LUISS

Department of Political Sciences *Security Studies Chair*

TITLE

The Cyber Security Challenge: A Comparative Analysis

TUTOR
Prof. Gen. Carlo Magrassi

CANDIDATE
Maria Grazia Nardoianni
Matr. 624562

CO-TUTOR
Prof. Francesco Niccolò Moro

ACADEMIC YEAR 2015/2016

Table of Contents

Introduction.

Today, the challenge posed by cyber security is a topic widely discussed and of significant importance. The cyber domain is still a largely unexplored area and this has consequences that cannot be underestimated. With the advent of the Internet, the increasing development of technology and the increasing role they take on in the daily life of every individual, protecting while ensuring the continuous operation of the cyber space, it becomes imperative.

Governments around the world, but especially those of the most advanced countries, are facing an issue that grows hand in hand with technological development. Technological progress could become then a double-edged sword if adequate measures are not adopted. In the present study will be analyzed several aspects related to cyber security, to be read in a comparative perspective with the Italian situation.

In the first chapter will be provided a set of basic definitions: the importance of the critical infrastructure for the proper functioning of industrialized societies and their growing interdependence. Then it will be explained how this interdependence makes them targets vulnerable to cyber attacks and thus why it is crucial that each country considers the protection of critical infrastructure as a key objective to achieve.

Firstly, in order to protect critical infrastructures from cyber attacks it should be made a proper distinction of both the types of attacks that can be perpetrated and the actors who can be held responsible for such attacks. Each attack has its own modality, its own specific goal, and the responsible/s behind the attack it belongs always to a specific typology of actors driven by a number of precise reasons.

All these parameters cannot be ignored otherwise the risk is of missing the ultimate goal, which is the protection and at the same time assurance of the operational continuity of critical infrastructures.

The concept of cyber security has always been linked to the problem of information: the interdependence between different software-based control systems has always been a sensitive target that required appropriate protection for allowing to the post-industrial economies continuous and reliable operation as well as for ensuring national security. Then, from this consideration, the critical information infrastructures emerged as a referent object.

Information, in turn, has always been an aspect related to power, diplomacy and armed conflict. Therefore, in light of this, the cyber domain falls perfectly into logics of geopolitics and international competition.

Providing the population of a country an access to a safe space where information can be safely exchanged or kept is a priority and intrinsic to national security. The concept of national cyber security will be explained in section 1.3.

In the second chapter, the investigation adopts a broader perspective to look at the issue: the cyber threat is a global problem.

Each country decides to avail itself of a series of tools in countering cyber crime. How countries decide to profit from these tools and the posture of a country towards the cyber issue are well explained in a comprehensive document that every country possesses and that will be fully explained, which is the National Cyber Security Strategy.

Four countries have been selected as case studies: United Kingdom, Estonia, United States of America and Canada.

These countries have been taken as examples of *best practices* based on their high level of development in this field, as well as their implementation of top quality strategies and more sophisticated cyber-responses.

A National Cyber Security Strategy can be developed through a number of methods and should always be combined with adequate resources. The principal mandates composing a National Cyber Security Strategy are the followings: Military Cyber Operations, Counter Cyber Crime, Critical Infrastructure Protection (CIP) & Crisis Management, Intelligence/Counter-Intelligence, and Cyber Diplomacy & Internet Governance.

This five mandates are exhaustively explained because they are indispensable for setting up the skeleton of a National Cyber Security Strategy, and they are also intertwined with four levels of government, namely the political/policy, strategic, operational and tactical levels, and with three so-called "*cross-mandates*": Information Exchange & Data Protection, Coordination as well as Research & Development and Education.

The importance to understand each of these mandates, to understand the differences among them but also the analogies, is pivotal to allow a more harmonized joint effort, which is directly linked to the powerfulness of a given National Cyber Security Strategy in achieving the prearranged goals.

The development of a National Cyber Security policy has to deal with many challenges both known and unknown. Furthermore, since both the national and international environment brings with it a large set of pre-existing treaties, the obstacles to the freedom of policymakers increase. For this reason, it would be an optimum if all the cyber security policies would be connected to a homogeneous architecture, which is entitled to manage the Information Security System, and at the same time reducing redundancies and overlapping legislations.

In this regard, NATO has recently increased its focus on cyber security and its cooperation with non-NATO nations, the European Union and International Organizations as well. But, unfortunately, there is still a lot of work that has to be done before achieving the so long-wished smooth synergy between all actors involved in cyber security.

Moreover, in the second chapter, regarding the analysis of the National Cyber Security Strategy, the European Union has been considered as a subject of investigation too, because as a supranational institution that legally binds its Member States, could not be ignored. Indeed, the effects of European policies in cyber security, along with other field's policies, easily spill over the legal frameworks of the Member States.

The chapter concludes with a glance to the Italian landscape, the guidelines followed and the challenges that Italy is tackling.
The third and final chapter will dedicate more space to the Italian current situation. After having explained in broad terms what is the attitude of Italy towards cyber security, here, the aim of the research is to depict the Italian current profile in matter of cyber security through a comparison with the other countries previously studied and following three lines of enquiry.

These lines revolve around:

1) The concept of threat and how threat is characterized within the cyber security picture.

A great challenge for all those engaged in the cyber field is coming to grips with the fluidity of the cyber domain. This fluidity implies a multiplicity of definitions of the actors involved, the measures to undertake and even what constitutes a threat. Clarifying the concept of threat can certainly be useful in order to better assess the proper measures to undertake for countering crime. Indeed, at the bottom of every risk assessment strategy there is the cyber threat concept.

2) The level of prioritization attributed to cyber threats by each State.

The challenge posed by cybercrime has led the most developed countries to amend their legislations to better cope with this issue. Some countries have even equated the cyber threat to others identically significant such as terrorism, for example.

Thus, according to the level of prioritization assigned, each country has adopted the response measures deemed adequate

3) The identification of leading authorities responsible of policies, law enforcement, and their roles.

Establishing who has to be in charge of managing the cyber security of a country is a significant decision. There are countries that opt for a solution implying a centralized control system and others that prefer a decentralized structure. Both aspects carry along consequences in terms of benefits and losses. After a concise overview of the governmental architecture designated to cyber security by each of the countries taken as case study, it will be deduced which one of the two aspects is better in relation to efficiency and resilience, or if a mixed approach would be more adequate.

Resources allocation is another key topic in cyber security. Thus, it won't be excluded from the discussion because it proves the concrete commitment of a country towards the issue and, of course, it gives a preview of the range of improvement that might occur in the field.

Even though in a comparative study there are many parameters that could be taken in consideration, these three are the selected ones to proceed with the study, because they have been considered important parameters that logically and prominently arose from the inquiry completed in the second chapter.

The last paragraph of the third chapter will illustrate the multifaceted framework in which Italy is entangled: even if there are some lacks in comparison with the case-studies' countries, there are also evidence of improvement and serious commitment in enhancing its security systems in order to properly countering cyber crime and keep pace with the most advanced countries.

Chapter 1.

Critical Infrastructure and Cyber Security

1.1. Critical Infrastructures Definitions

Industrialized societies depend on the proper functioning of a set of technological infrastructures such as power grids, roads, rail and telecommunications networks that due to its significance, are generically referred to as critical infrastructures.

These infrastructures, once substantially isolated systems and vertically integrated, have become increasingly interdependent to the point that an dangerous event hitting one of them in a given geographical location, it can spread to other infrastructures amplifying the negative effects and distressing displaced persons even in places very remote compared to the “source of ” the initial event.

Several cases in the last decade have highlighted the growing complexity of these infrastructures and, according to some scholars, they are so fragile that in case of extreme episodes, catastrophic consequences are almost unavoidable.

In this context, terrorists and criminals in general, could carry out attacks against these facilities, identified as attractive targets. Their attractiveness is due to their material and psychological effects related to the absence of the essential services they deliver to the population, and to its ease of identification and access to them.

These infrastructures are quite extensive and involve such a large amount of assets; for this reason the protection of all the individual constituent elements is virtually impossible, also because the types of threats are gradually amplifying and generalizing, due to the increasingly interdependence of the phenomena.

The identification of such threats and vulnerabilities of critical infrastructures has led to develop specific strategies generically referred to as CIP - Critical Infrastructure Protection.

These strategies, adopting an All-Hazard Approach, are intended to develop methodologies, tools and norms that aim primarily at reducing the negative impact that an infrastructure's malfunction, accidental or malicious, has on population, economy and society and to promote the resumption of normal function.[1]

Nowadays, all countries in the world consider protection of critical infrastructures one of their main objectives, but how can a critical infrastructure be defined?

There is no unique definition of critical infrastructure that is universally accepted, nonetheless critical infrastructure is often identified as that infrastructure whose incorrect functioning, even for a limited period, may negatively affect the economy of individual subjects or groups, causing economic losses and/or even expose population and facilities to a safety and security risk.[2]

There are also many definitions that try to explain what is a critical infrastructure and that can be recognized as valid. For instance, within the European Union a Critical Infrastructure is defined as "an asset, system or part thereof located in member states which is essential for the maintenance of vial societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a member state as a result of the failure to maintain those functions"[3].

[1] Prof. Roberto Setola, Rapporto di Ricerca 2011, *La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici*, Centro Militare di Studi Strategici CEMISS, http://www.masterhomelandsecurity.eu/wp-content/uploads/2012/08/Protezione-infrastrutture-e-risorse-critiche_Setola.pdf.

[2] M. Brunner and E. M. Suter. *International CIIP Handbook 2008/2009*. Center for Security Studies, ETH Zurich, 2008.

[3] TENACE PROJECT, Research Report 2014, *Critical Infrstructure Protection: threats, attacks and countermeasures*, pages 5-6. http://www.dis.uniroma1.it/~tenace/deliverables_eng.php?lang=eng&section=0.

Instead, a European Critical Infrastructure (ECI) is defined as a “critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure”.[4]

The ECI definition arises from the potential impact that can be caused by a failure/destruction of an infrastructure in terms of sectoral and inter-sectoral relevance.

The inter-sectoral evaluation criteria are connected to: potential victims, in terms of number of fatalities and/or injuries; potential economic effects, in terms of financial losses, deterioration of products or services, and environmental effects/damages; potential effects on population, in terms of impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services.[5]

Another type of critical infrastructure’s definition to take into account may be the one provided by the Public Law 107-56 (October 26, 2001) of the United States which identify critical infrastructures as “systems and assets, whether physical or virtual, that are so vital to the United States 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.”[6]

Basically, the above definitions show the main analogy: the critical infrastructures’ threats are caused by accidents, human error or attacks that automatically produce malfunctioning of the system.

[4] European Union Directive 2008/114/EC, 2008.
[5] TENACE PROJECT, Research Report 2014, *Critical Infrstructure Protection: threats, attacks and countermeasures*, pages 5-6. http://www.dis.uniroma1.it/~tenace/deliverables_eng.php?lang=eng&section=0.
[6] Ibidem, page 7.

Protection of the critical infrastructures is very important, both for autonomy of the infrastructures themselves and for those that are dependent on other infrastructures to function properly.

Obviously, the aforementioned protection requires a classification of exact areas in which the critical infrastructures operate.

Over the years the European government has provided such list of accurate areas (see Table 1) but with the promulgation of the council directive 2008/114/EC[7], accepted only two of the areas listed below, specifically transportation and energy, "forcing" other countries to draft their own list of critical infrastructure's areas.

Energy	Nuclear Industry
ICT	Water
Food	Health
Financial	Transport
Chemical Industry	Space
Research Facilities	

Table 1.: EU draft list of critical infrastructure activity areas.[8]

Critical infrastructures of each country may include: oil pipelines, electricity networks, transportation, water and gas networks and financial and banking systems.

All these are increasingly managed electronically and this implies a series of consequences both positive and negative. Obviously, the electronic management of the infrastructures improves

[7] European Union Directive 2008/114/EC, 2008.

[8] Directive of the council on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection. COM (2006) 787, Brussels, 2006.

their efficiency but also exposes them to new risks, i.e. the so-called cyber attacks, which with their destructiveness aim to paralyze the activity of the infrastructures and are feared for the domino effect that they can cause.

One feature to consider in the protection of critical infrastructure is absolutely the increasing interdependence between infrastructures. This interdependence, although it has positive effects such as cost reduction, quality of service and efficiency, lays open to the so-called domino effect, easily putting the infrastructures in jeopardy.

An interdependency is a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other.[9]

In order to facilitate their identification and analysis the infrastructures interdependence can be characterized according to various standards.
Focusing on the type of interdependencies, four classes have been specified in[10]: physical, cyber, geographic and logical.

- Physical interdependencies, which arise from physical links or connections among elements of the infrastructure. In this context disruptions and perturbations in one infrastructure can propagate to other infrastructures.
- Cyber interdependencies, which occur when the state of an infrastructure depends on information transmitted through the information infrastructure. Such interdependencies result from the increased use of computer-based information systems, such as SCADA systems, to support control, monitoring and management activities.

[9] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, pages 11-25, December 2011.
[10] *Idem*.

- Geographic interdependencies, which exist between two infrastructures when a local environmental event can create state changes in both of them. This generally occurs when the elements of the infrastructure are in close spatial proximity.
- Logical interdependencies, which gather all interdependencies that are not physical, cyber or geographic, caused for example by regulatory or policy constraints.[11]

Consequently, the impact of a cyber-attack on an interdependent infrastructure can produce much more losses than an attack directed to a single infrastructure and can exacerbate the damages.

1.2. Cyber Attacks: Features and Problems

There are three basic steps to follow in order to protect an infrastructure from cyber-attacks: identify the threat, reduce the infrastructure vulnerability, and identify the source of the damage or the origin of the attack. In order to analyze a threat, some distinctions are necessary.

First of all, cyber threats can be categorized as failures, accidents, and attacks.

Failures are potentially damaging events caused by deficiencies in the system or in an external element on which the system depends. Usually failures are internally generated events and may be happening due to software design errors, hardware degradation, human errors, or corrupted data.

Accidents include the entire range of randomly occurring and potentially damaging events such as natural disasters. Usually, accidents are externally generated events.

Attacks (both passive and active) are potentially damaging events orchestrated by a human adversary. They are the main focus of the cyber-security discourse.[12]

[11] TENACE PROJECT, Research Report 2014, *Critical Infrstructure Protection: threats, attacks and countermeasures*, page 24. http://www.dis.uniroma1.it/~tenace/deliverables_eng.php?lang=eng&section=0

The vulnerability of the infrastructure is also influenced by the existence of a multiplicity of actors that may launch treacherous attacks.

It is enumerated as follows, a short list of groups of actors to which the cyber-attacks may be attributed:

Nation States: are an important group of actors. They are important is due to the fact that CIs are relevant targets in modern cyber-warfare, and attacks against CIs can be politically or economically motivated. In this scenario, Nation States play an important role. An external subject paid or supported by Nation-states offices to compromise another nation's CIs can be included in this category.

Non-state organized threat groups: usually labeled as "cyber terrorists" are also a worrying threat. The potential for asymmetric warfare derives from the ease of attacking CIs through cyber-warfare means.

Hacktivists: the term "hacktivist" refers to an attacker, in many cases with limited technical skills, who relies on ready-to-use attack kits and services, or even third-party botnets, to cause damage to a system. Protests are often politically motivated. Although with different motivations than nation states, hacktivists also see CIs as an appealing target for their campaigns.

Business-oriented attackers: it is a more traditional category of attackers and they are basically interested in performing abusive activities against competitor-controlled CIs in order to cause concrete damage and gain business advantages.

