international Cyber Security Master's programme was started in 2009 jointly by Tallinn University of Technology and Tartu University. About half the students in the programme come from Estonia and the other half from the rest of the world. The programme is taught in English and includes instructors from the universities, as well as public and private sector entities. In addition, single courses or lectures are included in various study programmes, but there is much room for improvement in reaching the general student community [37].

Another noteworthy actor in the Estonian cyber security landscape is the so called Cyber Defence League, or the Cyber Defence Unit (CDU) of the Estonian Defence League. The Defence League (DL) is a volunteer national defence organization that is part of the military chain of command. In 2009, a grass roots initiative led to formation of first cyber defence sub-units in the conventional DL structure, uniting people who are willing to participate in national (cyber) defence out of their free time. It should be noted that the volunteer members

of the CDU do not receive a salary for their service. In 2011 the cyber defence sub-units were re-formed as the CDU. The CDU volunteers have organized and participated in various national and international cyber defence exercises [38], [39].

5.3 Finland

Finnish society has embraced the opportunities provided by information technology, in terms of personal interactions, business, e-governance, and more. However, as an information society, Finland must also consider and manage the risks that are associated with increased reliance on the cyber domain. This realization led to the development of Finland's Cyber Security Strategy, which was published in 2013. Due to its recent adoption, there has not been a lot of time for implementing the Strategy. Therefore, this section is primarily focused on the goals set in the document itself [40].

The vision offered in the Strategy is that [40]:

- »Finland can secure its vital functions against cyber threats in all situations.« This indicates that Finland considers cyber security in a broad manner, covering the entire threat spectrum.
- »Citizens, the authorities and businesses can effectively utilise a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally.« The second component of the vision further broadens the area of interest, which is in stark contrast with the approach of some other strategies that see cyber security as a military/government issue.
- »By 2016, Finland will be a global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats.« While difficult to achieve or measure, this statement provides an ambitious goal that is designed to inspire Finnish actors to improve the cyber security situation as much as possible in the coming years.

The Strategy proceeds with an overview of the cyber security management in Finland and the eight principles that support it. The first principle designates the Government as the default actor in cyber security and notes that each ministry is responsible for the cyber security in its sector. The second principle ties cyber security to the comprehensive security of society and the corresponding Security Strategy for Society. The third identifies the need for information security arrangements throughout the society. The fourth identifies the need for a 24/7 Cyber Security Centre that would coordinate information collection, analysis and sharing of the common situation picture. The fifth specifies that while the division of responsibilities exists and is regulated, the actors in cyber security should remain as flexible as possible in their activities. The sixth explains the need to participate in the international cyber security activities, in order to strengthen national expertise and the foundations of the information society. The seventh identifies the need to invest in cyber security education, research and development, in order to become a lead nation in this field. The last principle is that know-how is generated through business, and therefore Finland should provide the regulatory framework and incentives to support cyber security business [40].

After the principles, the Strategy defines ten strategic guidelines that will help in turning the vision into reality [40]:

- »Create an efficient collaborative model between the authorities and other actors for the purpose of advancing national cyber security and cyber defence.« This guideline addresses the need to share information and best practices and specifically promotes

the use of (international) exercises to improve the situation awareness of the various actors.

- »Improve comprehensive cyber security situation awareness among the key actors that participate in securing the vital functions of society.« The guideline identifies the need for the Cyber Security Centre, which would collect (in real time) and analyse relevant data and share the resulting situation picture with other actors.
- »Maintain and improve the abilities of business and organizations critical to the vital functions of society as regards detecting and repelling cyber threats and disturbances that jeopardise any vital function and their recovery capabilities as part of the continuity management of the business community.« The vital service providers are required to plan their defences so that they could remain operational even during cyber-attacks.
- »Make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime.« This includes providing input to, and receiving the cyber situation picture from the Cyber Security Centre mentioned in guideline two, as well as resourcing and organizational questions that need to be solved to maintain a well-trained, motivated and properly equipped police force that is able to handle cybercrime investigations.
- »The Finnish Defence Forces will create a comprehensive cyber defence capability for their statutory tasks.« Unlike many other states, the Finnish strategy clearly indicates that the Defence Forces cyber mission has a defensive, offensive and intelligence gathering component, which would be used in conjunction with other capabilities within the confines of the legal framework.
- »Strengthen national cyber security through active and efficient participation in the activities of international organisations and collaborative fora that are critical to cyber security.« Specifically, the Strategy mentions EU, UN, OSCE, NATO and OECD as some of the key organizations that Finland should work with.
- »Improve the cyber expertise and awareness of all societal actors.« Beyond individuals, the Strategy also identifies businesses and NGO's that provide vital services as key actors to focus on. This guideline also encompasses the establishment of a new centre of excellence in cyber security, which would facilitate top level research and lead to the establishment of a national cyber security cluster.
- »Secure the preconditions for the implementation of effective cyber security measures through national legislation.« The existing law needs to be reviewed and updated, while ensuring a balance between security (such as the need to collect certain data) on one hand and the personal liberties and favourable business climate on the other hand.
- »Assign cyber security related tasks, service models and common cyber security management standards to the authorities and actors in the business community.« Government entities need to identify the role assignment between government and private actors.
- »The implementation of the Strategy and its completion will be monitored.« The last guideline details the actors responsible for monitoring the fulfilment of the Strategy.

Since the Strategy was adopted in 2013, there have been some concrete changes in the Finnish cyber security situation. Most notably, the Cyber Security Centre (discussed in the fourth principle and the second guideline) was formed on January 1st 2014, primarily based on the existing CERT-FI. The Centre provides a situation picture based on collected and reported data, as well as vulnerability coordination services [41].

In 2013 the Ministry of Employment and the Economy selected five key focus areas to accelerate business and innovation in Finland, and assigned a lead city for each area. One of

the five was cyber security, which was assigned to the city of Jyväskylä. This city is home to Jyväskylä University and Jyväskylä University of Applied Sciences, both of which provide cyber security education. However, cyber security research and education is also available elsewhere in Finland [42].

On the private side, perhaps the best known cyber security actor in Finland is F-Secure, providing an array of cyber security solutions to customers world-wide. However, there are also a number of smaller companies offering state of the art solutions for narrower problem spaces. The Strategy aims to increase their number and success rate by providing incentives and opportunities through a business friendly infrastructure.

5.4 France

Cyberspace, like a virtual battleground, has become a place for confrontation: appropriation of personal data, espionage of the scientific, economic and commercial assets of companies which fall victim to competitors or foreign powers, disruption of services necessary for the proper functioning of the economy and daily life, compromise of information related to sovereignty and even, in certain circumstances, loss of human lives are nowadays the potential or actual consequences of the overlap between the digital world and human activity.

Given the sudden emergence of cyberspace in the field of national security and the extent of the challenges ahead, the French government decided to provide France with a structured defence and security capability [43].

Cyber Security Strategy of France:

- Become a cyber-defence world power in cyber defence;
- Safeguard France's ability to make decisions through the protection of information related to its sovereignty;
- Strengthen the cybersecurity of critical national infrastructures;
- Ensure security in cyberspace.

Seven areas of action:

- Anticipate and analyse;
- Detect, alert and respond;
- Enhance and perpetuate our scientific, technical, industrial and human capabilities
- Protect the information systems of the State and the operators of critical infrastructures;
- Adapt French legislation;
- Develop the international collaborations;
- Communicate to inform and convince.

Become a world power in cyber defence

While maintaining the strategic independence, France has worked to ensure that it belongs to the inner circle of leading nations in the area of cyber defence. Then it will benefit from the knock-on effect of cooperation both at an operational level and in the implementation of a unified strategy to face common threats [43].

Safeguard France's ability to make decisions through the protection of information related to its sovereignty

Governmental authorities and crisis management actors must have the resources to communicate in any situation and in total confidentiality. The networks that meet this need must be expanded, particularly at the local level.

Ensuring the confidentiality of the information circulating over these networks requires mastered security products. We must keep the necessary expertise to design them and optimise their development and production methods [43].

Strengthen the cybersecurity of critical national infrastructures

To function correctly, French society is increasingly dependent on information systems and networks, particularly the Internet. A successful attack on a French critical information system or the Internet could have serious human or economic consequences. In close collaboration with the relevant equipment manufacturers and operators, the State must work to guarantee and improve the security of these critical systems [43].

Ensure security in cyberspace

The threats to information systems simultaneously affect public services, private companies and citizens. Public services must operate in an exemplary fashion and improve the protection of their information systems and the data entrusted to them. Simultaneously, campaigns to raise information and awareness among companies and citizens must be undertaken. In terms of the fight against cybercrime, France promotes the strengthening of the current legislation and international judicial cooperation.

In order to meet these objectives, seven areas of action have been identified [43]:

1. Effectively anticipate and analyse the environment in order to make appropriate decisions.
2. Detect and block attacks, alert and support potential victims.
3. Enhance and perpetuate our scientific, technical, industrial and human capabilities in order to maintain our independence.
4. Protect the information systems of the State and the operators of critical infrastructures to ensure better national resilience.
5. Adapt French legislation to incorporate technological developments and new practices.
6. Develop international collaboration initiatives in the areas of information systems security, cyber defence and fight against cybercrime in order to better protect national information systems.
7. Communicate, inform and convince to increase the understanding by the French population of the extent of the challenges related to information systems security.

France's national cyber security protection system

As part of the reinforcement of cyber defence capabilities at the Ministry of Defence, the post of Cyber Defence General Officer was created in 2011, with responsibility for coordinating the Ministry's cyber defence activities and acting as the main interface in the event of a cyber-crisis [44].