Casual attackers: also called "script kiddies", are individuals who use existing computer scripts or code to hack into computers, lacking the expertise to write their own. Usually they are not very relevant, but they gain much more importance if considered in the context of CIs. Although

[12] Alan Collins, *Contemporary Security Studies*, Third Edition, Oxford University Press 2013, pages 363-364.

they don’t have normally lots of technical skills, launching an attack against an Internet-facing CIs can cause serious damage, much more than in the case of simple IT system (website).[13]

But what is behind an attack? What is the real primary objective?

In general, the main objective is the control of the full system, which allows the intruder to delay, disrupt, corrupt, exploit, destroy, steal or modify information.[14]

However, terrorists or hackers are driven by a set of motivations which can vary from a political nature to a financial one, where hitting valuable CI may result in a substantially higher financial impact than hitting a traditional IT system.[15]

The cyber attacks can be perpetrated through the use of different instruments. The totality of these instruments is generally referred to as malware, but can be easily divided into viruses, worms or other bugs, and Trojan horses.

Viruses, worms or other bugs are computer programs that replicate functional copies of themselves with varying effects ranging from mere annoyance and inconvenience to compromise of the confidentiality or integrity of information.

The Trojan horses are destructive programs that masquerade as benign applications but set up a back door so that the hacker can return later and enter the system. Often system intrusion is the main goal of more advanced attacks.[16]

The degree of severity of the attack is also correlated to the importance of the information manipulated, stolen, destroyed, and so on. The more such information is important, the greater, in terms of the damage, the impact of the attack is.

[13] TENACE PROJECT, Research Report 2014, *Critical Infrstructure Protection: threats, attacks and countermeasures*, pages 28-29. http://www.dis.uniroma1.it/~tenace/deliverables_eng.php?lang=eng&section=0
[14] libro ss pag 364
[15] TENACE PROJECT, Research Report 2014, *Critical Infrstructure Protection: threats, attacks and countermeasures*, page 29. http://www.dis.uniroma1.it/~tenace/deliverables_eng.php?lang=eng&section=0
[16] Alan Collins, *Contemporary Security Studies*, Third Edition, Oxford University Press 2013, page 364.

In addition, one of the major challenges of cyber-security is linked to the problem of attribution. The cyber domain is still, in some ways, unexplored and this makes it very difficult to identify the true responsible of an attack. Abiding by the logic of "who could gain from this attack?" in order to find out a hypothetical cyber-terrorist, it is not a valid justification for undertaking a political action, as it is too vague.

For high-profile criminals hiding in cyber space may be very simple, and often investigating the reasons that may have led to an attack is not enough to find out who was the culprit.

1.3. National Cyber Security Concept

The cyber security discourse originated in the United States in the 1970s, had its peak in the 1980s and then spread involving all other countries in the late 1990s.

The Cold War was decisive in shaping the strategic context in which the topic of cyber security was developed, and it witnessed the United States leaders of this emerging phenomenon, both from a technical and intellectual perspective[17].

The cyber security is and has always been linked to the issue of information. Information has always been a fundamental aspect of power, diplomacy and armed conflicts.

Initially, between the 1970s and 1980s, the information to be protected were those belonging to private sectors, which decided to digitalize them, and all government networks containing classified information.

[17] Alan Collins, *Contemporary Security Studies*, Third Edition, Oxford University Press 2013, page 364.

Towards the 1990s, the situation changed slightly: the information assumed a greater role, especially in international relations. Their importance grew thanks to the proliferation of information and communication technology (ICT).[18]

Also, it became clear that the interdependence between different software-based control systems was a sensitive target that needed adequate protection, in order to enable continuous and reliable operation for ensuring both national security and the proper functioning of a post-industrial economy. The referent object that emerged was the totality of critical (information) infrastructures that provide the way of life that characterizes our societies.[19]

The scenario offered by the social and economic revolution initiated by the Internet's advent, presented new opportunities and new threats as well: the markets have become more open, and the connections faster and more pervasive. Often, however, the latter are based on systems and computer networks increasingly assailable to offenses by those who wish to compromise them, harm them or use them to get information.

The new industrial revolution of Internet and cyber security has brought significant changes in every aspect of the life of a citizen. In the economic field, for example, it has seen a change also in the corporate organizational models and products.

Certainly, the huge opportunities are accompanied by many risks: the pervasiveness of the devices, the vulnerability of software systems and the reduction of costs allow the conditions for a large increase of attacks, both in terms of quality and number of the threat.

The cyber domain perfectly falls within the geopolitical logics and the international competition. Since it includes both physical and digital elements, such as cables, satellites, routers, public administrations and private computers, contains elements that connect them to a precise

[18] Ibidem, page 363.
[19] Ibidem, page 365.

geographical location, and data that has a strategic importance in terms of economy, politics and national security.

To provide the country with physical security for its population and the economic prosperity needed, is therefore necessary to ensure an access to places where information can be exchanged and/or kept safely. The safety of the national cyber space is thus a strategic goal, especially if it is desirable achieving the greatest degree of independence in the prevention and management of risks related to data and critical infrastructures.

Since the aforementioned is a strategic objective, therefore, it is an absolute priority of a country to finance research and industry in this area, as part of a broader strategy.[20]

The beginning of the construction of an institutional process in favor of the cyber space protection is relatively recent, but the commitment shown by governments of various countries has given proof of several initiatives.

The main objective in this field, not only concerning the Italian national security but all countries' one, is the consolidation of a reaction system which is able to operate quickly and in a very efficient manner in the event of accident or hostile action perpetrated against national infrastructures. This can only be achieved by a set of proposals.

First of all, it is crucial to increase the allocation of human and material resources in both the administrations and the bodies involved, in line with the standards of the major international partners.

It is also necessary, the creation of an institutional coordination, ensuring the sharing and circulation of information.

It has not be underestimated a further development of a public-private partnership, continuing the awareness' endeavor of economic operators, who run critical infrastructure and do

[20] *Il Futuro della Cyber Security in Italia*, 18 Novembre 2015, https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/il-futuro-della-cyber-security-in-italia.html.

business in areas of national strategic importance, and initiating interactions with other sectors potentially exposed to systemic capacity's cyber-attacks.

From a technological point of view, in order to have a realization of the most advanced defense and reaction systems, is also useful an increasing collaboration with universities and research centers for the development of the study and information security activities.

Finally, it is pivotal working to guarantee the national coordination as a precondition for an international cooperation, *conditio sine qua non* to assure the achievement of the same level of preparedness and interoperability.[21]

The road towards the achievement of an ever more effective cyber security system is still long and full of challenges, especially in a context that is evolving so rapidly and appears "liquid" in its threats and its protagonists.
But the work of institutional actors is increasingly timely and pro-active in warrantying the safety, even in the new dimension of the cyber domain.[22]

[21] *La Sicurezza del Cyberspazio Come Priorità Strategica*, 25 Novembre 2015, https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-sicurezza-del-ciberspazio-come-priorita-strategica.html.

[22] Ibidem.

Chapter 2.

The Cyber Threat: a Global Issue

2.1. National Cyber Security Strategy

Security is certainly one of the fundamental pillars of the proper functioning of a country. It has been well documented that a high percentage of citizens, particularly in middle-low income countries, express greater concern for safety, security and justice.

Safety and security represent many things, including a stable income, consistent housing, clothing, and food supplies as part of the predictability of daily life, protection from crime, and psychological security[23].

In an ever more connected world like today's, the challenges faced by the various countries are many.

Taking advantage of the most innovative technologies, putting them at the service of a government is on the agenda. There are, however, several tensions related to this aspect, and the solutions are still being tested. There is only one thing it can be taken for granted: the need to include a cyber security program on the national security agenda of a country, namely a national cyber security strategy.

The first country to talk about National Security Strategy were the United States, in 1947, which many times have changed the meaning associated with the term National Security[24] and have elaborated about 15 NCS only between 1986 – 2012[25].

[23] *The importance of safety, security and justice*, GSDRC, Applied Knowledge Services. http://www.gsdrc.org/topic-guides/safety-security-and-justice/concepts/the-importance-of-safety-security-and-justice.

[24] According to a US defence department manual, 'national security' is '[a] collective term encompassing both national defence and foreign relations of the United States. Specifically, the condition provided by: a. a military or

In 2007 there was a major change: the cyber attack perpetrated against Estonia was a real watershed, because it showed clearly the vulnerability of the contemporary societies[26]; as a direct consequence of this, there was a global spread of national security strategies and an increase in the elaboration of those, but the most important feature was the inclusion of cyber security in the National Security Strategy of a given country.

However, a National Cyber Security Strategy, like all strategies, has its costs and its dilemmas to cope with.

Basically, five fundamental dilemmas can be listed:

1) Stimulate Economic Growth VS Improve National Security

The way a nation uses its network and information systems essential to boost the economic development is closely linked to the nation's own capabilities to protect these systems and ensure their integrity, availability and confidentiality. The problem is that although the risks associated are increasingly known, fewer businesses and consumers are willing to invest massively in ICT, and then exploiting the existing advanced technologies to enhance the protective measures. This general lack of investment puts firms and consumers at greater risk, leading to economic loss at the individual and aggregate level and thus, directly poses a threat to national security[27].

defence advantage over any foreign nation or group of nations; b. a favourable foreign relations position; or c. a defence posture capable of successfully resisting hostile or destructive action from within or without, overt or covert' (U.S. Joint Chiefs of Staff, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, (Ft. Belvoir, VA: DTIC, 2012), http://www.dtic. mil/doctrine/new_pubs/jp1_02.pdf.).

[25] Alexander Klimburg, *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012, page 26, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

[26] Luca Locatelli, *In Estonia sul fronte della cyber guerra*, 24 Settembre 2014, L'Espresso, http://espresso.repubblica.it/plus/articoli/2014/09/22/news/in-estonia-sul-fronte-della-cyberguerra-1.181073.

[27] US Department of Commerce, *Cybersecurity, Innovation, and the Internet Economy (Green Paper)*, (Gaithersburg, MD: NIST, 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_ FinalVersion.pdf.

An appropriate solution could be the implementation of a right mix of policies involving the private sector with regard to the capabilities and responsibilities, without impeding the economic growth.

2) Infrastructure Modernization VS Critical Infrastructure Protection

The clash that opens up here is between the businesses' priorities and those of governments. Businesses are obviously oriented towards the capitalization of the ICT bonus, in order to derive maximum profits while saving on basic security.

The major concern of governments instead is public safety. As mentioned in the first chapter, the attack to an infrastructure can easily affect other infrastructures, creating a disastrous domino effect, which is exactly what the governments always seek to prevent.

Then, the ideal solution would be the implementation of appropriate security measures, which meet the costs of putting them in place without exceeding the State's budget or creating hurdles to innovation and economic development.

3) Private sector VS Public sector

The private sector can be considered in all respects the so-called "service provider" and the role it plays in National Cyber Security is crucial: governments have a clear interest in cooperating with the private sector, helping them to provide the essential services of a country; the problem revolves around how governments decide to interact with the private sector. Some governments make it through strongly interventionist policies, through the use of regulations for example, others may trust in a more "spontaneous" collaboration.

Since the State's involvement in private affairs is primarily an ideological matter, the situation varies from country to country.

However, the majority still opts for a shared responsibility in the Cyber Security sector.

4) Data Protection VS Information Sharing

At the heart of the cyber security there is a quite thorny tension, which is partly still unresolved: the need of governments to ensure citizens the protection of sensitive data and the expectation of the citizens themselves to be protected by governments vis-a-vis the need for information exchange to enhance national and transnational security.

Although nowadays many governments have introduced privacy rights for individuals and legislated extensively on data protection, the request for exchange of information for countering crime, cyber espionage and other illicit activities, remains high.

Thus, often it happens that national laws are not enough to guarantee citizens a privacy protection adequate to their expectations.

5) Freedom of Expression VS Political Stability

Recently has been illustrated by news and reports, how ICT and innovative use thereof can enhance or constrain the power of politicians and the general public.

For example, ICT raise privacy concerns because governments and corporations can use digital surveillance technologies to create digital dossiers of the citizens[28].

More and more often the case that new technologies are being used to change also the outcome of the struggle for freedom and progress: like the Iranian case, in 2012, when the Iranian Minister for Information and Communications Technology co-opted the internet as a tool to target and silence the citizens[29].

[28] Alexander Klimburg, *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012, page 41, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

[29] Iran announced that would have field a national Intranet and would have begun blocking several services like Google, Google Plus, Gmail, Yahoo and Hotmail, in line with the Iran's plan for a "clean Internet". These Western services would have be replaced with government Internet services like Iran Mail and Iran Search Engine. Amrutha Gayathri, *Iran To Shut Down Internet Permanently; 'Clean' National Intranet In Pipeline'*, International Business Times, 9 April 2012.

Most of the National Security Strategies have a fairly recent origin. As previously explained, the United States were the first to speak of NSS. Initially, all NSS existing in the world, differed in many respects, especially in the definition of what was understood as security, what had to be protected and what were the threats.

To date, however, it may be a certain convergence between all existing NSS, especially in terms of challenges and threats.

An NSS document is a significant backbone of a country as well as all encompassing, since it contains many elements ranging from internal security, external security, to defense and economy. Because of this, it catches the attention of policy-makers.

But from which perspective it can be observed the convergence between all existing NSS today?

The various policy-makers, responsible for creating these NSS, tend to follow certain trends that have proven to be shared from all the countries involved.

Firstly, over time, there has been a sort of fusion, from the point of view of the identification of the threats that a State has to face, such as, proliferation of weapons of mass destruction, terrorism, organized crime, and of course cyber security: surely, the terrorist attacks of 11/09 have shaken the international system, and enlightened the minds of policy-makers and heads of State, in order to find a junction point and develop a shared operational framework of dangers to be tackled, for guaranteeing and preserving the common good.

Another important trend easily found in today's NSS, is the inclusion of new threats and challenges.

A striking example can be the challenge posed by climate change, which, if not faced today with the proper means, is likely to have harmful effects in the long run. And, unfortunately, perhaps it is exactly this awareness of the non-impact in the short time that leads to underestimate the threat itself.

Obviously the cyber security is part of this trend, and its incorporation in the NSS entails ambiguous implications: despite all policy-makers agree on the need for international cooperation, a 2010 survey of specialists, business executives and policy-makers, indicates that little is being done, since the worldwide cyber-security cooperation is not working well on tactical level and is practically non-existent on the strategic level[30].

Another common feature of all current NSS, is the increasing awareness of the need to keep close the connection between internal and external security, and therefore to improve cooperation between all government departments (especially interior and justice, and foreign affairs and defense).

Of course, from this outlook it might be expected a greater integration between the various policies, on several levels: from the economic to the political and the military ones, as a direct consequence of the above-mentioned situation.

For this reason, it is often mentioned in the NSS, the so-called Comprehensive Approach[31].

Despite all these trends, the most general of all seems to be the high priority given to the cyber issue: to date, over 20 States have released a National Cyber Security Strategy (NCSS) or national information security strategy[32]. With respect to NATO members, nearly half have produced a NCSS that details national visions, guiding principles, perceptions of the threat and strategic objectives[33].

[30] EastWest Institute, *International Pathways to Cybersecurity*. Report of Consultation, Brussels: EastWest Institute, 2010, http://www.ewi.info/system/files/CyberSummaryReport.pdf.

[31] Alexander Klimburg, *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012, page 41, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

[32] Ibidem, page 53.

[33] Idem.

In the table below, there are four examples of National Cyber Security Strategies.

Nation	*Issued*	*Lead Agency*	*English version*	*Other Languages*
Canada	Oct. 2009	Public Safety Canada	Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada (nota 182)	French
Estonia	Sept. 2008	Ministry of Defence	Cyber Security Strategy (184)	Estonian
United States	Feb. 2003	White House	The National Strategy to Secure Cyberspace (202)	-
United Kingdom	Nov. 2011	Cabinet Office	The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. (201)	-

However there are many differences among States about the definition of cyberspace: for some of them it is limited to the Internet, while others attribute to it a broader meaning including also critical infrastructures.

Approximately, not all the existing NCSS have a direct link with the NSS, even if a NCSS can be a very important part of nation's declaratory policy: United States, for example, has repeatedly warned that it would consider a cyber attack an "act of war"[34].

[34] Most recently in the US DoD Cyber Strategy, commented on in the Wall Street Journal (see Siobhan Gorman and Julian E. Barnes, *'Cyber Combat: Act of War',* The Wall Street Journal, 30 May 2011.)

The limits that usually constrain a NCSS and prevent it from achieving the sought results are several.

First of all, there is a lack of clear definitions of all cyber-related terms, which increase the confusion about the topic.

Then, the level of transparency is not always high: in a NCSS, enunciating the goals it is not enough, while making the document available for the majority of the population, preferably written in English, recognized as international language, would be a much greater improvement.

Lastly, it is crucial illustrating to the stakeholders the national framework required, emphasizing on the collaboration between public & private sectors[35].

Before moving towards an in-depth analysis of a NCSS, it is worthy considering all the actors involved in this scenario, which can be gathered into three large groups: State Actors, the most powerful and well-resourced, Organized Non-State Actors, hacker organizations or cyber militia agencies, often supported by governments for espionage affairs, and Non-Organized Non-State Actors, who are usually small groups of hacktivists, poorly-equipped, or lone individuals.

Undoubtedly, as stakeholders, they all play a role in both defensive and offensive cyber activities.

The antithesis between these two types of activities is laid down as follows: the goals of the offensive actions may be those of spying, stealing monetisable information, disrupt malicious attacks; while those of defensive actions may be basically to protect the nation, detect the threats, and respond to the attacks, thus the defensive activities involve also an offensive-operational side[36].

Nowadays, when preparing a strategy, all the stakeholders involved have to bear in mind that a synergy at governmental, societal and international level is indispensable; and at the same time every government must be able to work in partnership with these stakeholders.

[35] Alexander Klimburg, *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012, pages 61-62, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.
[36] Ibidem, pages 78-79.

A NCSS can be developed through a number of methods and should always be combined with adequate resources that during periodic audits can be quantified: in essence is all about how and where the governmental resources will be allocated. Sometimes, this task has shown to be very difficult for State actors, who are usually curbed by a defined budget[37].

The principal areas composing a NCSS are the followings: Military Cyber, Counter Cyber Crime, Critical Infrastructure Protection (CIP) & Crisis Management, Intelligence/Counter-Intelligence, and Cyber Diplomacy & Internet Governance.

Let's briefly inspect each area:

Military Cyber Operations

This area is made up of many components, also very different between them. It ranges from the protection of the own ICT systems, through a so-called CERT or CSIRT, Computer Emergency Response Team or Computer Security Incident Response Team, to strategic cyber operations, which may include the ability to wage a "cyber war" on the war fighting capability of the enemy[38].

Counter Cyber Crime

Counter cyber crime is a multifaceted issue, thus this area comprises a broad set of organizations and sees the direct involvement of different ministries (from that of justice to the ministry of interior) in order to achieve the best results at the strategic and policy level.

Intelligence / Counter-Intelligence

This mandate is very thorny, since the boundaries separating military cyber operations launched to counter cyber crime and those launched for cyber espionage sometimes is very blurred. This is due to the difficulty of verifying who is really the perpetrator, which is an intrinsic

[37] Ibidem, pages 81-107.

[38] See, for instance, Gregory Rattray and Jason Healey, *Categorizing and Understanding Offensive Cyber Capabilities and Their Use, in Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy*, ed. National Research Council (Washington, DC: The National Academies Press, 2010).

hindrance of the cyber security, and thus how to response properly to a cyber attack or how to prevent it.

Cyber Security Crisis Management and CIP

The Cyber Security Crisis Management mandate implies the existence of a top crisis management advisory group (which may be a CERT or CSIRT) and this group, in addition to having a NCS fully integrated into it, it is also connected to the emergency management structure at political level[39].

Critical Infrastructure Protection (CIP) activities, instead, zoom in prevention. In order to be efficient, these activities require the adoption of a legislation ruling over information security standards and duties regulation of both government and private sector.

Internet Governance and Cyber Diplomacy

Internet governance builds on an infrastructure of non-governmental driven self- regulation, in which the Internet grew bottom-up with a minimum of government and public sector influence. The principal activity areas are related to pro-action/prevention.

Cyber diplomacy[40] is considered here to be the general formal state engagement of a nation's diplomatic processes in the overall theme of global cyber security. In particular, this refers to multilateral or bilateral activity aimed at managing state- to-state relationships in cyberspace[41].

These five mandates can be mapped along all the stages of the "cyber incident management cycle"[42], which is usually divided into six elements, as follows:

[39] Alexander Klimburg, *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012, page 125, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

[40] Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, page 7.

[41] Klimburg and Mirtl, *Cyberspace and Governance – A Primer (Working Paper 65)*.

[42] Lenny Zeltser, *The Big Picture of the Security Incident Cycle*, Computer Forensics and Incident Response, 27 September 2010.

Pro-action: "defined as 'activities that reduce or remove the structural causes of insecurity' ".[43]

Prevention: in an emergency management context this has been defined as 'actions to avoid an incident or to intervene to stop an incident from occurring.'[44]

Preparation: defined as 'planning, training and exercising' to ensure efficient coordination during incident response.[45]

Response: addresses the immediate and short-term effects, and prevents further damage after an incident occurs.[46]

Recovery: this encompasses 'activities and programs implemented during and after response that are designed to return the entity to its usual state or to a 'new normal'.[47]

Aftercare/follow up: takes into account the psycho-sociological impact of an incident to (parts of) the population covers incident and incident management investigation (such as fact finding and the writing of lessons identified), as well as forensic analysis, criminal investigation and the prosecution of suspects.

Nevertheless, the Aftercare/Follow up element, in some countries, may be incorporated in the recovery phase.

The five mandates previously analyzed, indispensable for setting up the skeleton of a National Cyber Strategy, are also intertwined with four levels of government, namely the political/policy, strategic, operational, and tactical levels, and with three so-called "cross-

[43] Dutch Ministry of Housing, Spatial Planning and the Environment, Handreiking Security Management, (The Hague: Dutch Ministry of Housing, Spatial Planning and the Environment, 2008), http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2010/11/26/handreiking-security-management/11br2008g225-2008613-154851.pdf.
[44] ICDRM, *Emergency Management Glossary of Terms*. 76.
[45] US Departmen to Homeland Security, National Incident Management System, (Washington,DC:FEMA, 2008), http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.
[46] ICDRM, *Emergency Management Glossary of Terms*. 85-6.

[47] Ibidem, page 82.

mandates": Information Exchange & Data Protection, Coordination as well as Research & Development and Education.

The importance to understand each of these mandates, to understand the differences among them but also the analogies, would allow a more harmonized joint effort, which is directly linked to the powerfulness of a given NCS in achieving the prearranged goals.

While, a lack of understanding the features of these areas, and also providing too many divergent definitions of each area or, even worse, avoiding to recognize the ties amongst the mandates, would result in a disastrous outcome because can lead to *stovepiped* approaches.

The main consequences of this type of approach are: conflicting legal requirements, frictions between cyber security functions, organizations and capabilities and misallocation of resources, especially when the latter are assigned without a proper policy.[48]

As it seen, the development of a National Cyber Security policy has to deal with many challenges both known and unknown. Furthermore, since both the national and international environment brings with it a large set of pre-existing treaties, the obstacles to the freedom of policymakers increase.

For this reason, it would be an optimum if all the cyber security policies would be connected to a homogeneous architecture, which is entitled to manage the Information Security System, and at the same time reducing redundancies and overlapping legislations.

In this regard, NATO has recently increased its focus on cyber security and its cooperation with non-NATO nations, the European Union and International Organizations as well. But, unfortunately, there is still a lot of work that has to be done before achieving the so long-wished smooth synergy between all actors involved in cyber security, especially because the legal

[48] Alexander Klimburg, *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012, page 108, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

framework of each country is, in turn, hindered by coinciding dispositions imposed by supranational organizations, like for example the EU itself, or national norms.

In this chapter, four countries, namely United Kingdom, Estonia, United States of America and Canada, will be taken as objects of investigation. Each country's cyber security strategy will be briefly examined, in order to verify what are the actions undertaken by those countries, in the light of what has been previously illustrated.

2.1.1. Case Study: United Kingdom

The "National Security Strategy and Strategic Defence and Security Review 2015" document, presented to the Parliament by the then-Prime Minister David Cameron, highlights the vision embraced by the country to tackle security issues and ensure the economic strength, as both aspects are seen by UK like two sides of the same coin.

According to this document, United Kingdom chose to invest substantial resources in defence and overseas development.

Particularly the British National Security Strategy focuses on the following priorities:

- Strengthening the Armed Forces and the security and intelligence agencies, so that they remain world-leading, and promoting a collaboration with the British close allies, including the US and France, to deter or defeat the adversaries.
- Enhancing the UK position as the world's leading soft power, promoting the values and interests globally.
- Investing more in British current alliances including NATO, building stronger relationships with growing powers, and working to bring past adversaries in from the cold.

- Strengthening the domestic resilience and law enforcement capabilities against global challenges, which increasingly affect British people, communities and businesses.
- Deterring state-based threats, responding to crises rapidly and effectively and building resilience at home and abroad.
- Tackling terrorism head-on at home and abroad in a tough and comprehensive way, countering extremism and challenging the poisonous ideologies that feed it, while remaining a world leader in cyber security.[49]

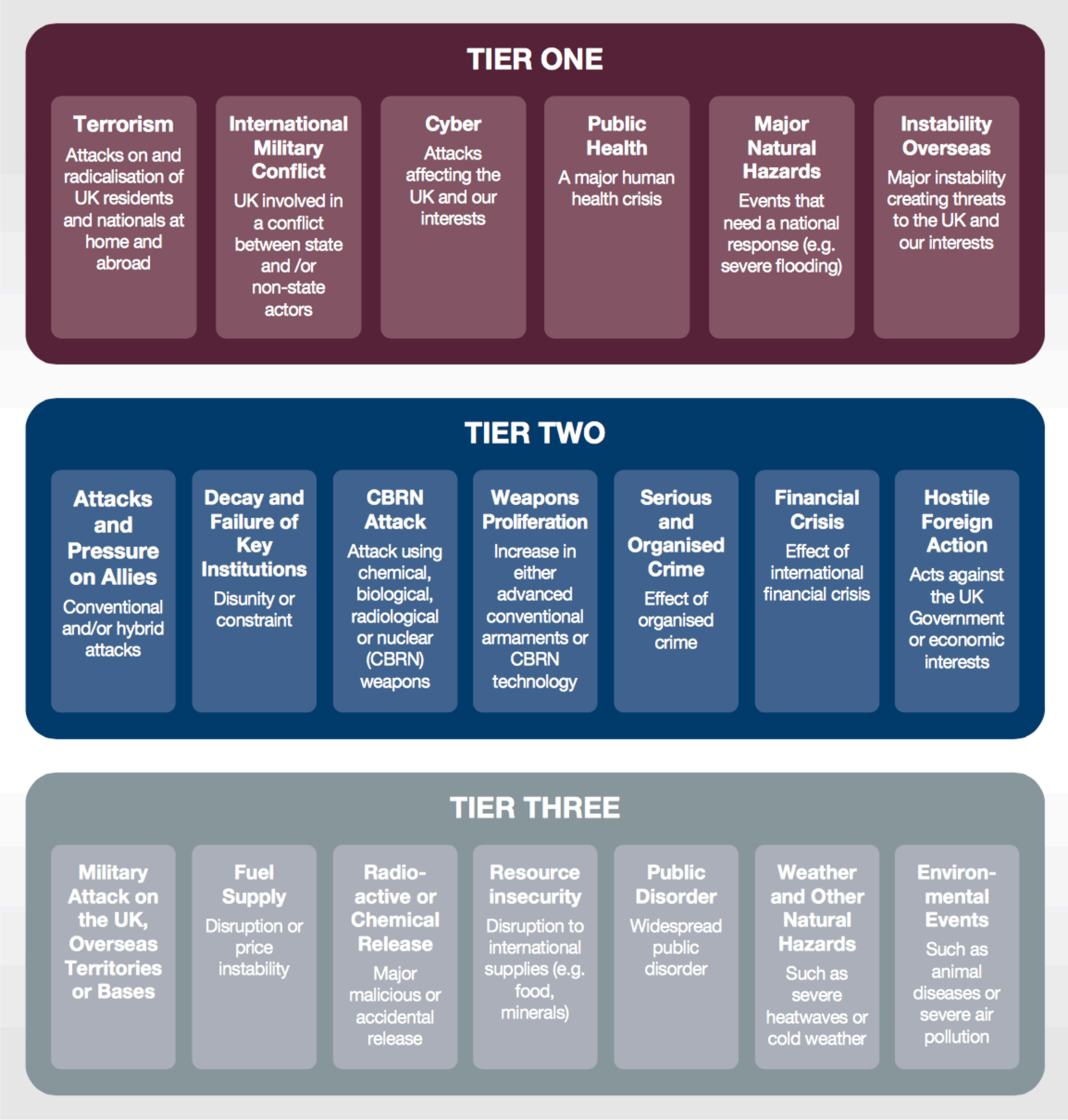
The cyber security is a considerable issue of extreme importance for United Kingdom.

Since the National Security Council places all the domestic and overseas risks that UK has to cope with into three tiers (see table 1 below), based on a judgment of the combination of both likelihood and impact, it can be observed that in recognition of the risks posed by cyber attacks, the cyber security issue is classified as a Tier One threat to the UK – that's the same level of terrorism or international military conflict.[50]

[49] National Security Strategy and Strategic Defence and Security Review 2015, *A Secure and Prosperous United Kingdom.* November 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf.

[50] *Chancellor Speech: Launching the National Cyber Security Strategy*, from HM Treasury and the Hon. Philip Hammond MP, November 1, 2016, https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy.

Table 1. Source: National Security Strategy and Strategic Defence and Security Review 2015, *A Secure and Prosperous United Kingdom.* November 2015, page 87.



TIER ONE

Terrorism Attacks on and radicalisation of UK residents and nationals at home and abroad

International Military Conflict UK involved in a conflict between state and /or non-state actors

Cyber Attacks affecting the UK and our interests

Public Health A major human health crisis

Major Natural Hazards Events that need a national response (e.g. severe flooding)

Instability Overseas Major instability creating threats to the UK and our interests

TIER TWO

Attacks and Pressure on Allies Conventional and/or hybrid attacks

Decay and Failure of Key Institutions Disunity or constraint

CBRN Attack Attack using chemical, biological, radiological or nuclear (CBRN) weapons

Weapons Proliferation Increase in either advanced conventional armaments or CBRN technology

Serious and Organised Crime Effect of organised crime

Financial Crisis Effect of international financial crisis

Hostile Foreign Action Acts against the UK Government or economic interests

TIER THREE

Military Attack on the UK, Overseas Territories or Bases

Fuel Supply Disruption or price instability

Radio-active or Chemical Release Major malicious or accidental release

Resource insecurity Disruption to international supplies (e.g. food, minerals)

Public Disorder Widespread public disorder

Weather and Other Natural Hazards Such as severe heatwaves or cold weather

Environ-mental Events Such as animal diseases or severe air pollution

In order to prove the effectiveness of the national response to cyber from the very top of government, the Chancellor of the Exchequer, Philip Hammond, in a public speech announced also the establishment of a permanent Cyber Committee, bringing together Cabinet Ministers from the

Foreign Office, Ministry of Defence, Home Office, Culture Media and Sport and Health among others.