National-level bodies and institutions to cybersecurity in France

The main authority for cyber defence is the French Network and Information Security Agency, established in 2009. Its missions include detecting and reacting to cyber-attack, mitigating cyber threats by supporting research and development, and providing information to government and critical infrastructure entities. It operates under the Prime Minister and is part of the General Secretariat for National Defence. In February 2011, the Agency released the official French cyber doctrine. France's four objectives in cyberspace are to become a global power in cyber defence, guarantee information sovereignty and freedom of decision, secure critical infrastructure, and maintain privacy in cyberspace [44].

France is also developing an offensive cyberwar capability under the purview of the Joint Staff and specialized services [45]. Both the army and the air force have electronic warfare units. Offensive capabilities are also being pursued by the intelligence services [45]. The Analysis and Combat Centre for Cyber Defence coordinates with the Network and Information Security Agency and other agencies to monitor military networks and respond to intrusions [46]. In addition, the Directorate for Defence Protection and Security is an intelligence agency within the Ministry of Defence that ensures the military's operational capacity by providing information about potential threats and vulnerabilities. It protects against the threats of espionage, sabotage, subversion, organized crime, and terrorism. The Directorate increasingly focuses on communicating cyber threats and vulnerabilities to network operators in the military and the defence industry in order to improve cybersecurity.

5.5 Germany

Cyber security plays an important role in Germany. The best indicator is the Federal office for Information Security BSI [47] which was established in 2005 and since then is the key institution in Germany regarding all matters of cyber security. The BSI investigates security risks associated with the use of IT, develops preventive security measures, provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions. The role of the BSI is similar to the role of CERTs (Computer Emergency Response Teams), but wider. Additionally, the BSI also works in the field of IT security testing and assessment and co-operates with industry. The target groups of BSI are: manufacturers, distributors and users of information technology. It also analyses development and trends in information technology. The BSI was also involved in the development of Germany's cybersecurity strategy and was the initiator of Germany's Cybersecurity Alliance (Ger. Die Allianz für Cyber-Sicherheit) [48]. The BSI also publishes best practices from the field of cybersecurity. An example is the best practices for industry computer peripherals (Ger. Anforderungen an netzwerkfähige Industriekomponenten) [48]. In scope of the cybersecurity alliance additional best practices have been published (e.g. Best practices for protection against DDOS attacks) [49].

Germany's Cybersecurity Alliance plays the role of the union of all key stakeholders in the field of cyber security in Germany. Its goals are to increase Germany's cybersecurity and to strengthen Germany's resilience against cyber-attacks. In order to achieve these objectives the alliance conducts the following actions/measures:

- Creates and maintains the state-of-the-art regarding cybersecurity;
- Provides in-depth background information resilience measure related to cybersecurity attacks;
- Intensifies the exchange of experience on cyber security;

- Development of cybersecurity competences in organizations with intensive use of IT

Therefore the alliance develops and maintains a large knowledgebase and initiates and promotes interest groups in different field of cyber-security, initiates and operates experience and expert circles for cyber security. This portfolio is further complemented by contributions of partners in the form of trainings and free availability certain security products of partners [50].

Germany's cyber security strategy mainly focuses on civilian approaches and measures, but is complemented by measure of the German army. The strategy focuses on ten strategic areas [51]:

1. *Protection of critical information infrastructures*
   The main priority of the cybersecurity strategy is the protection of the critical information infrastructure (CIP). The public and private sector have to establish good coordination. The Nation Cyber Security Council should participate in achieve goals for protecting CIP. Whether and where protective measures and additional powers are required has to be defined.
2. *Secure IT systems in Germany*
   The aim is to make information of security of IT systems available to citizens and SMEs (Small and medium enterprises). Those goals can be achieved through awareness rising, training and through availability of more secure products and services. Different initiatives, funds and task force will have to be established (e.g. task force on »IT security in industry«).
3. *Strengthening IT security in the public administration*
   The public administration and state authorities will have to enhance the security of IT systems and in such a way act as a role model. This would be achieved through a common, uniform and secure network infrastructure in the federal administration. The measure will be taken on federal level as well as on »Länder« level. In this context CERTs will have to intensify cooperation.
4. *National Cyber Response Centre (NCRC)*
   A National Cyber Response Centre (NCRC) which reports to the Federal Office for Information Security (BSI) will be set up. It will cooperate with other stakeholders, like the Federal Office for the Protection of the Constitution (BfV) and the Federal Office of Civil Protection and Disaster Assistance (BBK). The Federal Criminal Police Office (BKA), the Federal Police (BPOL), the Customs Criminological Office (ZKA), the Federal Intelligence Service (BND), the Bundeswehr and authorities supervising critical infrastructure operators all participate in this centre within the framework of their statutory tasks and powers.
   The main objectives of the NCRC would be to share information on vulnerabilities, weaknesses and other cybersecurity related threats and to take appropriate actions. The NCRC will submit recommendations to the National Cyber Security Council both on a regular basis and for specific incidents and in cases of imminent or already occurred crisis will inform a crisis management staff headed by the responsible State Secretary at the Federal Ministry of the Interior.
5. *National Cyber Security Council (NCSC)*
   A National Cyber Security Council (NCSC) has to be set up to facilitate collaboration between the public and private sector. Several federal institution will participate in the council: The Federal Chancellery and a State Secretary from each the Federal Foreign Office, the Federal Ministry of the Interior, the Federal Ministry of Defence, the Federal Ministry for Economics and Technology, the Federal Ministry of Justice, the Federal Ministry of Finance, the Federal Ministry of Education and Research and 6 representatives of the federal Länder. On specific occasions additional ministries will be included.

Business representatives will be invited as associated members. The objective of the council is to coordinate preventive tools and the interdisciplinary cyber security approaches of the public and the private sector. The NCSC will complement and interlink IT management at federal level and the work of the IT Planning Council in the area of cyber security at a political and strategic level.

6. *Effective crime control also in cyberspace*
   The capabilities of law enforcement agencies must be strengthened. To improve the exchange of know-how in this area the intention is to set up joint institutions with industry with the participation of the competent law enforcement agencies. Projects to support partner countries with structural weaknesses will also serve the aim of combating cybercrime. To face up to the growing challenges of global cybercrime activities a major effort will be made to achieve global harmonization in criminal law based on the Council of Europe Cyber Crime Convention. Furthermore, will be examined the necessity of additional conventions in this area at UN level.
7. *Effective coordinated action to ensure cyber security in Europe and worldwide*
   The aim is to shape Germany's external cyber policy in such a way that German interests and ideas concerning cyber security are coordinated and pursued in international organizations, such as the United Nations, the OSCE, the Council of Europe, the OECD and NATO. In this sense at the European level (e.g. ENISA) and other international bodies / institutions / organizations should coordinate their efforts regarding cybersecurity.
8. *Use of reliable and trustworthy information technology*
   The availability of reliable IT systems and components must be ensured on a permanent basis. The development of innovative protection plans for improved security which take into account social and economic aspects is strongly supported. Research on IT security and on critical infrastructure protection has to continue and should be intensified. The entire range of core strategic IT competences should be included in political strategies. The resources should be pooled with partners and allies, particularly in Europe. The aim is to use components in critical security areas which are certified against an international recognized certification standard.
9. *Personnel development in federal authorities*
   Whether additional staff is necessary in authorities in the interest of cyber security must be examined as a priority. Personnel exchange between federal authorities and appropriate further training measures must be intensified.
10. *Tools to respond to cyber-attacks*
    To tackle cybersecurity threats appropriate tools have to be created. This will be achieved through regular assessment of threats and taking appropriate protection measures. If necessary, we have to examine whether additional statutory powers must be created at federal or Länder level.

Due to the fact that information technologies used are subject to short innovation cycles, German's cyber security strategy will be regularly reviewed whether the aims have been achieved. The key role is delegated to the National Cyber Security Council.

5.6 Italy

Cybersecurity was recognized a matter of national security in Italy for the first time in the 2010 Italian annual report of the »Information System for the Security of the Republic«. The 2012 annual report highlighted how new technologies make cybersecurity threats »able to have a profound effect on the continuity of functions and vital interests of the country« (www.sicurezzanazionale.gov.it).

A 2008 decree of the Minister for the Interior identified critical IT infrastructures as all system and computer services supporting the institutional functions of:

1. Ministries, agencies and supervised authorities, operating in the fields of international relations, security, justice, defence, finance, communications, transport, energy, environment, health;
2. Bank of Italy and independent authorities;
3. State-owned companies, regions and metropolitan areas covering at least 500.000 people, operating in the fields of communications, transport, energy, health and water conservation;
4. Any other institution, administrative office, authority, public or private legal person whose business is considered of national interest because of public order or security [52].