The creation of this dedicated Committee has been a watershed in terms of innovation, because it remarks the willingness of the central government to work together – and with intelligence and security agencies – to deal with the cyber threats, as breaches of data, threats to military secrets, financial information and perhaps most important of all, to national infrastructure.[51]

Basically, the launched National Cyber Security Strategy 2016 – 2021, is based on three concepts: defense, deterrence and development. For defense, the British government intended to reinforce the defences, the critical infrastructures sectors (like transport and energy) and economy.

For deterrence, the British government meant to deter every individual, group, or terrorist organization that aims to steal, threaten or harm the UK's interests in cyberspace, especially through a massive investment in the development of offensive cyber capabilities, which are able to detect, trace and retaliate the cyber criminals.

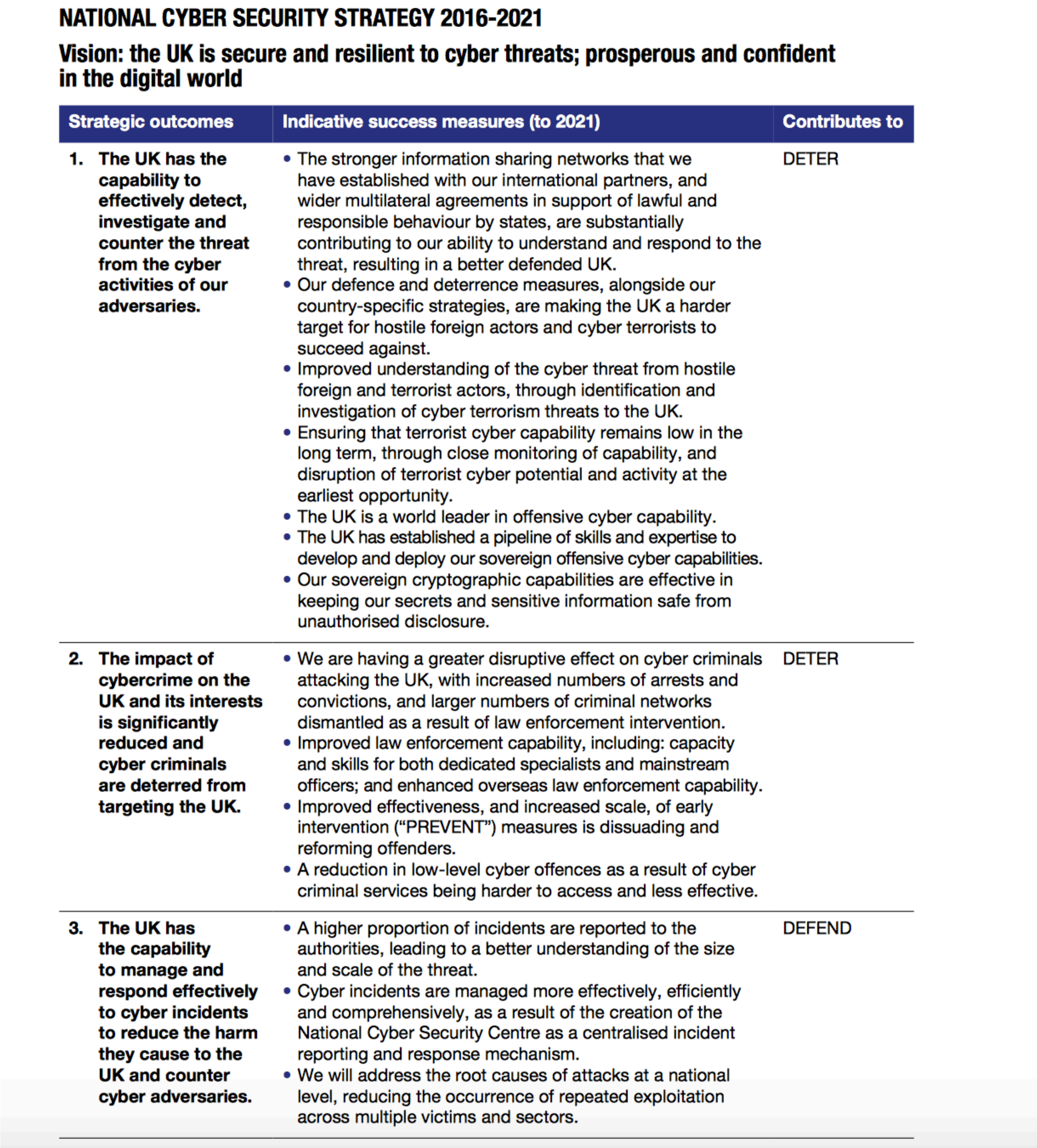
Lastly, for development, is implied the buildup of all those capabilities needed in the British economy and society to keep up with the threats also in the future. This can be performed endowing the next generation of students, experts and companies with the best tools and knowledge about cyber issue, so that they will become high skilled professionals.[52]

[51] *Chancellor Speech: Launching the National Cyber Security Strategy*, from HM Treasury and the Hon. Philip Hammond MP, November 1, 2016, https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy.

[52] Ibidem.

The figure in the next page (Table 2) sums up the vision of the United Kingdom enunciated in this National Cyber Security Strategy 2016 – 2021, the strategic outcomes and all the indicative success measures to 2021.

Table 2. *Source: National Cyber Security Strategy 2016 – 2021*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf



NATIONAL CYBER SECURITY STRATEGY 2016-2021

Vision: the UK is secure and resilient to cyber threats; prosperous and confident in the digital world

Strategic outcomes	Indicative success measures (to 2021)	Contributes to
1. The UK has the capability to effectively detect, investigate and counter the threat from the cyber activities of our adversaries.	• The stronger information sharing networks that we have established with our international partners, and wider multilateral agreements in support of lawful and responsible behaviour by states, are substantially contributing to our ability to understand and respond to the threat, resulting in a better defended UK. • Our defence and deterrence measures, alongside our country-specific strategies, are making the UK a harder target for hostile foreign actors and cyber terrorists to succeed against. • Improved understanding of the cyber threat from hostile foreign and terrorist actors, through identification and investigation of cyber terrorism threats to the UK. • Ensuring that terrorist cyber capability remains low in the long term, through close monitoring of capability, and disruption of terrorist cyber potential and activity at the earliest opportunity. • The UK is a world leader in offensive cyber capability. • The UK has established a pipeline of skills and expertise to develop and deploy our sovereign offensive cyber capabilities. • Our sovereign cryptographic capabilities are effective in keeping our secrets and sensitive information safe from unauthorised disclosure.	DETER
2. The impact of cybercrime on the UK and its interests is significantly reduced and cyber criminals are deterred from targeting the UK.	• We are having a greater disruptive effect on cyber criminals attacking the UK, with increased numbers of arrests and convictions, and larger numbers of criminal networks dismantled as a result of law enforcement intervention. • Improved law enforcement capability, including: capacity and skills for both dedicated specialists and mainstream officers; and enhanced overseas law enforcement capability. • Improved effectiveness, and increased scale, of early intervention ("PREVENT") measures is dissuading and reforming offenders. • A reduction in low-level cyber offences as a result of cyber criminal services being harder to access and less effective.	DETER
3. The UK has the capability to manage and respond effectively to cyber incidents to reduce the harm they cause to the UK and counter cyber adversaries.	• A higher proportion of incidents are reported to the authorities, leading to a better understanding of the size and scale of the threat. • Cyber incidents are managed more effectively, efficiently and comprehensively, as a result of the creation of the National Cyber Security Centre as a centralised incident reporting and response mechanism. • We will address the root causes of attacks at a national level, reducing the occurrence of repeated exploitation across multiple victims and sectors.	DEFEND

Strategic outcomes	Indicative success measures (to 2021)	Contributes to
4. Our partnerships with industry on active cyber defence mean that large scale phishing and malware attacks are no longer effective.	• The UK is harder to "phish", because we have large-scale defences against the use of malicious domains, more active anti-phishing protection at scale and it is much harder to use other forms of communication, such as 'vishing' and SMS spoofing, to conduct social engineering attacks. • A far larger proportion of malware communications and technical artefacts associated with cyber attacks and exploitation are being blocked. • The UK's internet and telecommunications traffic is significantly less vulnerable to rerouting by malicious actors. • GCHQ, Defence and NCA capabilities to respond to serious state-sponsored and criminal threats have significantly increased.	DEFEND
5. The UK is more secure as a result of technology products and services having cyber security designed into them and activated by default.	• The majority of commodity products and services available in the UK in 2021 are making the UK more secure, because they have their default security settings enabled by default or have security integrated into their design. • Government services are trusted by the UK public, because they have been implemented as securely as possible, and fraud levels against them are within acceptable risk parameters.	DEFEND
6. Government networks and services will be as secure as possible from the moment of their first implementation. The public will be able to use government digital services with confidence, and trust that their information is safe.	• Government has an in-depth understanding of the level of cyber security risk across the whole of government and the wider public sector. • Individual government departments and other bodies protect themselves in proportion to their level of risk and to an agreed government minimum standard. • Government departments and the wider public sector are resilient and can respond effectively to cyber incidents, maintaining functions and recovering quickly. • New technologies and digital services deployed by government will be cyber secure by default. • We are aware of, and actively mitigating, all known internet-facing vulnerabilities in government systems and services; • All government suppliers meet appropriate cyber security standards.	DEFEND

Strategic outcomes	Indicative success measures (to 2021)	Contributes to
7. All organisations in the UK, large and small, are effectively managing their cyber risk, are supported by high quality advice designed by the NCSC, underpinned by the right mix of regulation and incentives.	• We understand the level of cyber security across the CNI, and have measures in place to intervene, where necessary, to drive improvements in the national interest. • Our most important companies and organisations understand the level of threat and implement proportionate cyber security practices. • The UK economy's level of cyber security is as high as, or higher than, comparative advanced economies. • The number, severity and impact of successful cyber attacks against businesses in the UK has reduced, because cyber hygiene standards have been applied. • The UK has an improving cyber security culture, because organisations and the public understand their cyber risk levels, and understand the cyber hygiene steps they need to take to manage those risks.	DEFEND
8. There is the right ecosystem in the UK to develop and sustain a cyber security sector that can meet our national security demands.	• Greater than average global growth in the size of the UK cyber sector year on year. • A significant increase in investment in early stage companies.	DEVELOP
9. The UK has a sustainable supply of home grown cyber skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors, and defence.	• There are effective and clear entry routes into the cyber-security profession, which are attractive to a diverse range of people. • By 2021 cyber security is taught effectively as an integral part of relevant courses within the education system, from primary to post-graduate level. • Cyber security is widely acknowledged as an established profession with clear career pathways, and has achieved Royal Chartered Status. • Appropriate cyber security knowledge is an integral part of the continual professional development for relevant non-cyber security professionals, across the economy. • Government and the armed forces have access to cyber specialists able to maintain the security and resilience of the UK.	DEVELOP

Strategic outcomes	Indicative success measures (to 2021)	Contributes to
10. The UK is universally acknowledged as a global leader in cyber security research and development, underpinned by high levels of expertise in UK industry and academia.	• The number of UK companies successfully commercialising academic cyber research has increased significantly. There are fewer agreed and identified gaps in the UK's cyber security research capability, and effective action has been taken to close them. • The UK is regarded as a global leader in cyber security research and innovation.	DEVELOP
11. The UK government is already planning and preparing for policy implementation in advance of future technologies and threats and is 'future proofed'.	• Cross-government horizon scanning work and all-source assessment are integrated into cyber policy making. • The impact of cyber security is factored into all cross-government horizon scanning work.	DEVELOP
12. The threat to the UK and our interests overseas is reduced due to increased international consensus and capability towards responsible state behaviour in a free, open peaceful and secure cyberspace.	• Enhanced international collaboration reduces cyber threat to the UK and our interest overseas; • A common understanding of responsible state behaviour in cyberspace; • International partners increased their cyber security capability; and • Strengthened international consensus on the benefits of a free, open, peaceful and secure cyberspace.	INTERNATION-AL ACTION AND INFLUENCE
13. UK Government policies, organisations and structures are simplified to maximise the coherence and effectiveness of the UK's response to the cyber threat.	• The Government cyber security responsibilities are understood and its services are accessible. • Our partners understand how best to interact with Government on cyber security issues	CROSS-CUTTING

2.1.2. Case study: Estonia

The case of Estonia is a very singular one. Estonia gained relevance in the international scenario because of the cyber attacks that endured in 2007.

The attacks –mainly distributed in two phases, the first one characterized by regular DoS (denial of service) attacks, the second one, more massive, involving DDoS (distributed denial of service) attacks hijacking more than 85,000 computers [53] – were a reaction to the relocation of a Soviet World War II memorial.

Those cyber attacks targeted Estonian governmental agencies, media channels, private websites, as well as were able to render inoperative the online services of two Estonian biggest banks[54].

The Estonian CERT-EE (Computer Emergency Response Team of Estonia) became the coordinating body for response to the attacks and in a certain way, it was able to reduce the impact of them. However, it lacked the authority to enforce its recommendations on all parties involved[55].

Even if, according to some security analysts, the size of the attacks were not groundbreaking and the Estonian government declared shortly after the attacks that the country's normal daily activities were not paralyzed, surely this event shed light on an important issue: the riskiness of the cyberspace[56].

[53] Eneken Tikk, Anna-Maria Talihärm, *International Cyber Security, Legal & Policy Proceedings* 2010, pages 44-45, CCD COE Publications.

[54] Ibidem.

[55] Evron, Gadi, *Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War*, Georgetown Journal of International Affairs, Winter/Spring 2008, page 123.

[56] Eneken Tikk, Anna-Maria Talihärm, *International Cyber Security, Legal & Policy Proceedings* 2010, CCD COE Publications.

The Estonian government, after that episode, modified the national legislative, organizational and policy framework, in order to include the cyber issue in the National Security Concept of Estonia[57] that was then approved by the Parliament in 2010.

As part of this broad review, in 2009 the Emergency Act was issued and several structures were reorganized while others were created to serve the purpose of what later was stated in the National Security Concept.

The new organizational framework revolves around the organization of the Estonian Informatics Centre and its modernization, the definition of the roles of the CERT-EE –which is still subordinated to the Ministry of the Economic Affairs and Communications (MAEC) –the creation of the Critical Information Infrastructure Protection (CIIP) Department, and the creation of the Cyber Defence League.

The Estonian Informatics Centre is a state agency administered by the MAEC, and its core tasks are: the coordination of execution of development plans for Estonian information society, development and administration of the components supporting state information systems and ensuring their security, and coordinating incident handling Estonian in computer networks[58].

The Centre is made up of six departments, among them there are the CERT-EE and the Critical Information Infrastructure Protection Department. Recently, the Centre has been modernized and upgraded from a ministry-administered state agency into a government agency with autonomous executive powers, namely monitoring and regulating undertakings that own and

[57] National Security Concept of Estonia 2010, available at https://www.eda.europa.eu/docs/default-source/documents/estonia---national-security-concept-of-estonia-2010.pdf.

[58] Eneken Tikk, Anna-Maria Talihärm, *International Cyber Security, Legal & Policy Proceedings* 2010, page 61, CCD COE Publications.

run critical information infrastructure, as well as supervising other governmental agencies dealing with information infrastructure[59].

The objective of this renovation is to better qualify the Centre to enforce the principles enunciated in the National Cyber Security Strategy and guaranteeing its efficient implementation. As a consequence of the adoption of the 2009 Emergency Act, the CIIP Department was created in order to deal with the protection of important IT systems of the public and private sector alike, coordinating general prevention and response activities while the owners of each vital service concerned remain responsible for the daily defence of their systems.

The CIIP Department will also be able to give recommendations on improving the defence of information systems[60].