In 2012, the most targeted sectors by cyber-crime were the government, political organizations and industry. The number of Italians connected to the Internet was 33 million (+8.3% from 2011). However, only 33% of Italian users utilize data security specific software (vs. 44% on a global scale), and only 45% employ privacy settings to control personal information flow. 44% (vs. 40% worldly) do not follow standard directives about passwords security, using weak and/or never changing keywords [53]. This naive approach to Internet security has a cost: approx. 44% of PCs in Italy are attacked by malware while browsing the Internet (compared to 20% in Denmark, for example), and cybercrime made approx. 8.9 million victims in 2012, for a total cost of 85 billion € (275€ per person, which is higher than global average of 144€) [54]. From a recent survey [52] among employees of 68 organizations of the Public Administration (PA), public utilities, financial, and industrial sector, emerged that institutions are not very prepared as well. PA only implements employee training, and information classification/access control policies. On the other hand, financial and industrial institutions focus on restricting the use of personal emails, cloud services, and personal devices. Organizations do not seem to realize that such security measures should be used altogether. Almost all the respondents felt the necessity to improve the training, suggesting lack of self-confidence concerning security competences. Concerning attacks detection and response, only 29% reputed their IT infrastructure able to detect Advanced Persistent Threats. Half of the respondents admitted not to test their web applications for security (at least not using standard and well established methodologies). More generally, only 80% of the participants actively test their systems (47% relying on external companies). Finally, 25% of the PA respondents admitted not to have the capabilities to respond to a cybersecurity incident. More generally, the ability to fix incidents often relies on external resources.

From a Governance and Legislative point of view, Italy presents a gap with respect to the most developed countries of the EU, which it has been trying to fill in the last 15 years.

In 1999, a working group composed of representatives from the Ministries of Communications, Justice and Interior was conceived, whose task was to support administrative and regulatory interventions for NIS. In 2003 such group became the Permanent Observatory for Network and Communications Protection and Security (OPSTRC), within the Ministry of Economic Development. OPSTRC, which involves representatives of the Ministries of Defence and of Productive Activities, and the Departments of Public Service and of Innovation and Technology, significantly helped translating the EU Directive 2002/58/EC into facts.

In 2008, the Ministry of the Interior established a special unit within the Italian Postal and Communication Police Service called National Anti-Cybercrime Centre for the Protection of Critical Infrastructure (CNAIPIC). CNAIPIC is active 24/7 and comprises both an operational and a technical department. Its purpose is to intervene to prevent and fight cyber-attacks, cybercrime, and industrial espionage, threatening infrastructures operating in sensible

sectors (e.g., health care, transport, telecommunications and energy). The Unit of Cybercrime Analysis was created as part of CNAIPIC, to study and analyse the phenomenon of cybercrime in partnership with major Italian Universities.

In 2009, according to EU Directive 114/2008, the Inter-Ministerial Coordination for Critical Infrastructure Protection was established within the Italian Presidency of the Council of Ministers. Its scope was to enforce coordination, coherence and synergy between the initiatives and activities of the authorities concerned with the protection of critical infrastructures. The crisis management system was instead reorganized in 2010 by a decree of the President of the Council of Ministers, which established the Organization for Crisis Management. Two new bodies were introduced: the Politic Strategic Committee (CoPS), permanent and appointed of strategic guidance of crisis, and the Inter-Ministerial Unit for Situation and Planning (NISP), tasked to support CoPS in monitoring the national and international security situation to foresee and prevent possible crisis. Along this line, in 2011 the European Directive on Critical Infrastructures was transposed in Italy into Legislative Decree 61/2011. It establishes that any infrastructure's operator, with the support of NISP and of several Ministries, must draw up an Operator Security Plan, to identify assets and existing solutions for their protection.

In the last years fundamental improvements of the digitalization of Italy was made. In 2012, the Italian Digital Agenda (ADI) was approved, as part of a decree covering development and infrastructure investments. ADI addresses open data, digital identities, electronic health records, electronic student records and measures to make the judicial system more efficient by increasing the use of electronic communication and online notifications. ADI stresses the importance of investment in infrastructure aimed at improved access to faster network for the population, and the need to ensure safety and reliability of such infrastructure through threats detection and contrast tools, public-private cooperation, and enhanced mechanisms for incident response. ADI paved the way to a re-engineering of the Italian PA system: a few months after ADI, Law n.147 established the Agency for Digital Italy DigitPA, responsible for the digitalization of the PA [52].

Law n. 133/2012 started to delineate a more precise strategy for national cybersecurity, attributing new and more detailed responsibility to the Italian intelligence system. In particular, the Prime Minister was given the faculty to issue directives to the Intelligence and Security Department (DIS), after prior consultation with the Inter-Ministerial Committee for Security of the Republic (CISR), in order to strengthen security intelligence activities when necessary. Along this line, the President of Council of Ministries' Decree 24 January 2013 responded to the requirement of a national strategic framework comprising mechanisms to reduce vulnerability, improve risk prevention, provide timely response to attacks, and permit immediate restoration of the functionality of the system in the event of crisis. The decree identifies CISR as the entity that shall:

1. implement the national plan for cyberspace security;
2. plan the detailed activities required to achieve this aim;
3. promote the collaboration among institutional bodies and private market players operating in the national cybersecurity field.

The CISR is assisted in achieving these tasks by DIS, and the Agencies for the Internal and External Information and Security.

To handle cyber risks or incidents, the Cybersecurity Team (NSC) was established to plan and coordinate the response to cyber-attacks and restore the networks and systems functionality. NSC is also responsible for interacting with correspondent bodies appointed by other nations or international organizations, such as EU, NATO, and UN. Responses planned by NSC are implemented by the Inter-Departmental Board of Cybernetic Crisis and, as far as network and

technical aspects are concerned, by the national CERT. Finally, the decree prescribes that Italian private market players (i.e., those supplying information services and the operators of critical infrastructures, both at national and European levels), must notify the NSC of all relevant violations of their networks and adopt specific »best practices« to achieve cybersecurity [55].

5.7 Slovenia

Slovenia has not yet published its cybersecurity strategy and the development process in its earlier stage. The key institution responsible for the national cybersecurity strategy is the Ministry of Educations, Science and Sport.

However, there are normative regulations related to cybersecurity: in compliance with the European directive 2009/140/EC [56], Slovenian communication act (Zakona o elektronskih komunikacijah (ZEKom-1, Ur. l. RS, št. 109/2012) was amended. The new act enforces the management of threats for protection of networks and services and delegated this responsibility to the communication service providers (CSP). The CSPs are also obliged to report any security incidents to the Slovene Agency for communications networks and services (slo. Agencija za komunikacijska omrežja in storitve - AKOS). Based on the seriousness of the incident AKOS can delegate any other activities to the Slovenian Computer Emergency Response Team (SI-CERT).

Some best practices are already included in Slovenia, but the general cyber-security situation including the strategy remains unregulated.

5.8 Spain

In Spain, cybersecurity is currently established as a priority national security objective that is necessary to guarantee the development of strategic economic sectors. To this end, since 2005, several measures have been adopted to ensure a general legal and institutional framework for cybersecurity matters [55].

The first step was towards eGovernment: reduce bureaucracy, simplify procedures and eliminate unjustified delays relying on new technologies. Two plans, »Avanza« (2005) and »Avanza2« (2009) were conceived by the Ministry of Industry, Tourism and Trade (in close cooperation with the Ministry of Territorial Policy and Public Administration, the Autonomous Communities and the Local Governments), to:

1. ensure a wider use of ICTs among households and citizens;
2. enhance the adoption of technologically advanced solutions in Small and Medium Enterprises (SMEs), encouraging and funding the development of new ICT products, processes, applications, contents and services;
3. incorporate ICTs in the education and training process, massively including both citizens and companies, in particular SMEs and their employees;
4. enable new, user-friendly and better public eServices, and Public Administration (PA);
5. deploy a broadband infrastructure, so as to connect the entire country, generate citizens and businesses' confidence in the use of new technologies, provide advanced security mechanisms and promote the creation of new digital content;

6. increase ICT security, so as to foster citizens' and businesses' trust in ICT and improve the accessibility of eServices. The report »Avanza2 plan - 2011-2015 Strategy« further extended »Avanza2«, adding demand for:
7. spreading ICT in healthcare and for the welfare;
8. modernizing the education and training model through the use of ICT;
9. strengthening the digital content sector and intellectual property rights in the current technological context and within the Spanish and European legal framework;
10. developing green ICTs [57].

Three public organizations are mainly responsible for Network and Information Security (NIS) in Spain: The Ministry of Industry, Tourism and Trade (MITYC), the Ministry of Interior (MI), and the National Cryptologic Centre (CCN).

MITYC, in particular the Secretary of Telecommunications and Information Society (SETSI), is appointed to delineate government policy in the area of electronic communications networks and services, and the Information Society.

MI has overall responsibility for critical infrastructure protection (CIP/CIIP). Within MI, the Secretary of Security (SES) is responsible for development of the National Critical Infrastructure Protection Plan.

CCN is responsible for ensuring the security of the information technologies in all areas, for keeping informed concerning the coordinated acquisition of cryptologic material, and for providing training for PA resources that specialise in this field.

On the private side, NIS is primarily enforced by CNCCS and eSEC.

CNCCS is a private council bringing together the 17 Spanish industry leaders in Computer Security. The objectives of CNCCS are primarily to protect consumer identity, Critical Infrastructure, and corporate information, and to help the government structure to create a national legislation to combat cyber-crime.

eSEC, created by the Association of Enterprises of Electronics, Technologies, Information, Telecommunications and Digital Contents (AMETIC), is a network for scientific and technological cooperation that brings together companies and research institutes focused on technologies for the improvement of security and trust in the Information Society ([58].

Notwithstanding the efforts of both public and private organizations, »Information Society« reports carried out within the »Avanza« and »Avanza2« proved that training and awareness in computer security matters still need to be increased in both citizens and enterprises. Since 2009, the National Institute of Communication Technologies (INTECO) raised as a public initiative to improve the cybersecurity readiness of Spain, through cooperation with the CERT, the National Security Helpdesk for Citizens, and the Information Security Observatory. During 2009 and 2010 INTECO developed two awareness campaigns, one focused on citizens (which reached nearly 16.000 citizens in 2010), and the other on SMEs (which reached nearly 2.000 SMEs). The purpose was to make SMEs and citizens aware of the significance of considering and properly tackling the aspects related to computer security and communication networks.