Another notable body set up after the promulgation of the 2009 Emergency Act is the Cyber Defence League, operating as part of the Defence League, a voluntary military national defence organization founded already in 1918 whose traditional aim has been enhance the readiness of the nation to defend its independence and its constitutional order, but supporting civil structures such as rescue services and police, as well[61].

The framework in which the Cyber Defence League (CDL) operates it's basically the same of the Defence League's; its mission is to protect the high-tech lifestyle of the country, defending information infrastructure and working to raise awareness, share best practices and create a network of specialists that are able to support mitigation efforts in the case of a cyber incident.

[59] Ibidem, page 63.

[60] EIC creates unit for defence of critical information systems. Press release by the Estonian Informatics Centre, 30 Sept. 2009, http://www.ria.ee/eic-creates-unit-for-defence-of-critical-information-systems.

[61] Eneken Tikk, Anna-Maria Talihärm, *International Cyber Security, Legal & Policy Proceedings* 2010, page 64, CCD COE Publications.

The CDL may be used in emergency response as well as preventing or deterring acts of terrorism. However, in any case has always to follow the procedure established by the Estonian government.[62]

The 2009 can be recognized as a meaningful year for Estonia because a lot of relevant decisions were taken in order to develop cyber security. To better serve this purpose, cyber security was firstly divided in three categories, such as critical infrastructure and vital services, cyber crime and national defence.

Secondly, for the development of cyber security, it was decided that attention should be given also to educating people and increasing their awareness, by shaping the legal space and international relations.

Furthermore, in 2009, the Cyber Security Council was established at the Security Committee of the Government of the Republic. The Secretary General of the Ministry of Economic Affairs and Communications chairs the Council and its task is to contribute to smooth co-operation between various institutions and conduct surveillance over the implementation of the goals of the Cyber Security Strategy.[63]

The Estonian Cyber Security Strategy 2014 – 2017, lays down four important objectives:

- The implementation of a comprehensive system of security measures, consisting of different levels to ensure cyber security at national level.
- Estonia has to be seen as a country characterized by a very high level of information security competence and awareness.

[62] Ibidem.

[63] Cyber Security, Republic of Estonia, Ministry of Economic Affairs and Communications, available at https://www.mkm.ee/en/objectives-activities/information-society/cyber-security#cyber-crime1

- Proportionate legal regulations serve to support the secure and extensive use of information systems.
- Estonia is one of the leading countries in international co-operation to enhance cyber security.[64]

The vision that emerges from these objectives is that Estonia is a country able to ensure national security and support the functioning of an open, inclusive and safe society.

Thus, the four-year main goal of the Cyber Security Strategy 2014 – 2017 is to increase cyber security capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace.

This principal aim is then structured in five sub-goals, which are the followings:

1) Ensuring the protection of information systems underlying important services

The functioning of the Estonian state and society, the economic and social wellbeing of every person, their life and health, increasingly depend on the security of the systems and services.

One of the main aims of the strategy is to describe methods for ensuring the uninterrupted operation and resilience of vital services, and the protection of critical information infrastructures against cyber threats.

2) Enhancing of the fight against cybercrime

The economic damage deriving from cybercrime reduces trust in digital services, and, in a worst-case scenario, could lead to loss of life. Greater awareness among the general public about cyber security risks helps to prevent cybercrimes.

[64] Ibidem.

Greater awareness is achieved by addressing cyber-related topics at all levels of education and informing people based on research and analysis of secure behaviors.

3) Development of national cyber defense capabilities
Civil, military, and international cooperation based on the resources at the disposal of the state must also function adequately in cyberspace – with regards to warning, deterrence and active defense.

4) Estonia manages evolving cyber security threats
To maintain and improve its cyber security capability, Estonia will adopt independent cyber security solutions, which are backed by cyber security training and training opportunities, research and development and entrepreneurship. In order to ensure the sustainability of solutions, the state acts as a smart contractor, and supports the export of cyber security solutions.

5) Estonia develops cross-sectoral activities
To improve the capabilities necessary for combating cyber threats, a number of overarching objectives are addressed. Adjusting the legal framework and developing cyber foreign policy are vital for protecting critical services, the fight against cybercrime, as well as for designing national defense in cyberspace.[65]

[65] *Estonian Cyber Security Strategy 2014 – 2017*, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

2.1.3. Case study: United States of America

The cyber issue is particularly familiar to United States.

The origins of Internet are found in ARPANET, a computer network established in September 1969 in the USA by the Advanced Research Projects Agency (ARPA). ARPA was created in 1958 by the US Department of Defense in order to expand and develop the research, especially in the aftermath of the Soviet Union's technology overtaking, which launched the first satellite (Sputnik) in 1957, conquering the American skies: when NASA succeeded in the management of space programs, ARPA took control of all the long-term scientific research in the military.

However, as the Secretary of Defense Ashton B. Carter declared, there is no way the ARPA researchers could have imagined how their creation would change our world. What began as a tool for scientists to share information grew quickly into the global network of computers, systems and data that nowadays we call Internet.

The United States, like many other countries in the world today, relies heavily on the Internet and the systems and data of cyberspace for a wide range of critical services. This reliance is the reason why the country is basically vulnerable in case of a cyber attack and why a timely action supported by a proper National Cyber Security Strategy is compelling and vital.[66]

President Obama has identified cyber security as one of the most serious economic and national security challenges that United States has to face and at the same time one that U.S. as a government or as a country, are not adequately prepared to counter. Thus, shortly after taking

[66] *The DoD Cyber Strategy*, 17 April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

office, the President ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing America's digital infrastructure.[67]

The U.S. security is managed by the Department of Defense (DoD), which is responsible for deterring all kinds of attack, including the cyber ones, and defending the homeland from those attacks and any adversary that seeks to harm U.S. national interests.

To carry out this aim, the Department of Defense has developed a wide range of capabilities that combined with diplomatic, informational, military, economic and law enforcement tools, and has woven together a series of partnerships with international actors and private sector in order to build new and stronger alliances while ensuring a global strategic stability.[68]

In this perspective, the DoD has released a remarkable document: the *Department of Defense Cyber Strategy*, in April 2015, with the aim of guiding the development of DoD's cyber forces and strengthen its cyber defense and cyber deterrence posture.

The document focuses on building cyber capabilities and organizations for DoD's three cyber missions: defend DoD networks, systems, and information; defend the United States and its interests against cyber-attacks of significant consequence; and provide integrated cyber capabilities to support military operations and contingency plans.

[67] *The Comprehensive National Cybersecurity Initiative,* The White House, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.
[68] *The DoD Cyber Strategy*, 17 April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

The strategy is made up of five strategic goals and establishes specific objectives for the Department of Defense to achieve over the next five years and beyond. [69] These goals are the followings:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations.

2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.

3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence.

4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.

5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.[70]

But what drove DoD to develop a new cyber strategy? Basically, three major drivers can be recognized.

First is the increasing harshness and sophistication of the cyber threat to U.S. interests, including DoD networks, information, and systems. It is known that the Department of Defense has the largest network in the world and it must take aggressive steps to defend its own networks, secure its data, and mitigate risks to its missions.

[69] *Fact Sheet: The Department of Defense (DoD) Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf.

[70] *The DoD Cyber Strategy*, 17 April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Second, as previously pointed out, in 2012 President Obama directed DoD to organize and plan to defend the nation against cyber-attacks of significant consequence, in concert with other U.S. government agencies. This new mission required new strategic thinking.[71]

Lastly, in response to the threat, in 2012 DoD began to build a Cyber Mission Force (CMF) to carry out DoD's cyber missions. The CMF has a unique role within the Department. Once fully operational, the CMF will include nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components.

The Cyber Mission Force represents a major investment by the Department of Defense and the United States as whole, and a central aim of this strategy is to provide clear guidance for the CMF's development.[72]

The Department of Defense Cyber Strategy is a comprehensive and very ambitious document, which obviously requires a high level of expertise in the management of the resources that should be conveyed to the realization of its goals. In fact, aligning and managing the appropriate resources is fundamental for ensuring progress along with a more-than-ever close cooperation among the American partners – U.S. agencies, international allies, private sector.

Only in this way, the United States can defend their interests while keeping pace with the challenges posed by the digital age.

[71] *Fact Sheet: The Department of Defense (DoD) Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf.
[72] *The DoD Cyber Strategy*, 17 April 2015, page 6, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

2.1.4. Case study: Canada

The digital era we are living and witnessing is a unique phenomenon that entangles all the developed countries and combines to bring about many consequences for them.

Canada, as one of the wealthiest countries in the world could not be exempted by all those outcomes, which are both positive and negative.

For this reason, in order to cope with the negative side effects of the Cyber Age, Canada, as many other countries, has developed its own National Cyber Security Strategy. The Canada's Cyber Security Strategy, launched in 2010, represents the foundation of the Canadian government's commitment against the cyber threat.

The Strategy focus firstly on the economic reliance that ties the country to the massive use of technology. Indeed, it shows how, in 2007, Canadian online sales, for example, were estimated at $62.7 billion and that the 87% of Canadian businesses used the Internet. Canadian businesses moved quickly to adopt the most modern digital applications, including next generation and mobile technologies.

Canada's governments have also become increasingly dependent on the Internet; as a matter of fact, the federal Government alone now offers more than 130 commonly used services online, including tax returns, employment insurance forms and student loan applications.[73]

The positive economic performance of the country also depends much on the strategic exploitation of the cyber tools, that's why it is important for Canada to counter the cyber threats: it is a way of ensuring safety while preserving the economic stability as well.

[73] Public Safety – Canada, Canada's Cyber Security Strategy, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.

Basically, the cyber threats identified by Canada are the same targeted by other countries, namely those cyber attacks that include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information.[74]

Cyber attacks can be perpetrated from terrorist groups or can be instruments of most traditional actions of cyber crime, such as identity theft, money laundering and extortion.[75]

Anyway, the cyber threats can come also from most advanced military activities and from the intelligence services of foreign states that try to breach the networks in order to gain every sort of advantage in economic, politic and military terms. These kind of attacks are very dangerous because are often well resourced and efficient; at the same time, it is also very hard to detect who is really behind these attacks, producing unequivocally difficulties at diplomatic level, that may undermine the global stability.

The 2010 Canada's Cyber Security Strategy has been structured to meet five requirements and it has been built on three pillars.

The requirements can be summarized as follows:

1) It has to reflect the Canadian values such as the rule of law, accountability and privacy.

2) It has to allow continual improvements to be made to meet emerging threats.

3) It has to integrate activities across the Government of Canada.

[74] Canada's Cyber Security Strategy, 2010, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

[75] Ibidem.

4) It has to emphasize partnerships with Canadians, provinces, territories, business and academe.

5) It has to build upon the Canadian close working relationships with its allies.[76]

Furthermore, three core pillars underpin the 2010 Canada’s Cyber Security Strategy:

1. Securing Government systems – Canadians trust Government with their personal and corporate information, and also trust Government to deliver services to them. They also trust that the Government will act to defend Canada's cyber sovereignty and protect and advance the national security and economic interests. The Government 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 economic prosperity and Canadians' security depend on the smooth functioning of systems outside the Government. In cooperation with provincial and territorial governments and the private sector, the Government will support initiatives and take steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors.

3. Helping Canadians to be secure online – 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.[77]

In this discourse, once again, cooperation is the keyword: in order that the strategy will be implemented efficiently, cooperation among those governmental bodies and agencies that work in

[76] Ibidem.
[77] Ibidem.

the security field is mandatory. Also, at the federal level, communication, info-sharing and collaboration between the provinces and the territories it would be definitely an asset.

Last but not least, the non-governmental actors play a pivotal role, as well; those actors are non-governmental organizations, private sector and individuals. Each of these categories of actors can contribute positively in the enhancement of the national cyber security, because each of them possesses unique features and capabilities that, if combined with others, may result in a valuable outcome to secure Canada and increase its productivity and prosperity.

In conclusion, it can be surmised that cyber security is believed to be a shared responsibility, one in which Canadians, their governments, the private sector and our international partners all have a role to play. The Strategy reflects this shared responsibility, and since the implementation will be a collective effort, much of its success will depend on the ability for everybody to work together.[78]

2.2. The EU Cyber Security Strategy

The European Union started to tackle the cyber security issue in 2000, but it is important to underline that the word "cybersecurity" did not appear in the official documents until 2008. In fact, until that year, all the documents spoke about cybercrime, data protection and critical infrastructures protection, in generic terms.

[78] Ibidem.

In 2001, the European Commission issued a document centered around the definition of the so-called NIS, Network and Information Security, which aimed to realize a pertinent European policy.[79] This document expresses the definition of the NIS and a general framework of all those threats that may have an impact, in terms of security, on the NIS itself.

In 2003, the European Union has developed its own security strategy without mentioning the concept of "cybersecurity" and pinpointing an "interdependence" among several infrastructures' sectors (transportation, energy, ITC, and so on) that exposes the European Union to vulnerability.[80] This EU security strategy drafted in 2001 was never modified or updated, leaving the 2003 EU Security Strategy in force.[81]

However, the following year 2004 was a turning point for the development of the European cyber security: indeed it saw the approval of the EU regulation 460/2004 [82] for the establishment of the European Union Agency for Network and Information Security (ENISA from the abbreviation of European Network and Information Security Agency), that took place officially in 2005.

ENISA has to assist the Commission, the Member States and the business community in meeting the requirements of network and information security, including present and future EU legislation. It has to contribute to the promotion of a new culture of security, so that the cyber security issue would be better faced both at the European and national level.

[79] Commissione Europea, *Sicurezza delle Reti e dell'Informazione: proposta di un approccio strategico europeo*, COM 2001/298, 6 Giugno 2001.

[80] Consiglio dell'Unione Europea, *Un Europa sicura in un mondo migliore. Strategia Europea in materia di sicurezza*. 12 Dicembre 2003, pag. 2.

[81] Consiglio dell'Unione Europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione* (S407/08), 11 Dicembre 2008.

[82] Regolamento (CE) n. 460/2004 del 10 marzo 2004, che istituisce l'Agenzia Europea per la sicurezza delle reti e dell'informazione, art. 1.1.

The agency, ultimately, plays a role of centre of expertise, assistance and consulting for all Member States and EU Institutions, with the aim of fostering a general development in matter of cyber security and increasing the level of competencies.[83]

The principal activity of ENISA is identifying the *best practices* and elaborating documents and guidelines to share with the Member States in order to keep the European Union updated about the cyber issue. In this way, it can also prepare the Member States in giving a homogenous response to the cyber threat, and enabling them to implement the most advanced practices.

From this perspective, the commitment of the agency is outstanding and the issuing in 2012, of the National Cyber Security Strategies manual proves it: the manual is addressed to all those Member States who are still not equipped of the necessary tools to manage efficiently the cyber security issue.

This guide is also addressed not only to the public sector but to the private one as well, analyzing in details every single step considered fundamental for the construction of a national cyber security strategy.[84]

The work of ENISA is extremely important for what concerns the promotion of cooperation in the cyber security field. For this reason it has been established an incident reporting mechanism, to incentivize the Internet and Service Providers (ISP) in communicating, publicly and promptly, to the European Institutions and other Member States the cyber attacks endured.

Through this *info-sharing mechanism,* multiple actors would be involved: EU Institutions, ENISA, national authorities, providers and users. But, at the end, only the EU Commission and

[83] Ibidem, art. 2.1.

[84] ENISA, National Cyber Security Strategies. Practical Guide on Development and Execution. December 19, 2012. https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

ENISA would be entitled to adopt the best security measures and address them to the national authorities and to the providers.[85]

Basically, ENISA intends to put the European Institutions at the top of a decisional and operative process, so that the European Union would have a supranational guide in charge of taking the lead in emergency cases.

However, the info-sharing mechanism, is the major weakness of the ENISA's work: the Member States' reluctance in publicly revealing the attacks endured is still very high, mostly because they prefer not to show to the international community their own deficiencies, in order to preserve their *status*.

That's why ENISA strives for promoting a new culture of information and network security based on principles of transparency, reciprocal trust and accountability.

Up to date, ENISA organized two exercises, called "Cyber Europe", in 2010 and in 2012.

The 2010 exercise was based on an attack-simulation against the Internet Interconnected Site (IIS), and it was characterized by the increasing loss of internet interconnectivity among all Member States participating at the exercise. The purpose of the exercise was to trigger the cooperation among Member States for reactivating the proper functioning of the Internet throughout Europe.

The 2012 exercise's scenario was slightly more complex: it focused on a set of cyber incidents on large scale involving all the participating States. This exercise represented a big leap

[85] Claudia Cencetti, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014. http://www.iai.it/sites/default/files/iaiq_12.pdf.

forward because beyond the 25 countries, which took part in it, there were lots of representatives of the private and industrial sector as well. This clearly has marked a progress both in terms of *know how* and cooperative level.

The commitment of the European Union for a safer cyberspace is noteworthy and it traces back to 2006 when the European Commission adopted the European Programme for Critical Infrastructure Protection (EPCIP) and it also created a European Reference Network for Critical Infrastructure Protection (ERN-CIP), to foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities.

The ERN-CIP aims to link together existing European laboratories and facilities, in order to carry out critical infrastructure-related security experiments and test new technology, such as detection equipment.[86] The European Union approved and consequently adopted several documents dealing with the internal security of the Union and preset many goals to achieve it.

The priority, however, is increasing the security level in the cyberspace for both citizens and businesses.

Essentially, to accomplish this goal the EU action cannot avoid to "interfering" with the Member States' national authorities: indeed, first of all, a major *Europeanization* of the legal prosecution procedures of the criminals is considered an advantage in the fight against cybercrime.

[86] European Commission website, Critical Infrastructure Section, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

Then, the creation of national CERTs (Computer Emergency Response Team) designated to work along with CERT-EU would boost the cooperation and paving the way to a greater info-sharing mechanism.[87]

For this reason, between 2012 and 2013, the EU Commission upheld many changes. The European Centre for Cybercrime was instituted, substituting the old Hi-Tech Crime Centre.

The EU Commission, thus, asked officially to the Europol to create the European Cyber Crime Centre (EC3), which became the focus of the European battle against cybercrime. The EC3 offering support to the Member States and to the European Institutions in developing analytical and technical capabilities to tackle the cyber-challenges and promoting the international cooperation among all partners, became the landmark for cybercrime in Europe.

Furthermore, the EU set up the CERT-EU (Computer Emergency Response Team of the European Union), the European body entitled to monitor the cyber-threats and response to cyber-attacks. The CERT-EU is made up of individuals with high expertise in this field also coming from European Institutions and collaborates with the national CERTs of all Member States.

At this point, it is crucial that all Member States play their role adapting their legal framework to that of the EU, founding similar structures and facilitating the dialogue.[88]

However, to date, just 23 Member States are provided with their national CERT.[89]

In 2013, the EU Commission and the Higher Representative released the EU Cyber Security Strategy: it was the first EU comprehensive policy document in this area. It covers the internal

[87] ENISA, National Cyber Security Strategies. Practical Guide on Development and Execution. December 19, 2012. https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.
[88] Claudia Cencetti, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014, pag. 35. http://www.iai.it/sites/default/files/iaiq_12.pdf.
[89] Ibidem, pag. 35-36.

market, justice and home affairs and foreign policy angles of cyberspace. The Strategy is accompanied by a legislative proposal to strengthen the security of the EU's information systems.

This will encourage economic growth as confidence in buying online and using the internet grows.

It also makes clear the principles for EU international cyberspace policy, which are the followings:

1) Freedom and openness: the strategy outlines the vision and principles on applying core EU values and fundamental rights in cyberspace.

2) The EU's laws, norms and core values apply as much in cyberspace as in the physical world: responsibility for a more secure cyberspace lies with all players within the global information society, from citizens to governments.

3) Developing cyber security capacity building: the EU engages with international partners and organizations, the private sector and civil society to support global capacity building in third countries. This includes improving access to information and to an open Internet, and preventing cyber threats.

4) Fostering international cooperation in cyberspace: preserving open, free and secure cyberspace is a global challenge, which the EU is addressing together with relevant international partners and organizations, the private sector and civil society.[90]

The purpose of the EU is that of safeguarding an online environment providing the highest possible freedom and security for the benefit of everyone. While acknowledging that it is

[90] *EU International Cyberspace Policy*, https://eeas.europa.eu/topics/eu-international-cyberspace-policy_en.

predominantly the task of Member States to deal with security challenges in cyberspace, the Strategy proposes specific actions that can enhance the EU's overall performance.

These actions are both short and long term, they include a variety of policy tools[91] and involve different types of actors, be it the EU institutions, Member States or industry.

The EU vision presented in this Strategy is articulated in five strategic priorities, which address the challenges highlighted above:

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.

In July 2016, the European Parliament adopted the “Directive on security of network and information systems” (the NIS Directive) and such Directive entered in force in August, leaving to Member States 21 months to transpose it into their national laws.

[91] Ibidem.

This Directive is of outstanding relevance, because provides legal measures to boost the level of cyber security in the EU by ensuring:

- Member States preparedness by requiring them to be appropriately equipped (for example, via a Computer Security Incident Response Team and a competent national NIS authority)

- Cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set a CSIRT Network, for promoting effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
- A culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive. [92]

This Directive presents those measures needed to achieve a high common level of security of network and information systems within the Union. This is a crucial step to take in order to improve the functioning of the internal market, which is the main objective of the Directive.

[92] The Directive on security of network and information systems (NIS Directive), July 2016. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

The proper functioning of many pillar-systems, indeed, supports the functioning of the internal market, and among them certainly there is the security system.[93]

It is important to remark that even if politicians decide the priorities, the real innovation can come just from the private sector. Thus, is very important for every Member State to foster the Public-Private Partnership (PPP) and incentivize this type of collaboration.

In order to align with this scope and to let the Member States meet the minimum common requirements in terms of security, the Strategy proposes also a set of legislative measures to adopt at national level.

Nevertheless, the differences among Member States are still several: there are countries particularly developed for what concerns the cyber-security issue –as, for example, U.K. or Estonia– and others that are still striving for achieving good results because this issue is not properly dealt with.[94]

In conclusion it can be said that both the Strategy and the NIS Directive assume an important concept: the advocacy of a perspective that climbs out both the national and European borders in pursuance of a valuable cooperation and the establishment of all those indispensable tools required for confidence building amidst Member States. This definitely would be a big step towards the achievement of a comprehensive European cyber-security.

[93] Directive (Eu) 2016/1148 of the European Parliament and of the Council of 6 July 2016. http://eur-lex.europa.eu/legal-content/EN-IT/TXT/?uri=CELEX:32016L1148&from=EN.

[94] Claudia Cencetti, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014, pag. 48-49. http://www.iai.it/sites/default/files/iaiq_12.pdf.

2.3. Italy and Cyber Security: Guidelines and Issues

Once illustrated the National Cyber Security Strategy of the four countries that have given a decisive contribute to the cyber issue and having analyzed also the topic from a European perspective, it is important to focus on the Italian position related to the cyber security issue.

Before focusing on the guidelines and the challenges that Italy has to face, a brief digression can spotlight the major developments achieved by Italy in this area.

During the ‘90s, cyber crimes were officially recognized as legally prosecutable and it was founded a “child agency” of the State Police (*Polizia di Stato*) to tackle these crimes, which is the so-called *Polizia Postale* (Post and Telecommunications Police).

The 2000’s were years during which Italy raised its awareness towards the existence of serious potential threats posed by the cyber challenge. Italy modified its legislation in order to introduce new relevant bodies entitled to deal with the national cyber-security and new laws that would have protect both the information managed by the Public Administration and those belonging to critical infrastructures.

Unfortunately Italy started to adapt its national legislative framework to the emerging cyber challenges just in 2011 when transposed in the Italian judicial system much of the European directives, in order to harmonize the Italian legislative framework with that of other Member States, with the aim of promoting the intra-European cooperation.

Two years later, in 2013, Italy launched the National Cyber Security Strategy which is made up of two documents: Italy’s National Strategic Framework for Cyberspace Security and Italy’s National Plan for Cyberspace Protection and ICT Security.

With remarkable delay compared to other developed European countries, in 2014 Italy finally endowed its system with an official strategy meant to protect the cyberspace.[95]

The National Strategic Framework for Cyberspace Security is a four-year program (2014-2017), it aims at enhancing the capabilities of the country to face the cyber challenges; it delineates who are the institutional actors involved in the national cyber security, which are the threats, it underlines the importance of critical infrastructures protection as a State's obligation and it shows the proper measures to adopt for an adequate policy of ITC security.

Italy's National Plan for Cyberspace Protection and ICT Security is the *operative* document: its goal is to implement what is declared in the National Strategic Framework in a range of two-years time (2014-2015).

To carry out this, it established 11 operational guidelines and it stressed the value – especially in economic terms – of a project that takes in consideration both multilateral and bilateral partnerships between multiple actors, including the private stakeholders.

The 11 operational guidelines are the followings:

1) Strengthening of intelligence, police, civil protection and military defense capabilities.

2) Enhancement of the organization, coordination and dialogue between national private and public stakeholders.

3) Promotion and dissemination of the Culture of Cybersecurity. Education and training.

[95] Claudia Cencetti, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014, pag. 93-94. http://www.iai.it/sites/default/files/iaiq_12.pdf.

4) International cooperation and exercises.

5) Implementation of national CERT, CERT-PA and ministerial CERTs.

6) Promotion of ad hoc legislation and compliance with international obligations.

7) Compliance with standard security requirements and protocols.

8) Support to industrial and technological development.

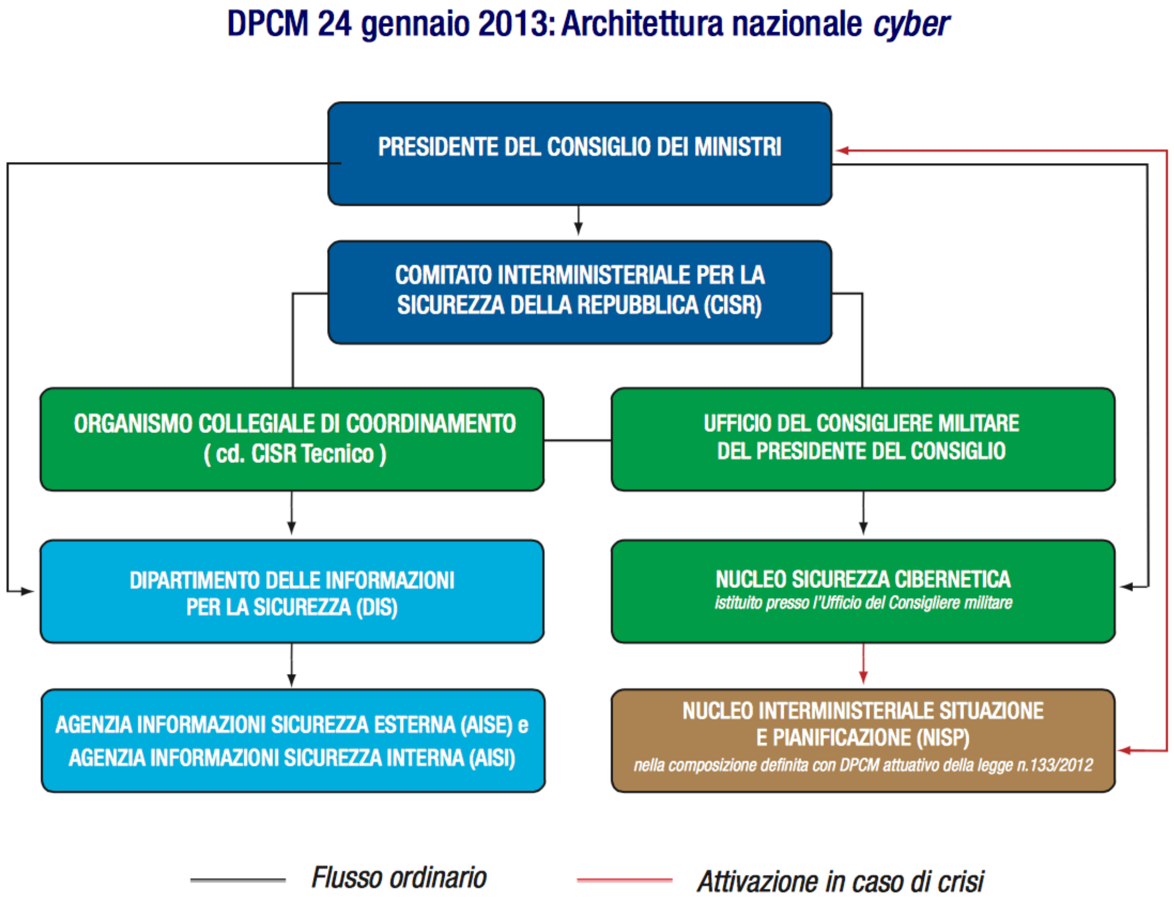
9) Strategic communication.

10) Resources.

11) Implementation of a national system of Information Risk Management.[96]

[96] Presidency of the Council of Ministers, *The National Plan for Cyberspace Protection and ICT Security*, December 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf

The Italian national architecture designated to cyber-security is showed in the Figure 1 below (Source: Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza*, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/relazione-2013.pdf)


DPCM 24 gennaio 2013: Architettura nazionale *cyber*
PRESIDENTE DEL CONSIGLIO DEI MINISTRI
COMITATO INTERMINISTERIALE PER LA SICUREZZA DELLA REPUBBLICA (CISR)
ORGANISMO COLLEGIALE DI COORDINAMENTO (cd. CISR Tecnico)
UFFICIO DEL CONSIGLIERE MILITARE DEL PRESIDENTE DEL CONSIGLIO
DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA (DIS)
NUCLEO SICUREZZA CIBERNETICA
istituito presso l'Ufficio del Consigliere militare
AGENZIA INFORMAZIONI SICUREZZA ESTERNA (AISE) e AGENZIA INFORMAZIONI SICUREZZA INTERNA (AISI)
NUCLEO INTERMINISTERIALE SITUAZIONE E PIANIFICAZIONE (NISP)
nella composizione definita con DPCM attuativo della legge n.133/2012
Flusso ordinario
Attivazione in caso di crisi

Let's see briefly the role of each member of this structure.

The President of the Council of Ministers is at the top of the hierarchy and is entitled to elaborate both the National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace Protection and ICT Security, following the proposals of the inter-ministerial committee CISR, *Comitato Interministeriale per la Sicurezza della Repubblica*.

The CISR covers multiple tasks: promotion of info-sharing and *best practices*, fostering the Public-Private Partnership, supporting activities of major international events, especially those organized by the EU or NATO, that are relevant to Italy and can guarantee its participation.

Among all its duties, CISR has to communicate the proper directives to follow to: DIS, the Department for Information Security (*Dipartimento delle Informazioni per la Sicurezza*) and to the two agencies entrusted of managing the information security externally and internally, which are respectively AISE (*Agenzia Informazioni Sicurezza Esterna*) and AISI (*Agenzia Informazioni Sicurezza Interna*).

The DIS it has to send the relevant information in terms of cyber-security out to another organism: the NSC (*Nucleo Sicurezza Cibernetica*), an operational core functional 24/7, which belongs to the Office of the Military Advisor to the Prime Minister (*Ufficio del Consigliere Militare*).

The NCS is a sort of national reference point for cyber issues affecting bilateral and multilateral relations between Italy and other States, European Institutions and international organizations such as NATO or UN.