INTECO provided best practices, recommendations, security bulletins and alerts, vulnerabilities management service, precautions guides and security tools in order to improve security. It developed a Catalogue of ICT Security companies and Solutions to help training, prevention and reaction tools & services against incidents in information security matters. INTECO indeed acts as a link between SMEs and citizens and companies of the Information Technologies security sector. It provides security studies, indicators of spam, eFraud, security levels at households and SMEs, information and indicators about vulnerabilities, alerts and

advice on new threats targeted at Information Systems, compiled from different renowned and prestigious companies [57].

The Royal Decree 3/2010 regulated the National Security Framework (ENS) foreseen in the article 42 of Spain's Law on Citizens' Electronic Access to Public Services (Law 11/2007, or 'Law on eGovernment') (Spanish Council of Ministers). The ENS introduces the common elements to guide the activity of PA in relation to security and the common language that will facilitate the interaction among public administrations as well as the communication of security requirements to the ICT Industry. In order to create such conditions, the ENS sets out the security policy to be applied by all PAs in Spain for the use of electronic means in the frame of eGovernment. The ENS establishes basic principles and minimum requirements for information security, provides the procedure to fulfil them and to respond to security incidents, and prescribes regular security audits. The ENS further recognizes the role of certified products in the fulfilment of the minimum security requirements, the relationship with the Certification Body of the National Evaluation and Certification Scheme.

On February 15 2013, the government approved the Digital Agenda for Spain as the reference framework for creating a roadmap to finally establish Spain's strategy for achieving the objectives of the Digital Agenda for Europe. Concerning cybersecurity, the recently approved »Trust Plan in the Digital Field« establishes the implementation of European regulations, including the Policy for the Networking and Information Security, the Regulations for Electronic Identity and Trust Services, and the Regulations for Protection of Personal Data. On May 31, the Council of Ministers approved the 2013 National Security Strategy that conceives national security in a more comprehensive and global manner, extending the traditional concept of national security (which was restricted to defence and public safety) to new parties of the private sector and to new threats, including cyber threats. The 2013 Strategy prescribes that:

1. INTECO is the central body to manage and oversee the development of the measures to be adopted in matters of Spanish cybersecurity;
2. Royal Decree 3/2010 (which only covers the PA) must be extended to cover all public and private sectors, in particular critical infrastructures, companies, and citizens;
3. fully developed General National Cybersecurity rules are needed soon, and must take into consideration the Law 15/99 of December 13 of Protection of Personal Data and General Telecommunications Law, the Law of the Information Society and Electronic Commerce, and the Spanish Penal Code;
4. actions to strengthen public–private collaboration and the security and reliability of the networks, products, and services used by ICT employees in the industrial sector are necessary;
5. promoting the training of professionals in cybersecurity and the implementation of a solid cybersecurity culture, and motivating Spanish industry through a research and development plan, is of primary importance;
6. international collaboration is fundamental to achieve a safe international cyberspace.

Finally, on July 15, the Secretary of State for Telecommunications and the Information Society anticipated that the Government wanted, »before the year-end« a National Cybersecurity Strategy that allows [55]:

1. identification of the potential threats;
2. determination of how to respond to these threats;
3. coordination between Administrations and companies for the adoption of measures; and
4. definition of an organization that has »national reference centres« and an »increased coordination« among all companies, Administrations, and States.

5.9 Sweden

Israel, Finland and Sweden are judged to be the nations which are most resilient to cyber-attacks on their public and private computer systems, according to an in-depth study into cybersecurity published on January 30, 2012 by a Brussels-based think–tank.

Sweden developed a 'Strategy to improve Internet security in Sweden' [59]. The National Post and Telecom Agency (PTS) has been assigned by the Government to submit proposals on a strategy to improve Internet security in Sweden. The aim of the strategy is to facilitate and clarify future work to secure Internet infrastructure.

In the past years, the Government's overall information technology (IT) policy objective is for Sweden to become the first country to create an information society for all. Future efforts in the IT sector are described in an action plan identifying the measures required. Tax relief is proposed as a means of encouraging access to the broadband network. Government funding is also to be made available for the establishment of regional networks and for the purpose of facilitating access to the broadband network in sparsely-populated areas. In addition, the Swedish National Grid is to undertake the construction of a backbone network on strictly commercial terms.

Swedish Government established Government Bill titled 'From an IT policy for society to a policy for the information society' [60]. The goal of the Government was: 'Sweden must be sustainable information society for all'. To this end, related to cyber security issues, the following initiatives and activities are defined:

- A strategy for a more secure Internet in Sweden should be to prevent large-scale disruptions or breakdowns that make it difficult or impossible for large groups of individuals or important companies, public agencies and organisations to use the Internet;
- Internet users should be made aware of the risks they are exposing themselves to and how to minimise them;
- The Government has commissioned the Swedish Emergency Management Agency to develop an Internet-based information system for the actors in the emergency management system;
- The Government wants to try to obtain a wider circle of users for the RAKEL radio communication system (for protection and security purposes).

In Sweden, many organisations are aimed on addressing cyber security organisational, technical and research issues, as follows:

1. *Swedish Defence Research Agency (Totalförsvarets forskningsinstitut, FOI)*

FOI is a Swedish government agency for defence research that reports to the Ministry of Defence. Their activities in the field of IT security stem from deep technical considerations of vital importance to the security of computer based systems, from social aspects and from security principles at system level. The combination of these three points of departure paves the way for results that are based both on insight into the possibilities of technology and the capabilities of users and organisations as well as an understanding of the system and the needs of the customer.

2. *The Internet Infrastructure Foundation (II Foundation or IIS)*

The II Foundation has two main functions: first, to manage and develop the Internet's Swedish top-level domain, .se; second, to promote the development of the Internet infrastructure in Sweden. The II Foundation was founded in 1997 on the initiative of ISOC-SE for this purpose, as the .se domain had started to grow more and more rapidly and needed a stable organisation that could take long-term responsibility. At the same time, the Foundation launched the wholly-owned operations company NIC-SE to look after the daily operational and administrative management of .se. There was a reorganisation in 2006 when NIC-SE was dissolved as a private company and in conjunction with this the II Foundation took over the operational management of the .se domain. Since 2004, the II Foundation has been annually giving out grants to selected natural or legal persons in order to promote initiatives within Internet security and development and support projects that do not normally receive money from research councils, research foundations and other research funding bodies.

3. The Industry Security Delegation of the Confederation of Swedish Enterprise

The Industry Security Delegation (NSD) is a forum for the exchange of ideas, experience and knowledge for issues relating to security. This is to promote better security and risk awareness in business and among the public. Work within the NSD aims to encourage risks being assumed on a well-informed basis through the exchange of experiences, increased knowledge, continuous awareness of reality and contacts with stakeholders within the field of security

5.10 UK

As the UK's dependence on cyber space grows, so the security of cyber space becomes ever more critical to the health of the nation. Cyber space cuts across almost all of the threats and drivers outlined in the National Security Strategy [3]: it affects all people, it reaches across international borders, it is largely anonymous, and the technology that underpins it continues to develop at a rapid pace.

Cyber Security Strategy of the United Kingdom

The Strategy highlights the need for Government, organisations across all sectors, international partners and the public to work together to meet our strategic objectives of reducing risk and exploiting opportunities by improving knowledge, capabilities and decision-making in order to secure the UK's advantage in cyber.

The aim of the strategy was to secure the UK's advantage in cyber space by reducing risk from the UK's use of cyber space, by:

- Reducing the threat of cyber operations by reducing an adversary's motivation and capability;
- Reducing the vulnerability of UK interests to cyber operations;
- Reducing the impact of cyber operations on UK interests and exploiting opportunities in cyber space;
- Gathering intelligence on threat actors;
- Promoting support for UK policies and;
- Intervening against adversaries through improving knowledge, capabilities and decision-making;
- Improving knowledge and awareness;

- Developing doctrine and policy;
- Developing governance and decision making [61].

The vision for cyber security in the United Kingdom

Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience.

Cyber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers.

Motivation for Cyber Security Strategy

The UK is increasingly dependent on cyber space. As cyber space continues to evolve, we will pursue the increasing number and variety of benefits that it can offer; however, with growing dependence also comes a greater exposure to the rapidly evolving threats and risks. Government must lead a coherent UK response to the security challenges that arise from these threats and risks and a strategic approach is fundamental to achieving this aim.

National Vision:

Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space:

- working together, at home and overseas;
- to understand and address the risks;
- to reduce the benefits to criminals and terrorists;
- to seize opportunities in cyber space to enhance the UK's overall security and resilience.

The guiding principles of security in cyber space

The Government's approach to cyber security must be consistent with the overarching principles of the National Security Strategy:

- The UK approach to national security is clearly grounded in a set of core values, including: human rights, the rule of law, legitimate and accountable government, justice, freedom, tolerance and opportunity for all;
- Inform about the risks, aims, and capabilities;
- High possibility of tackle security challenges early;
- Favour a multilateral approach for overseas;
- Favour a partnership approach for home;
- Develop a more integrated approach for Inside government;
- Retain strong, balanced and flexible capabilities;
- Continue to invest, learn and improve to strengthen UK security [61].