NCS has the duty of obtaining information and signals from abroad, and in case of an imminent danger, alerting the internal bodies committed to national security. If it would happen an emergency crisis, the NCS would activate a special force that directly oversees: the so-called NISP (*Nucleo Interministeriale Situazione e Pianificazione*).

NISP is an inter-ministerial nucleus appointed to supervise the correct management of a cyber crisis from public and private institutions and administrations. If believed necessary, the NISP can avail itself of the aid of the national CERT.[97]

Cyber security is increasingly regarded as a horizontal and strategic national issue affecting all levels of society. Italy, as Member of a supranational institution like the European Union, is subject to several confrontations.

To evaluate both Italy's improvements and lacks in cyber-security, in comparison with other European Member States or with the countries analyzed previously in the case studies, it is helpful the analysis of the ENISA's Guide about National Cyber Security Strategies.[98]

This document is meant to support the Member States in harmonizing their legislation in the cyber field and it's based on a two-phases model: development & implementation and evaluation & adjustment.

Italy, nowadays it seems to be better framed in the first phase, which is the only one that will be taken in consideration.

This phase focuses on 18 stages:

1) Establish vision, purpose, objectives and priorities.
2) Follow a *risk assessment* approach.
3) Carry out a survey of policies, regulations and already existing capabilities.
4) Develop a clear governance structure.

[97] Claudia Cencetti, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014, pag. 86. http://www.iai.it/sites/default/files/iaiq_12.pdf.
[98] ENISA, *National Cyber Security Strategies*, May 8, 2012, https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.

5) Identify and involve all stakeholders.

6) Establish efficient information sharing mechanisms.

7) Develop national emergency plans.

8) Organize exercises.

9) Lay down the basic safety requirements.

10) Establish incident reporting mechanisms.

11) Contribute to raising awareness among users.

12) Major incentives for research and development (R & D).

13) Strengthen the training and education programs.

14) Carry out a response capacity to incidents (CERT).

15) Face down the cybercrime.

16) Foster international cooperation.

17) Create public-private partnership.

18) Balance security and privacy.

Crosschecking national data and documents to each of the aforementioned stages, it comes up that Italy has achieved heterogeneous results.

For what concerns the first four points, the ENISA's Guide take as a model of *best practices* the U.K. Italy has definitely fulfilled the first four recommendations with the adoption of the National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace Protection and ICT Security; nevertheless while scopes and objectives are explicit, the Italian vision of cyber-security is not but it can be easily inferred.

The fifth point concerns the *multi-stakeholders* involvement for a more efficient security. In Italy, there is a sort of unilateral mechanism of information sharing: while all the ITC enterprises and private entities are bound to provide to the Government their documentation about cyber events, cyber breaches, cyber security systems and so on, the Government doesn't have any legal obligation imposing to do the same. This, in turns, negatively affects the stage 6 as well, in which Italy is experiencing several deficiencies.

Another phase crucial to the development of a national cyber-security strategy is represented by the elaboration of national emergency plans (stage 7), that delineate what is an emergency crisis, how to tackle it and the subjects responsible of taking actions. Nevertheless, Italy lacks these plans and this surely represents a setback for the country.

The participation at exercises (stage 8) organized at national, European, or international level, is essential for a country to increase the general level of procedures and capabilities. Italy, concerning this stage, has recorded good results: it regularly engages in exercises organized by NATO, as for example "Cyber Coalition 2013",[99] Tallinn's CCD COE and ENISA. Italy also participated to the exercise "CybIt 2013", in which for the first time the private sector were also involved.[100]

Stage 9 indicates that laying down the basic safety requirements has proved to be a difficult task for Italy. The uphill problem for our country is that to date it is not clear if the security protocols and standards have to be formulated according to national, European or international guidelines, even if the international perspective is still the most accredited.[101]

[99] Ministero della Difesa, *Cyber Coalition 2013: conclusa l'esercitazione NATO di Cyber Defence*, 29 Novembre 2013, http://www.difesa.it/SMD_/Eventi/Pagine/CyberCoalition2013.aspx.

[100] Claudia Cencetti, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014, pag. 105. http://www.iai.it/sites/default/files/iaiq_12.pdf.

[101] Per maggiori informazioni, si veda ISO/IEC 27001 – Information Security Management, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

The point 10 is about the need of clear mechanisms of incident reporting. Unfortunately, Italy compared to other European countries or developed countries as U.S. or Canada, is still facing several hurdles: as already said, the communication between Government and ITC enterprises and private entities is unilateral. This happens also for what concerns incident reporting, not only for information sharing.

The relation between public and private sector is not regulated at national level, with the exception of the relation between Internet service providers, qualified national authorities, ENISA and the European Commission.[102]

The 11, 12 and 13 stages are all revolving around the active participation of the population in the cyber issue, they all focus on the importance of Research & Development and on improving the quality of education programs about cyber security, making them available for the people.

Estonia and United Kingdom have already launched specific university programs in this field and they are the European *cornerstones* in this sense.

Internationally, United States and Canada perform this role. Especially U.S. can be considered a pioneer country in investing massively in education programs and R&D.

These three stages are fundamental aspects for the cyber security development but at the same time they suppose the availability of *ad hoc* financial funds to tapping into.

The Italian Stability Law No. 208 for 2016 approved and published in the Official Gazette on December 30, 2015 assumed an allocation of 150 million Euros to cyber-security. This is certainly a progress for Italy.[103]

[102] Decreto del Presidente del Consiglio dei Ministri, 24 Gennaio 2013, http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.

The success of the following stage, the 14th, is consequential to the importance of these investments, because it's through them that can be trained a high-skilled team of experts and analysts ready to operate in the national CERT, which regarding Italy, is already functioning and cooperates actively with both the Defense-CERT and the PA-CERT.

For what concerns the stages 15, 16 and 17 there are some considerations to point up. Italy is making several efforts in combating the cybercrime since the early '90s and it has demonstrated to be always on the frontline in this field with its participation to numerous exercises and with its continuous work on fostering both the international cooperation and the public-private cooperation.

Surely it is recommendable to boost the latter but it is true that with the approval of the National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace Protection and ICT Security, Italy has shown its willingness to progress.

Stage 18, the last one, rests on balancing national security and privacy rights: a very thorny argument. The *Datagate* scandal that happened in 2013 in U.S. has shaken the world: Edward Snowden's revelations about National Security Agency's indiscriminate espionage to the detriment of companies like Google, Facebook, Apple, of individuals, but mostly of leading political figures such as the French Presidents Jacques Chirac, Nicolas Sarkozy, Francois Hollande or the Brazilian President Dilma Rousseff, has unveiled a vulnerability in the system.[104]

Since the early 2000's Italy has legislated on the subject approving important codes and regulations that aim to protect the privacy of individuals without exposing the country to any risk, though it's always up to each Government deciding how to exploit its technological resources.

[103] Ministero dell'Economia e Finanza, Legge di Stabilità 2016, 8 Gennaio 2016, http://www.mef.gov.it/focus/article_0014.html.
[104] Internazionale, *Cos'è il Datagate e come è cominciato*, 25 Giugno 2015, http://www.internazionale.it/notizie/2015/06/25/datagate-snowden-spionaggio.

A recapitulatory evaluation about the Italian situation in the cyber field highlights that the issuing of the National Strategic Framework for Cyberspace Security and the National Plan for Cyberspace Protection and ICT Security constituted a watershed in the cyber-security Italian panorama: it brought several news and elements that increase Italy's awareness of the cyber challenges and it shows Italy's interest in renovating its commitment in fighting the cybercrime and in enhancing its structures and systems in order to keep pace with the international community progresses.

Chapter 3.

Italian Profile in Cyber Security: a Comparative Study

The cyber security scenario is pretty worrying: in the face of threats that are becoming more frequent, large and pervasive, a strong response by stakeholders delays in coming.

But if it's true that the ICT is already omnipresent and it is a matter of fact that where there is a computer system sooner or later there will be an attack by cyber-criminals, it becomes essential to tackle the problem of how to try to limit the damage.

It has been illustrated in the previous chapters that developed countries avail themselves of a set of tools to address cyber threats. How countries decide to profit from those tools and the posture of a country toward the cyber security issue are well explained in an exhaustive document that all of them have, such as the National Cyber Security Strategy.

The countries chosen as case studies to analyze are examples of best practices and are those countries with a high level of development in this field as well as sophisticated strategies and cyber-responses.

Also, the European Union has been chosen as subject of investigation, because as a supranational institution that legally binds its Member States could not be ignored. Indeed, the effects of European policies in cyber security, along with other fields' policies, easily spill over the legal frameworks of the Member States.

In this chapter the analysis will focus on the Italian current situation. It has already been explained in broad terms what is the attitude of Italy towards cyber security, its progresses and lacks.

However, here the aim of the research is to depict the Italian current profile in matter of cyber security through a comparison with the other countries previously studied and following three lines of enquiry.

These lines revolve around:

1) The concept of threat and how threat is characterized within the cyber security picture.
2) The level of prioritization attributed to cyber threats by each State.
3) The identification of leading authorities responsible of policies, law enforcement, and their roles.

Even though in a comparative study there are many parameters that could be taken in consideration, these three are the selected ones to proceed with the study, because they were considered important parameters that logically and prominently arose from the comparison with the aforementioned case studies.

3.1. The Concept of Threat

A great challenge for all those engaged in the cyber field is coming to grips with the fluidity of the cyber domain. This fluidity implies a multiplicity of definitions of the actors involved, the measures to undertake and even what constitutes a threat.

Clarifying the concept of threat can certainly be useful in order to better assess the proper measures to undertake for countering crime. Indeed, at the bottom of every risk assessment strategy there is the cyber threat concept.

3.1.1. Italy

According to the Italian National Strategic Framework for Cyberspace Security, the cyber threat is “the complex of malicious conducts that can be exercised in and throughout cyberspace, or against cyberspace and its fundamental elements. The threat is carried out by means of cyber attacks, by […] individuals and organizations, both governmental and non-governmental, aiming at disrupting, damaging or impeding the regular functioning of computer systems, ICT networks or supervisory control and data acquisition systems and data processing, or at compromising the authenticity, the integrity, the availability or the confidentiality of data residing in those systems or transiting through the networks.”[105]

Basically, Italy distinguishes four kinds of threats, depending on the actors involved and the goals pursued, and those are the followings:

- Cyber crime: all malicious activities with a criminal intent carried out in cyberspace, such as swindles or internet fraud, identity theft, stealing of data or of intellectual property;
- Cyber espionage: improper acquisition of confidential or classified data, not necessarily of economic or commercial value;

[105] Presidency of the Council of Ministers, *The National Strategic Framwork for Cyberspace Security*, December 2013, page 12 https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.

- Cyber terrorism: ideologically motivated exploitations of systems' vulnerabilities with the intent of influencing a state or an international organization;
- Cyber warfare: activities and operations carried out in the cyber domain with the purpose of achieving an operational advantage of military significance.

Thus, the Italian National Cyber Security Strategy underlines the intrinsic nature of the cyber threat, therefore, favoring the defense over the attack and requiring that all major stakeholders, both public and private, implement a continuous process of analysis so as to be able to update their security standards and procedures to the evolving operational and technical circumstances.[106]

3.1.2. United Kingdom

The National Cyber Security Strategy of United Kingdom published in 2011 focused on a wider classification of cyber threats, which were mainly gathered in two types: cyber attacks targeting critical infrastructure and cyber attacks resulting in breach of data confidentiality.

The former has scored 3 out of 5 in terms of relative impact with a medium-low likelihood of occurring over the next five years, while the latter have a score of 1 out of 5 in terms of relative impact but with a high relative likelihood of occurring over the next five years.[107]

[106] Ibidem.

[107] N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security Threat Characterisation*, Rand Europe Report, page 27, RAND Corporation Publications 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf

Since then, the trends described accelerated and Internet-based technologies and applications improved especially in the most developed countries, also intertwining them in a closer collaboration in economic and social fields.

Both these Internet-reliance and the change of the international geopolitical landscape, led United Kingdom to reshape its definitions of what constitutes a cyber attack.

According to its last National Cyber Security Strategy, United Kingdom recognizes two kinds of cyber threats:

- Cyber-dependent crimes – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity); and
- Cyber-enabled crimes – traditional crimes that can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).[108]

As highlighted in the National Cyber Security Strategy, the most serious cyber threats – fraud, extortion and theft – against UK continues to be perpetrated mainly by financially motivated Russian-language organized criminal groups (OCGs) in Eastern Europe.

[108] UK National Cyber Security Strategy 2016 – 2021, page 17. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Even when the cyber criminals responsible for such attacks are identified is often difficult for the UK and the international law enforcement agencies to prosecute them, since they are located in jurisdictions with limited extradition arrangements.

There is equal concern also for those attacks less sophisticated but widespread, perpetrated by State or State-sponsored actors, such as groups who tend to penetrate UK networks for a broad range of scopes (political, diplomatic, commercial, strategic advantage, etc.) with a particular focus on the UK's critical infrastructures.

Other dangerous actors identified are: terrorists, hacktivists, decentralized and issue-orientated groups, and the so-called "script kiddies", less-skilled individuals who use programmes developed by others. However, terrorists are believed to have a low-level technical capability, thus the current assessment is that physical, rather than cyber, terrorist attacks will remain the priority for terrorist groups for the immediate future.[109]

3.1.3. Estonia

Both the Estonia Cyber Security Strategy of 2008 – 2013 and that one of 2014 – 2017 characterize cyber threats by focusing on the effects of threat actors. Cyber attacks are mainly those against critical information infrastructure or cybercrime.

The strategies put an emphasis on the need of a more secure cyberspace and concentrate on information systems.

[109] Ibidem.

Among all the measures recommended there are an improved public-private partnership, regulation measures, investments in education and collaboration at both national and international levels and intergovernmental level.[110]

3.1.4. United States of America

The United States' perception of a cyber threat changed a lot and has been rearticulated many times over the years, going at the same pace of the challenges that the country had to face.

In a document of December 2011, namely the Strategic National Risk Assessment, there is a detailed classification of cyber threats and also their impact in shaping other threats (*domino-effect*).

In the top echelon of threats there are:

- Cyber attacks against data: which seriously compromises the integrity or availability of data
- Cyber attacks against physical infrastructure: the cyber attack is instrumental to achieve greater disastrous effects that goes beyond the ITC systems and may result in massive economic losses.[111]

In the recent years, United States shifted their attention especially on those threats emanated from States such as Russia and China, for the targeting and disruptions of the IT infrastructure, and nation-states and criminals engaged in industrial espionage and terrorism (Al Qaeda, Hamas, Hezbollah).

[110] N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security Threat Characterisation*, Rand Europe Report, page 14, RAND Corporation Publications 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf.

[111] Ibidem, page 30.

With the 2011 US International Strategy for Cyberspace, the discussion evolved and have been lately identified as major threats not only the previously analyzed cybercriminals but also their proxies.[112]

3.1.5. Canada

The 2010 Canada's National Cyber Security Strategy is the reflection of the Canadian commitment against the cybercrime. As aforementioned in the second chapter, basically, the cyber threats established by Canada are the same targeted by other countries.

Those threats are clearly divided in the following categories, in combination with the perpetrators:

- Military and intelligence organizations undertaking state-sponsored cyber military and espionage activities – political, economic, commercial and military purposes.
- Cybercriminals – identity theft, money laundering, extortion.
- Terrorist groups – recruitment, fundraising, propaganda, attacks.

The economic reliance that ties Canada to the ICT systems leads the country to prioritize counter-cybercrime posing a particular accent on the economic aspect of the conditions.

[112] Ibidem.

3.2. The Level of Prioritization

The challenge posed by cybercrime has led the most developed countries to amend their legislations in order to better cope with this issue. Some countries have even equated the cyber threat to others identically significant such as terrorism, for example.