Education and skills

UK's cyber security sector means that we need more people with the right skills and education to support this. The National Cyber Security Programme is working with business, academia and the education sector to ensure we have a future workforce with cyber skills and expertise, as well as a basic understanding and awareness of cyber security among the public in general.

UK government are addressing skills at every level and have funded development of cyber security learning and teaching materials at GCSE and A-level, with further materials to be released to schools in January 2014. Also, there are funding initiatives at university level for graduates and post graduate students, as well as internship and apprenticeship initiatives, such as the one being run by GCHQ to attract technically-minded people.

To promote research in cyber security, UK government have taken few measures such as:

- set up 11 Universities as Academic Centres of Excellence in Cyber Security Research (Imperial College, Lancaster University, Newcastle University, Queens University Belfast, Royal Holloway, University of London, University College London, University of Birmingham, University of Bristol, University of Cambridge, University of Oxford, University of Southampton);
- established 4 new Research Institutes in the Science of Cyber Security (University College London, working with University of Aberdeen; Imperial College, working with Queen Mary College and Royal Holloway, University of London; Royal Holloway, University of London; Newcastle University, working with Northumbria University);
- set up 2 cyber security Centres for Doctoral Training to ensure the UK gains the high-end cyber security skills needed to tackle current and future cyber challenges (Oxford University Centre for Doctoral Training in Cyber Security, and Royal Holloway, University of London Centre for Doctoral Training in Cyber Security).

Cyber security in higher education

The government's strategy identified higher education as a sector of strategic importance that is potentially vulnerable. The UK Cyber Security Strategy identifies higher education as a strategic national asset that is vulnerable to various forms of cyber-crime. The cyber threat is highly relevant for universities seeking to protect their intellectual property, reputations and institutional systems from theft and damage. The UK government has published a progress report praising its own achievements in the two years since it launched an ambitious plan to make Britain the best place to do e-commerce.

The National Cyber Security Strategy (NCSS), launched in November 2011, also has the goals of making the UK more resilient to cyber-attacks, building partnership between government and the private sector and developing the UK's cyber security knowledge, skills and capability.

The strategy is supported by £860m from the National Cyber Security Programme, an increase from the initial funding allocation of £650m [62].

Building skills can help UK-based security software developers and consultancies to bring in export sales. The UK government has set a target of more than doubling annual cyber exports from the UK to £2 billion a year by 2016 [63] [62].

UK Cyber Security Standards

The Office of Cyber Security & Information Assurance (OCSIA) supports the minister for the Cabinet Office, the Rt Hon Francis Maude MP and the National Security Council in determining priorities in relation to securing cyberspace.

The OCSIA is headed by James Quinault. Alongside the Cyber Security Operations Centre, it works with other lead government departments and agencies such as the Home Office, Ministry of Defence (MOD), Government Communications Headquarters (GCHQ), the Communications-Electronics Security Department (CESG), and the Centre for the Protection of National Infrastructure (CPNI), the Foreign & Commonwealth Office (FCO) and the Department for Business, Innovation & Skills (BIS).

UK vision and objectives

The vision for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where it actions, guided by core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society [61].

Objectives: The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace; The UK to be more resilient to cyber-attacks and better able to protect our interests in cyberspace; The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies; The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives.

6 Cybersecurity Strategies and Best Practices of other Countries

6.1 Australia

Australia's Cyber Security Strategy [64], released in 2010, follows the Prime Minister's indication that cyber security is a top national priority. The documents recognise that the Australian economy is at high risk of cyber threats, especially when financial transactions and commercial or personal identity information are involved.

The strategy states that »confronting and managing these risks must be balanced against the civil liberties of Australians, including the right to privacy, and the need to promote efficiency and innovation to ensure that Australia realises the full potential of the digital economy«.

The main goal is to maintain »a secure, resilient, and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy«.

The following lines are quoted from the executive summary of the strategy, and precisely describe the contents of the strategy.

Guiding principles

Consistent with the enduring principles outlined in the Prime Minister's National Security Statement, the Australian Government's cyber security policy is based on the following guiding principles:

National leadership: the scale and complexity of the cyber security challenge requires strong national leadership.

Shared responsibilities: All users, in enjoying the benefits of ICT, should take reasonable steps to secure their own systems, exercise care in the communication and storage of sensitive information and have an obligation to respect the information and systems of other users.

Partnerships: In light of these shared responsibilities, a partnership approach to cyber security across all Australian governments, the private sector and the broader Australian community is essential.

Active international engagement: given the transnational nature of the Internet, in which effective cyber security requires coordinated global action, Australia must adopt an active, multi-layered approach to international engagement on cyber security.

Risk management: In a globalised world where all Internet-connected systems are potentially vulnerable and where cyber-attacks are difficult to detect, there is no such thing as absolute cyber security. Australia must therefore apply a risk-based approach to assessing, prioritising and resourcing cyber security activities.

Protecting Australian values: Australia must pursue cyber security policies that enhance individual and collective security while preserving Australians' right to privacy and other

fundamental values and freedoms. Maintaining this balance is a continuing challenge for all modern democracies seeking to meet the complex cyber security challenges of the future.

Objectives

The objectives of the Australian Government's cyber security policy are:

- All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online.
- Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers.
- The Australian Government ensures its information and communications technologies are secure and resilient.

Strategic priorities

To achieve these objectives the Australian Government applies the following strategic priorities to its programs:

- Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest.
- Educate and empower all Australians with the information, confidence and practical tools to protect themselves online.
- Partner with business to promote security and resilience in infrastructure, networks, products and services.
- Model best practice in the protection of government ICT systems, including the systems of those transacting with government online.
- Promote a secure, resilient and trusted global electronic operating environment that supports Australia's national interests.
- Maintain an effective legal framework and enforcement capabilities to target and prosecute cybercrime.
- Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions.

New capabilities

Integral to the Australian Government's Cyber Security Strategy are two new mutually supporting organisations: CERT Australia and the Cyber Security Operations Centre (CSOC).

The Australian government is bringing together Australia's national computer emergency response team (CERT) arrangements into a new body, CERT Australia. CERT Australia will be the national coordination point within the Australian Government for the provision of cyber security information and advice for the Australian community, and be the official point of contact in the expanding global community of national CERTs to support more effective international cooperation.

Established as an initiative of the Australian Government's Defence White Paper, the CSOC provides the Australian Government with all-source cyber situational awareness and an enhanced ability to facilitate operational responses to cyber security events of national importance. The CSOC will identify and analyse sophisticated cyber-attacks, and assist in

responses to cyber events across government and critical private sector systems and infrastructure.

These new initiatives will build on existing Australian Government cyber security capabilities.

6.2 Canada

Canada recognises the increasing reliance on cyber technologies in all kinds of activities, from citizens' daily life to business and critical infrastructure. It also recognizes the big impact that cyber threats may have on the economy of the country and on the quality of life of its citizens. The plan for meeting the cyber threat has been released as *Canada's Cyber Security Strategy* [65] in 2009.

This document contains the following main chapters:

Introduction. In the two-pages long introduction the document describes the high penetration of the cyberspace in the life of Canadians, and how businesses, the government, and citizens become increasingly dependent on the Internet. The growth of cyber technology requires an adequate response to cyber threats.

Understanding Cyber Threats. This chapter gives and overall view of cyber threats. Cyber-attacks can affect citizens and companies. Even if the tools and techniques required by certain attacks may be costly and sophisticated, most of cyber-attacks are recognised as *inexpensive, easy, effective, and low risk.* Three types of threats are further discussed

- State sponsored cyber espionage and military activities: quoting the document »the most sophisticated cyber threats come from the intelligence and military services of foreign states«. To address the risk from this kind of threats Canada and its allies needs to modernise the military doctrines. For this reason the NATO has adopted several policy documents about cyber defence.
- Terrorist use of the Internet: terrorist networks are using cyber tools and techniques for their activity, due to the western world's dependency on cyber systems with their vulnerabilities. The cyber-attacks performed by terrorists have not caused serious damage in the past, but this capability will develop.
- Cybercrime: organised criminals are increasing the use of sophisticated cyber-attacks for their aims. Selling stolen information like credit cards number or username and password pairs is an important business, thus any citizen is at risk. Moreover, criminal organizations are developing customised attack software and using sophisticated technologies to protect their assets and identity.

The frequency and severity of cyber threats is accelerating, and protecting Canadians in cyberspace is an evolving challenge. The Cyber Security Strategy documents mandate a range of actions and responses accompanied by continuing investments and vigilance over the long term.

Canada's Cyber Security Strategy. This chapter starts addressing the cyber threats overviewed in the previous one, defining three main pillars of the strategy:

1. *Securing Government systems.* The government is recognised as a crucial system to secure. Canadians trust the Government with their personal and corporate information and trust the delivered services. Protecting citizens is among the duties of Canada's Government and it will put in place the necessary structures, tools and personnel to meet its obligations for cyber security.

2. *Partnering to secure vital cyber systems outside the federal Government.* Canada's economy depends on the proper functioning of systems outside the Government. The Government needs to strengthen Canada's cyber resiliency in cooperation with provincial and territorial governments and the private sector.
3. *Helping Canadians to be secure online.* Quoting the strategy, »the Government will assist Canadians in getting the information they need to protect themselves and their families online, and strengthen the ability of law enforcement agencies to combat cybercrime.

Specific Initiatives. After describing the three main pillars of the strategy, the document defines a series of initiative to meet the cyber threats for each pillar, as summarised below.

Securing Government systems. The Government handles citizens' private information and transmits highly classified information essential to military and national security, and has been target of several cyber-attacks. Securing the Government is a matter of national security, protecting lives and safeguarding the economy. The strategy mandates the need to strengthen the Government's capability to detect, deter, and defend against cyber-attacks. The main initiatives in the setting of securing government systems follow:

- Establishing clear federal roles and responsibilities. It is crucial to avoid ambiguity in terms of who does what. The strategy specifies each role of each department. Public Safety Canada will design a whole-of-Government approach to reporting on the implementation of the strategy; within it the Cyber Incident Response Centre coordinates security monitoring, provides advice on mitigation, and directs the response. The Communication Security Establishment Canada enhances the capacity to detect and discover threats, provides foreign intelligence, and responds to attacks against Government networks. The Canadian Security Intelligence Service analyses domestic and international threats with the help of the Royal Canadian Mounted Police. The Treasury Board Secretariat strengthens the incident management capabilities across Government through policies, standards, and assessment tools. Foreign Affairs and International Trade Canada advises on international dimensions of cyber threats or incidents and develop a cyber-security foreign policy. The Department of National Defence and the Canadian Forces defend their own networks, identify threats and possible responses, and exchange information with allied militaries.
- Strengthening the security of federal cyber systems. There is an escalation of methods to secure the cyberspace and the methods to circumvent such security measures. For this reason the strategy mandates to continually invest in the expertise, systems, and governing frameworks. The Government needs to enhance the security of its cyber architecture, and a set of amendments to its Policy of Government Security has been made.
- Enhancing cyber security awareness throughout Government. The success of securing the Government depends on its employees. Awareness is crucial to reduce errors and incidents.

Partnering to secure vital cyber systems outside the federal government. Private sector depends on intellectual properties, business transactions and financial data. It is important to protect private companies and the infrastructure systems, which are two main contributors to quality of life. The public must be more aware of vulnerabilities to avoid identity theft and financial loss. The Government has to build on existing programs and expertise to better support cyber security research and development. It has to collaborate with the private sector and Academia to enhance information sharing activities. To this aim, partnering with the provinces and territories and partnering with the private sector and critical infrastructure sectors are recognised to be crucial. Among critical infrastructures, the collaboration towards security of process control systems and related training and exercise programs are mandated.

Helping Canadians to be secure online. It is important at the same time to deny detect and discover cybercriminal activities and to protect the privacy of Canadians. The strategy mandates activities for combating cybercrime and recognises the importance of equipping police properly. The Royal Canadian Mounted Police is given the resource to establish a centralised Cyber Crime Fusion Centre to improve the response capability to request from the Canadian Cyber Incident Response Centre. Moreover the strategy document mentions the changes in the legislation in order to enhance the capacity of law enforcement to investigate and prosecute cybercrime. On the other hand, the strategy recognise the importance of public awareness of cyber threats. It is important to know and follow the basis cyber security practices, and the Government is supposed to increase Canadians' awareness promoting such good practise. The goal is to create a culture of cyber safety, and this requires efforts in the long term.

6.3 Japan

In Japan, since 2006, ministries and agencies, other governmental organizations, think tanks, and scholars have faced sophisticated cyber-attacks from so-called »advanced persistent threats (APT)« aimed at stealing top-secret information from specific organizations and individuals. Only recently, however, Japan has recognized the reality of wide-ranging cyber espionage against not only government ministries and agencies but also against private-sector businesses. The year 2011 could be named »first year of cyber war« for Japan, being the year in which the scope of the threat became widely known. It was revealed, for example, that there had been cyber espionage on defence industrial companies and on the internal network of the House of Representatives [66].

In the face of new challenges, in March 2012 the Ministry of Economics, Trade and Industry (METI) of Japan and eight Japanese electronics companies established a »Control System Security Centre (CSSC).« This is a technology research association designed to strengthen the security of control systems of important infrastructure and to establish verification methods and evaluation of control systems. In collaboration with eighteen companies including manufacturers, vendors, and consumers of control systems, the CSSC opened a test-bed laboratory for the security of control systems in Miyagi, Tohoku in May 2013. The laboratory has several objectives: 1) to provide the latest security verification tools for controls systems, 2) to develop secure technology for control systems, 3) to drive international system security standardization, 4) to develop certification tools, 5) to provide incident support, 6) to develop human resources, and 7) to establish security guidelines.

In order to protect cyberspace, early detection of cyber-attacks is essential and warnings must be shared without delay among like-minded countries. At the same time, it is difficult to defence against cyber-attacks and cyber espionage through defensive measures alone. It will also be necessary to invade attackers' networks in return as measures of cyber-counterattacks in self-defence for purpose of identifying enemies' activities and striking back at them. This may be considered collective cyber defence.

Japan could make an important contribution to collective cyber defence by developing secure technology for control systems and by promoting global standardization of control system security. This dual track would help create a more robust social infrastructure among allies and like-minded countries.

Japan and USA have reached to an agreement to make alliance against cyber-attacks. Japan and the U.S. seek in particular to enhance the »collective cyber defence« capability of the

alliance, aiming to make it a foundation for information security and information protection more broadly. The joint statement announced in Tokyo covers a gamut of alliance-related concerns but places particular emphasis on revising the U.S.-Japan 1997 Defence Guidelines by the end of 2014 in a way that reflects new challenges, such as in the space and cyber domains, and enhancing the alliance to enable a more active international role [67].

Japan Information Security Policy Council (ISPC) has established latest Cyber security strategy in June 2013, in order to make clear the necessity to widely promote measures related to cyberspace and approach of these measures as distinguished from efforts for assuring „information security« up. The main goals are construction of world-leading, flexible and powerful cyberspace, and incorporate this cyberspace as a social system to realize a »cyber security nation« as a society that is strong against cyber-attacks, full of innovation [66].

Japan aims to construct flexible cyberspace and enhance its defensive and recovery capabilities against cyber-attacks and incidents by improving functions for recognition and analyses of cyber-attacks and for information sharing about it. For construction flexible cyberspace it is essential to define measures for all stakeholders, countermeasures and measures for defence of cyber space. Construction of vigorous cyberspace will be achieved through the activation of industry which plays a key role in responding to cyber-attacks, developing advanced technologies, providing training and fostering of human resources and literacy, and other measures that allow independently respond to the risks surrounding cyberspace. World-leading cyberspace in Japan shall be constructed and attempts shall be made to fortify contribution and outreach capabilities in the global strategic space by strengthening ministerial level dispatches, building multilaterally partnership with nations which share the same basic principles as Japan, participation in CS committees in the UN, active participation in the international rulemakings, active outreach into overseas markets, sharing good practices with overseas operators, capacity building support and confidence building measures.

The previous Japanese CS strategies were based on responsibility of individuals, but this, latest, are based on shared responsibilities and promoting cooperation between stakeholders. All stakeholders are distributed in 5 groups and each group has strictly defined role.

1. *The Government* must implement cyberspace crime countermeasures and »defence of cyberspace« to protect cyberspace related to the nation from cyber-attacks. Also Government must promote cooperation with other countries in CS areas and take participation in the formation of relevant international rulemaking.
2. Specific attention is given to *Critical infrastructure providers (CIP)*, in order to protect crucial fields, such as information and communication, finance, aviation, railways, electricity, gas, government and administrative services, medical services, water and logistic, that provide services/products for regular peoples' lives and economic activities. Strategy requires initiatives for CIP and their active participation.
3. *Private companies, educational institutions and research institutions* must implement individual CS measures and collective measures such as sharing information related to cyber-attacks cross each other.
4. As *Small and medium-sized enterprises* make up the majority of businesses in Japan, they have important role in establishing cyber nation. Also 80% of total Japan population is internet users, scope of requirement for information security measures of *Individual users* is extremely wide. Individual users must understand their responsibility for protecting themselves.
5. *Cyberspace-related operators*, who provide products and services related to cyberspace, endeavouring to ensure that no vulnerabilities are created in these products and services at the time of development, that they will also implement measures to maintain the

cyberspace hygiene by preventing the spread of damages through eliminating vulnerabilities by implementing appropriate countermeasures.

By strategy is anticipated the analysis of communications content by telecommunication carriers if necessary, the establishment of a cyber-defence unit within the Self-Defence Forces and the establishment of a cyber-security centre within the government in 2015 as the nation's highest-level organization to deal with cyber-attacks, which include the theft and destruction of data stored in computer systems at government organizations and companies, and the paralysis and destruction of such computer systems. The government's move to deal with cyber-attacks deserves praise. The government should proceed with utmost care to ensure that this constitutional provision is not undermined. It also should make sure that efforts by various public and private organizations to cope with cyber-attacks are coordinated to maximize their effect.

Analysis of communications will be indispensable in the investigation of cybercrimes. But secrecy of communications as guaranteed by the Constitution is closely linked with the freedom of expression, also guaranteed by the Constitution.

The strategy plans a setting up a cyber-defence unit within the SDF to cope with cyber-attacks that are carried out as part of an attack on the nation. The government should work out detailed rules on what conditions the proposed unit can take action. It should take care so that the unit will operate strictly following the nation's traditional defence-only defence posture. It is also necessary for the government to allocate enough resources to nurture a sufficient number of cyber security experts, and to develop and install advanced equipment to deal with cyber-attacks.

6.4 USA

The role of USA in cyber security field at global level is already mentioned in Section 3.2. More specifically, the United States released the International Strategy for Cyber-space [16] in May 2011, which describes a set of activities across seven interdependent areas, based on a collaborative model involving government, international partners and the private sector:

- *Economy*: Promoting International Standards and Innovative, Open Markets.
- *Protecting Our Networks*: Enhancing Security, Reliability, and Resiliency.
- *Law Enforcement*: Extending Collaboration and the Rule of Law.
- *Military*: Preparing for 21st Century Security Challenges.
- *Internet Governance*: Promoting Effective and Inclusive Structures.
- *International Development*: Building Capacity, Security, and Prosperity.
- *Internet Freedom*: Supporting Fundamental Freedoms and Privacy.

The National Institute of Standards and Technology (NIST) under the US Department of Commerce, pleased to release the first version of the Framework for Improving Critical Infrastructure Cybersecurity [68] (February, 2014). Framework details are presented in Section 3.2 which gives the prioritized, flexible, repeatable, and cost-effective approach helping owners and operators of critical infrastructure to manage cybersecurity related risk. NIST is also pleased to issue a companion Roadmap that discusses NIST's next steps with the Framework and identifies key areas of cybersecurity development, alignment, and collaboration.

Furthermore, the Department of Homeland Security is responsible for protecting USA Nation's critical infrastructure from physical and cyber threats. Cyberspace enables businesses and government to operate, facilitates emergency preparedness communications, and enables critical control systems processes. Protecting these systems is essential to the resilience and reliability of the Nation's critical infrastructure and key resources and to our economic and national security.

They established the National Cybersecurity & Communications Integration Center (NCCIC) which serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC's partners include other government agencies, the private sector, and international entities. Working closely with its partners, NCCIC analyses cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts.

The NCCIC's missions include:

- Leading the protection of federal civilian agencies in cyberspace;
- Working closely together with critical infrastructure owners and operators to reduce risk;
- Collaborating with state and local governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC);
- Cooperating with international partners to share information and respond to incidents;
- Coordinating national response to significant cyber incidents in accordance with the National Cyber Incident Response Plan (NCIRP);
- Analysing data to develop and share actionable mitigation recommendations;
- Creating and maintaining shared situational awareness among its partners and constituents;
- Orchestrating national protection, prevention, mitigation, and recovery activities associated with significant cyber and communication incidents;
- Disseminating cyber threat and vulnerability analysis information;
- Assisting in the initiation, coordination, restoration, and reconstitution of National Security or Emergency Preparedness (NS/EP) telecommunications services and facilities under all conditions, crises, or emergencies;
- Executing Emergency Support Function 2- Communications (ESF-2) responsibilities under the National Response Framework (NRF).

The NCCIC is comprised of four branches:

- NCCIC Operations & Integration (NO&I);
- United States Computer Emergency Readiness Team (US-CERT) which brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reduces risk to the nation's critical infrastructure by strengthening control systems security through public-private partnerships. ICS-CERT has four focus areas: situational awareness for CIKR stakeholders; control systems incident response and technical

analysis; control systems vulnerability coordination; and strengthening cybersecurity partnerships with government departments and agencies.

- National Coordinating Center for Telecommunications (NCC) which leads and coordinates the initiation, restoration, and reconstitution of NS/EP telecommunications services or facilities under all conditions. NCC leverages partnerships with government, industry and international partners to obtain situational awareness and determine priorities for protection and response.

7 Conclusion and Follow-Up

The comprehensive overview of existing cyber security frameworks presented in this report has shown that each strategy started by focusing on just a smaller subset, but would acknowledge the other mandates or dimensions of cyber security areas, as follows:

Three Dimensions. It focuses most on governmental activities, but should at least also mention international and national stakeholders as well. In future, these last two are likely to grow in importance as the role of international and non-state actors is increasingly realised.

1. **Governmental:** requires a Whole of Government approach for improving the coordination of government actors.
2. **International:** a Whole of System approach for improving international, trans-border, and 'like-for-like' coordination.
3. **National:** a Whole of Nation approach for cooperating with internal national non-state actors, from civil society to critical infrastructure providers.

Five Mandates. In addition to looking across the three dimensions of governmental, international, and national actions, it should also be considered the five main 'mandates' of governments in cyberspace. The most comprehensive strategies will include political aims, strategic goals and organisations for all five.

1. **Military Cyber:** a national military must not only defend itself from cyber incidents but consider how to use cyber capabilities offensively as well. Defence is usually considered the first priority; however offensive capabilities will increasingly important in the future.
2. **Counter Cyber Crime:** fighting crime and reducing its impact are typical centrepieces for most NCSS.
3. **Intelligence and Counter-Intelligence:** using cyberspace for espionage – and stopping adversaries from doing the same – is increasingly important for states.
4. **Critical Infrastructure Protection and National Crisis Management:** includes protecting key sectors and institutional structures to enhance cooperation and response.
5. **Cyber Diplomacy and Internet Governance:** diplomacy adapting to the new global information environment, and managing the future of the internet.

There are also **'Cross Mandate'** areas including cyber security research and development, coordination, and information sharing and data protection.

Five Dilemmas: Making implicit or explicit decisions about several key areas that can be seen as trade-offs between two public goods.

1. **Stimulate the Economy or Improve National Security:** there can be an inherent tension between the openness required for innovation and the requirements of public security.
2. **Infrastructure Modernization or Critical Infrastructure Protection:** the economic gains of adopting new technologies must be balanced against possible increases in security risks.

3. **Focus on Private Sector or Public Sector:** governments have a key role to play in cyber security but need to decide on either a 'regulatory' (mandated) or 'voluntary' approach to critical infrastructure protection.
4. **Data Protection or Information Sharing:** while information sharing is absolutely essential to NCS, the reality of (vitally needed) data protection legislation complicates these efforts.
5. **Freedom of Expression or Political Stability:** governments must ascertain to what extent, if any, they think the curtailment of 'internet freedoms' is justifiable for public safety.

References

[1] J. Ferwerda, N. Chourci and S. Madnick, »Institutional Foundations for Cyber Security: Current Responses and New Challendges«, Massachusetts Institute of Technology, Cambridge, 2010.

[2] G. Killcrece, »Steps for creating national CERTs«, Software Engineering Institute, 2009.

[3] »G8 24/7 High Tech Contact Points«, Cyber Security Co-Operation, 2009.

[4] OECD, »What is the Working Party on Information Security and Privacy (WPISP)?«, 2014. [Online]. Available: http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html.

[5] ITU, 2014. [Online]. Available: http://www.itu.int/osg/csd/cybersecurity/WSIS/.

[6] ITU, »Global Cybersecurity Agenda (GCA)«, 2014. [Online]. Available: http://www.itu.int/osg/csd/cybersecurity/gca/.

[7] ITU, 2014. [Online]. Available: http://www.itu.int/ITU-D/ict/.

[8] UNESCO, »UN-backed anti-cyber-threat coalition launches headquarters in Malaysia«, 2014. [Online]. Available: http://www.un.org/apps/news/story.asp?NewsID=30246#.U2idXfmSyiB.

[9] »IMPACT - International Multilateral Partnership Against Cyber Threats«, 2014. [Online]. Available: http://www.impact-alliance.org.

[10] ITU, »Technical and Procedural Measures«, 2009. [Online]. Available: http://www.itu.int/osg/csd/cybersecurity/gca/tech-proced.htm.

[11] CCDCOE, »Cooperative Cyber Defence Centre of Excellence«, 2009.

[12] NIST, National Institute of Standards and Technology, »Discussion Draft of the Preliminary Cybersecurity Framework«, NIST, 2013.

[13] ISO/IEC ISO/IEC-27001, »ISO/IEC 27001:2005 - Information security management system (ISMS) standard«, ISO/IEC, 2005.

[14] MindTools, »Plan-Do-Check-Act (PDCA)«, 2011. [Online]. Available: http://www.mindtools.com/pages/article/newPPM_89.htm.

[15] ISO/IEC, »ISO/IEC 17799: 2005«, ISO/IEC, 2005.

[16] USA, »International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World«, Seal of the President of the USA, 2011.

[17] B. Fraser, »Site Security Handbook«, Network Working Group, 1997.

[18] V. Abend, B. Peretti and W. Axlerod, »Cyber Security for the Banking and Finance Sector«, in *Wiley Handbook of Science and Technology for Homeland Security*, John Wiley & Sons, Inc, 2008.

[19] S. K. Das, K. Kant and N. Zhang, Handbook on Securing Cyber-Physical Critical Infrastructure, Morgan Kaufmann, 2012.

[20] ITU, »'ITU Global CYbersecurity Agenda«, http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf, 2007.

[21] ITU, »Understanding Cybercrime:A Guide for Developing Countries«, http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html, 2009.

[22] ITU, »The ITU Toolkit for Cybercrime Legislation«, http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html, 2009.

[23] ITU, »WTSA Resolution 58: Encourage the creation of national computer incident response teams, particularly for developing countries«, http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf, Johannesburg, 2008.

[24] ITU, »ITU National Cybersecurity/CIIP Self-Assesment Tool«, http://www.itu.int/ITU-/cyb/cybersecurity/projects/readiness.html, Geneva, 2009.

[25] ITU, »ITU Toolkit for Promoting a Culture of Cybersecurity«, http://www.cybersecurity-gateway.org/promoting_culture.html, 2008.

[26] ITU, »ITU National Cybersecurity Strategy Guide«, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf, 2011.

[27] OECD, »OECD guidelines towards building a culture of security«, 2002.

[28] EU, »Cybersecurity Strategy of the European Union:«, EUROPEAN COMMISSION, 2013.

[29] European Commission, »EU Cybersecurity plan to protect open internet and online freedom and opportunity«, European Commission, Brussels, 2013.

[30] Federal Chancellery of the Republic of Austria, »Austrian Cyber Security Strategy«, Federal Chancellery, Vienna, 2013.

[31] Federal Chancellery of the republic of Austria, »National ICT Security Strategy Austria«, Federal Chancellery, Digital Austria, Vienna, 2012.

[32] Cyber Security Strategy Committee, »Cyber Security Strategy«, Estonian Ministry of Defence, Tallinn, 2008.

[33] C. Czosseck, R. Ottis and A.-M. Talihärm, »Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security«, *International Journal of Cyber Warfare and Terrorism (IJCWT),* vol. 1, no. 1, pp. 24-34, 2011.

[34] »Estonian Information System Authority«, 2014. [Online]. Available: https://www.ria.ee/en/. [Accessed 28 February 2014].

[35] M. N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, M. Schmitt, Ed., Cambridge: Cambridge University Press, 2013.

[36] »NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia«, 2014. [Online]. Available: http://www.ccdcoe.org/. [Accessed 28 February 2014].

[37] Tallinn University of Technology, »Cyber Security«, 2014. [Online]. Available: http://www.ttu.ee/cybersecurity. [Accessed 28 February 2014].

[38] Kaitseliit, »Estonian Defence League's Cyber Unit«, 2014. [Online]. Available: http://www.kaitseliit.ee/en/cyber-unit. [Accessed 28 February 2014].

[39] S. Cardash, F. Cilluffo and R. Ottis, »Estonia's Cyber Defence League: A Model for the United States?«, *Studies in Conflict & Terrorism,* vol. 36, no. 9, pp. 777-787, 2013.

[40] Government Resolution 24.1.2013, »Finland's Cyber security Strategy«, Forssa Print, Helsinki, 2013.

[41] Finnish Communications Regulatory Authority (FICORA), »National Cyber Security Centre Finland (NCSC-FI)«, 2014. [Online]. Available: https://www.cert.fi/en/index.html. [Accessed 28 February 2014].

[42] Jykes, »Five cities to lead the INKA programme: Jyväskylä represents cybersecurity«, 2014. [Online]. Available: http://www.jykes.fi/en/news-a-events/2143-five-cities-to-lead-the-inka-programme-jyvaskyla-represents-cybersecurity. [Accessed 28 February 2014].

[43] »Information systems defence and security - France's strategy«, The French Network and Information Security Agency (ANSSI), Paris, 2011.

[44] J. A. Lewis and K. Timlin, »Cybersecurity and Cyberwarfare 2011«, Center for Strategic and International Studies, 2011.

[45] »The French White Paper on defence and national security«, Présidence de la république, 2008.

[46] The International Institute for Strategic Studies, »The Military Balance 2012«, The International Institute for Strategic Studies, 2012.

[47] BSI, »Bundesamt für Sicherheit in der Informationstechnik«, 2014. [Online]. Available: https://www.bsi.bund.de/.

[48] Allianz für Cyber-Sicherheit, »Anforderungen an netzwerkfähige«, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2013.

[49] R. Hartenstein, »Best Practice Ansätze zum DDoS-Schutz«, Link11 GmbH, Frankfurt am Main, 2013.

[50] Bundesamt für Sicherheit in der Informationstechnik, »Allianz für Cyber-Sicherheit«, 2014. [Online]. Available: https://www.allianz-fuer-cybersicherheit.de.

[51] Bundesministerium des Innern, »Cyber-Sicherheitsstrategie für Deutschland«, Bundesministerium des Innern, Berlin, 2011.

[52] CIS Sapienza, »2013 Italian Report on Cyber Security: Critical Infrastructure and Other Sensitive Sectors Readiness«, CIS Sapienza - Cyber Intelligence and information Security, Universita di Roma, 2013.

[53] CLUSIT, »Rapporto Clusit 2013 sulla sicurezza ICT in Italia«, CLUSIT, Milano, 2013.

[54] Symantec, »2012 Norton Cybercrime Report«, Symantec, 2012.

[55] »Europe Proposes New Laws and Regulations on Cybersecurity«, 2014. [Online]. Available: http://www.jonesday.com/europe-proposes-new-laws-and-regulations-on-cybersecurity-01-02-2014/.

[56] European Commision, »Directive 2009/140/EC of the European Parliament and of the Council«, Official Journal of the European Union, 2009.

[57] ENISA, »Spain Country Report«, ENISA, 2011.

[58] »Council of Ministers«, 2014. [Online]. Available: http://www.lamoncloa.gob.es/IDIOMAS/9/Gobierno/CouncilMinisters/index.htm.

[59] Post&Telestyrelsen, »Strategy to improve Internet security in Sweden«, National Post and Telekom Agency, 2006.

[60] E. a. C. The Ministry of Industry, »From an IT policy for society to a policy for the information society«, 2005.

[61] »The UK Cyber Security Strategy«, London, 2011.

[62] J. Leyden, 2013. [Online]. Available: http://www.theregister.co.uk/2013/12/13/uk_cyber_security_strategy_update/.

[63] W. Hammonds, »Cyber security in higher education«, 2013. [Online]. Available: http://blog.universitiesuk.ac.uk/2013/11/04/cyber-security-higher-education/.

[64] Australian Government, »Cyber Security Strategy«, Commonwealth of australia, 2009.

[65] Government of Canada, »Canada's Cyber Security Strategy«, Government of Canada, 2010.

[66] Information Security Policy Council, »Cybersecurity Strategy«, Informtion Security Policy Council, Tokyo, 2013.

[67] J. Osawa, »Collective cyber defense in the future«, *Brookings East Asia Commentary,* 2013.

[68] USA, »Framework for Improving Critical Infrastructure Cybersecurity«, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, 2014.

[69] Ministry of Defence, [Online]. Available: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf. [Accessed 28 February 2014].

[70] C. Czosseck, R. Ottis and A.-M. Talihärm, »Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security«, in *Proceedings of the 10th European Conference on Information Warfare and Security*, Tallinn, 2011.

[71] Estonian Information System Authority, [Online]. Available: http://www.ria.ee. [Accessed 28 February 2014].

[72] M. Schmitt, Ed., Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge: Cambridge University Press, 2013.

[73] NATO Cooperative Cyber Defence Centre of Excellence, [Online]. Available: http://www.ccdcoe.org. [Accessed 28 February 2014].

[74] Tallinn University of Technology, »Cyber Security«, [Online]. Available: http://www.ttu.ee/cybersecurity. [Accessed 28 February 2014].

[75] Kaitseliit, »Küberkaitse üksus«, [Online]. Available: http://www.kaitseliit.ee/et/kuberkaitse-uksus. [Accessed 28 February 2014].

[76] Government Resolution 24.1.2013, »Finland's Cyber security Strategy«, 24 January 2013. [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf. [Accessed 28 February 2014].

[77] »CERT-FI - Home Page«, [Online]. Available: https://www.cert.fi/en/index.html. [Accessed 28 February 2014].

[78] »Five cities to lead the INKA programme: Jyväskylä represents cybersecurity«, [Online]. Available: http://www.jykes.fi/en/news-a-events/2143-five-cities-to-lead-the-inka-programme-jyvaskyla-represents-cybersecurity. [Accessed 28 February 2014].

[79] N. I. o. S. a. T. NIST, »Discussion Draft of the Preliminary Cybersecurity Framework«, NIST, 2013.

[80] ISO/IEC-27001, »Information technology- Security techniques- Information security management systems- Requirements«, 2005.

[81] USA, »International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World«, Seal of the President of the USA, 2011.

[82] B. Fraser, »Site Security Handbook«, Network Working Group, 1997.

[83] V. Abend, B. Peretti and W. Axlerod, »Cyber Security for the Banking and Finance Sector«, in *Book Title Wiley Handbook of Science and Technology for Homeland Security*, John Wiley & Sons, Inc, 2008.

[84] J. Ferwerda, N. Chourci and S. Madnick, »Institutional Foundations for Cyber Security: Current Responses and New Challendges«, Massachusetts Institute of Technology, Cambridge, MA 02142, 2010.

[85] OECD, »What is the Working Party on Information Security and Privacy (WPISP)?«, 2009.

[86] WSIS, »WSIS C5«, 2009.

[87] ITU, »Global Cybersecurity Agenda (GCA)«, 2009.

[88] ITU, »Information and communication technology«, 2009.

[89] UNESCO, »UN-backed anti-cyber-threat coalition launches headquarters in«, 2009.

[90] IMPACT, »Welcome to the coalition«, 2009.

[91] ITU, »Global Cybersecurity Agenda (GCA): Technical«, 2009.

[92] BSI, »Bundesamt für Sicherheit in der Informationstechnik Startseite«, 2014. [Online]. Available: https://www.bsi.bund.de/.

[93] ACS, »Allianz für Cyber-Sicherheit Startseite«, 2014. [Online]. Available: https://www.allianz-fuer-cybersicherheit.de.

[94] Bundesamt für Sicherheit in der Informationstechnik, »Allianz für Cyber-Sicherheit«, Bundesamt für Sicherheit in der Informationstechnik, 2012.

[95] European Commision, »Directive 2009/140/EC of the European Parliament and of the Council«, Official Journal of the European Union, 2009.

[96] »Cyber Security Strategy«, 2009.

[97] Informtion Security Policy Council, »Cybersecurity Strategy«, Informtion Security Policy Council, Tokio, 2013.

[98] Jun Osawa, »Collective cyber defense in the future«, *Brookings East Asia Commentary,* 2013.

[99] »Canada's Cyber Security Strategy«, 2010.