Thus, according to the level of prioritization assigned, each country has adopted the response measures deemed adequate.

3.2.1. Italy

The Italian hierarchy of threats positions terrorism as the top of priorities, followed by the migratory issue and the cyber threat.[113]

As stated in the National Strategic Framework for Cyber Security, "the security and the prosperity of a country increasingly depend on the protection of the ICT networks, which host this ever growing wealth of knowledge and connections. Therefore, is more compelling to ensure in cyberspace the respect of the rights and duties already preserved in the civil society and in the International Community."[114]

From these words, it can be easily deduced the Italian government's commitment in guaranteeing that democratic principles and values are shared and respected also in the digital arena.

[113] Jean-Pierre Maulny and Sabine Sarraf, Assessment and Prospects of Security Threats, Report of Institute de Relations Internationales et Stratégiques, April 2016, http://www.iris-france.org/wp-content/uploads/2016/04/TAC-Report-2016-ENG-V3.pdf.

[114] Presidency of the Council of Ministers, *The National Strategic Framwork for Cyberspace Security*, December 2013, pp. 5-6. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.

3.2.2. United Kingdom

As underlined in the second chapter, the current National Cyber Security Strategy of United Kingdom identifies improving cyber security as a "Tier 1 risk", based on a judgment of the combination of both likelihood and impact.[115]

Ranking cyber security at the same level of terrorism or international military conflict implies the need of massive investments in this field. Indeed, it paved the way for cyber-security related agencies to be allocated a four-year budget of £ 650 million.[116]

Surely, this demonstrates the outstanding priority that United Kingdom gives to the cyber issue.

3.2.3. Estonia

According to the 2011 update of the Estonian national emergency risk assessment, the likelihood of cyber-attack is rated as "high" (4 on a 5x5 matrix of impact and likelihood).

The following threats were classified in the same category: pollution, coastal pollution, and epidemics. Heat waves, wildfires and mass poisoning were allocated the same degree of likelihood but less dangerous impact.

[115] HM Government, UK National Cyber Security Strategy 2016 – 2021. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[116] N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security Threat Characterisation*, Rand Europe Report, page 26, RAND Corporation Publications 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf.

The effects of a cross-border nuclear incident, industrial fires, formation or dissolution of ice and groundwater contamination were allocated the same level of impact, but with less likelihood.[117]

It has to be remembered that the cyber attacks Estonia has endured in 2007 have pushed the country into the spotlight with respect to cyber-security. Estonia was the first EU Member State to publish a cross-government, national cyber-security strategy in 2008 and its threat assessment stems very much from a desire to increase resilience and manage the consequences of such attacks in future.[118]

3.2.4. United States of America

In United States the cyber domain has always been something of major concern and a persistent theme at the top of the US government agenda, for at least a decade. However, by the time went by, the way the threat has been perceived and characterized has changed a lot, especially after 09/11.

Lately, the emphasis has shifted from non-state terrorism to state actors' activities, and from a predominantly political to an economic matter.[119]

Terrorism has always been a top-priority threat to address for United States, but the improvements made in the digital field have brought US to reconsider the security's global framework giving to cybercrime the proper credit. As stated, for example, by the FBI Director

[117] Ibidem, page 13.
[118] Ibidem.
[119] Ibidem, page 29.

Robert S. Mueller, the cyber threat is growing, is crucial to address and is not so unbelievable that cyber threats will equal or surpass the threat from terrorism in the near future.[120]

In United States, the cyber threat debate continues to develop, and the focus has shifted to boosting private actors to increase their endeavors to protect their information infrastructures. President Barack Obama's administration has stated an intention to fortify the security of critical cyber systems through his executive powers, although lobbying from interests that see the regulation of private networks as economically damaging never ceased.[121]

Cyber challenge for United States, as for many other countries, is not over yet.

3.2.5. Canada

Looking at the 2010 Canada's Cyber Security Strategy can be easily inferred the degree of importance bestowed to this issue by the country. As analyzed in the second chapter, the strategy is built on three pillars, which aim to secure government systems, promote a wide range of partnerships and help Canadians to be secure online.[122]

For Canada, cyber security is one of seven highest national security priorities approved annually by the Cabinet's Ad Hoc Committee on Security and Intelligence and it's classified alongside the followings:

- International terrorism and extremism;
- The mission in Afghanistan;

[120] Ibidem.
[121] Ibidem.
[122] Canada's Cyber Security Strategy, 2010, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

- The proliferation of weapons of mass destruction;
- Foreign espionage and interference;
- Canada's Northern Strategy; and
- International security and prosperity interests.[123]

3.3. Leading Authorities

Establishing who has to be in charge of managing the cyber security of a country is a significant decision. There are countries that opt for a solution implying a centralized control system and others that prefer a decentralized structure. Both aspects carry along consequences in terms of benefits and losses.

After a concise overview of the governmental architecture designated to cyber security by each of the countries taken as case study, in the next paragraph it will be deduced which one of the two aspects is better in relation to efficiency and resilience, or if a mixed approach would be more adequate.

Resources allocation is another key topic in cyber security. Thus, it won't be excluded from the discussion because it proves the concrete commitment of a country towards the issue and, of course, it gives a preview of the range of improvement that might occur in the field.

[123] N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security Threat Characterisation*, Rand Europe Report, page 10, RAND Corporation Publications 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf.

3.3.1. Italy

In the second chapter, it has been extensively explained the Italian national architecture designated to cyber-security. Without repeating the same concepts, the most relevant features will be illustrated.

Cyber security coordination in Italy is directly under the responsibility of the cabinet office (Presidenza del Consiglio dei Ministri). Thus, the Italian Prime Minister's Office is formally entrusted of developing and implementing the national cyber security strategy and the implementation plan through a set of directives and measures.

The Prime Minister's Office is supported in this task by the Inter-Departmental Committee for the Security of the Republic (CISR – Comitato Interministeriale per la Sicurezza della Repubblica), which promotes info-sharing and best practices, advocates for the adoption of additional legislative initiatives, approves guidelines to foster private-public partnerships, approves other measures to strengthen national cyber security.[124]

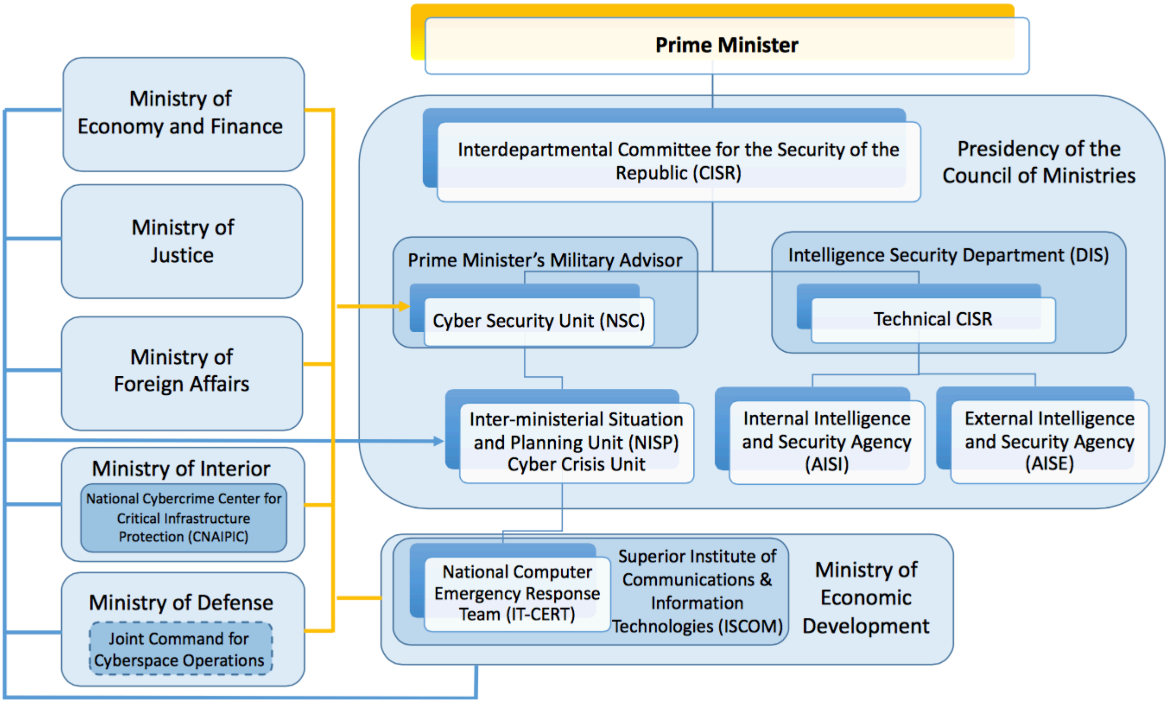
The CISR is backed in its activities by various national intelligence public entities, including DIS (Dipartimento delle Informazioni per la Sicurezza), AISE (Agenzia informazioni e sicurezza esterna) and AISI (Agenzia informazioni e sicurezza interna).

In 2013 was also established a permanent body within the Prime Minister's Office, the Cyber Security Unit (NSC – Nucleo per la Sicurezza Cibernetica), an operational core functional

[124] M. Hathaway, C. Demchak, J. Kerben, J. McArdle, F. Spidalieri, *Italy Cyber Readiness at a Glance*, Potomac Institute for Policy Studies Publications, November 2016, page 8. http://www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf.

24/7 with the aim of collecting information and signals from abroad and alerting the internal bodies committed to national security, in case of an imminent danger.

In such cases, to gain further help in the crisis management, NSC activates another force, which directly rules, the NISP (Nucleo Interministeriale Situazione e Pianificazione)[125].


Prime Minister
Ministry of Economy and Finance
Ministry of Justice
Ministry of Foreign Affairs
Ministry of Interior
National Cybercrime Center for Critical Infrastructure Protection (CNAIPIC)
Ministry of Defense
Joint Command for Cyberspace Operations
Interdepartmental Committee for the Security of the Republic (CISR)
Presidency of the Council of Ministries
Prime Minister's Military Advisor
Cyber Security Unit (NSC)
Intelligence Security Department (DIS)
Technical CISR
Inter-ministerial Situation and Planning Unit (NISP) Cyber Crisis Unit
Internal Intelligence and Security Agency (AISI)
External Intelligence and Security Agency (AISE)
National Computer Emergency Response Team (IT-CERT)
Superior Institute of Communications & Information Technologies (ISCOM)
Ministry of Economic Development

Italy Cyber Security Organizational Chart (2016).

Source: M. Hathaway, C. Demchak, J. Kerben, J. McArdle, F. Spidalieri, *Italy Cyber Readiness at a Glance*, Potomac Institute for Policy Studies Publications, November 2016, http://www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf.

[125] Claudia Cencetti, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014, pag. 105. http://www.iai.it/sites/default/files/iaiq_12.pdf.

In a Directive of the Prime Minister, emanated in 2015, it can be noticed the intention of the government to enhance the development of a more comprehensive institutional architecture, to foster closer collaboration among both public and private entities working in the telecommunications and critical infrastructures' sectors and to establish stronger incident response capabilities.[126]

Speaking of resources allocation, Italy has made several progresses. In the 2015 Digital Growth Strategy, the Italian government committed €50 million to securing citizens and businesses' digital identities and ensuring safe and secure access to digital services, including from mobile devices.[127]

Furthermore, the 2016 Stability Law (Legge di Stabilità 2016), approving the Fiscal Year 2016 budget, allocated €150 million for national cyber security efforts, of which €15 million to the Italian Postal and Communications Police Service and its "National Cybercrime Centre for Critical Infrastructure Protection" (CNAIPIC) – a special unit responsible for all activities of prevention, containment, mitigation, and investigation of cyber crime and other malicious cyber activities conducted against critical infrastructure.[128]

Finally, a recent September 2016 Prime Minister's Decree allocated the remaining €135 million of the FY 2016 budget to national cyber security efforts under the responsibility of the DIS,

[126] M. Hathaway, C. Demchak, J. Kerben, J. McArdle, F. Spidalieri, *Italy Cyber Readiness at a Glance*, Potomac Institute for Policy Studies Publications, November 2016, page 8. http://www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf.

[127] Presidenza del Consiglio dei Ministri, *Strategia per la Crescita Digitale 2014 – 2020*, Marzo 2015. http://www.agid.gov.it/sites/default/files/documentazione/strat_crescita_digit_3marzo_0.pdf.

[128] M. Hathaway, C. Demchak, J. Kerben, J. McArdle, F. Spidalieri, *Italy Cyber Readiness at a Glance*, Potomac Institute for Policy Studies Publications, November 2016, page 8. http://www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf.

in order to strengthen both traditional preventive and defense measures against cyber risks that rise to the national level and to prioritize the protection of national cyberspace.[129]

3.3.2. United Kingdom

Cyber security in United Kingdom sees the participation of many stakeholders upholding the UK Cyber Security Strategy. In the European context, United Kingdom is considered the cornerstone of the fight against cyber crime and it can be deduced also by both the numbers of entities involved in the field and the significant amount of resources invested.

In the National Cyber Security Strategy 2016-2021, the Chancellor of the Exchequer Philip Hammond, announced that the guidelines that UK will observe in the following years, take in consideration many factors: first of all, the cyber attacks are growing more frequent, sophisticated and damaging when they succeed[130] and secondly, there is a need of recognition that despite all the efforts made by the country to protect its systems, the attacks will happen anyway.

This recognition is a turning point in shaping a new strategy because it supposes that the guidelines would revolve more around the concept of resilience rather than absolute protection and resistance. This in turn would lead to an enhancement of the incident response mechanism and to citizens' increased awareness of the cyber culture.

[129] Ibidem.

[130] HM Government, UK National Cyber Security Strategy 2016 – 2021, page 6. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

The £1.9 billion investment announced in the Strategy testifies the UK's outstanding commitment in defending the systems and infrastructure, deterring the adversaries, and developing a whole-society capability – from the biggest companies to the individual citizen.[131]

The National Cyber Security Centre (NCSC) is the UK's authority on cyber security. It belongs to the Government Communications Headquarters (GCHQ) and it brings together and replaces CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).

The NCSC's main purpose is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. NCSC works along with UK organizations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management.[132]

The UK has a specialized Office of Cyber Security and Information Assurance (OCSIA) as well, which supports Cabinet Office ministers and the National Security Council in determining priorities in relation to securing cyberspace. The role of the unit is to guide a close cooperation and collaboration between the various national-level agencies and departments and fostering a common policy approach.[133]

[131] Ibidem.

[132] National Cyber Security Centre, https://www.ncsc.gov.uk/about-us.

[133] N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security Threat Characterisation*, Rand Europe Report, page 7, RAND Corporation Publications 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf.

The OCSIA collaborates with other lead government departments and agencies such as the Home Office, Ministry of Defence (MOD), GCHQ, the Foreign & Commonwealth Office (FCO) and the Department for Culture, Media & Sport.[134]

Lastly, has to be pointed out the relevance of the National Crime Agency, which is UK's national law enforcement and police agency against not only cyber crime but also organized crime, human, weapon and drug trafficking, both national and transboundary economic crime, and technically, can be tasked to investigate any other crime. NCA was born in 2013 from the merger of the two preceding agencies, the Serious Organised Crime Agency (SOCA) and the Police Central E-Crime Unit.

3.3.3. Estonia

Estonia, today, represents the most advanced reference point in the global cyber war. Not only because endured those memorable cyber attacks in 2007, but also because it is the "digital State" of the European Union: with thousands of public Wi-Fi spots, online political consultations, 90% of bank transactions that take place via the Internet, thousands of start-ups in information technology and telecommunications.

Economics, politics and citizen's services: everything here takes place online and the entire nation is optical fiber-wired. Indeed, the name of the State is often ironically deformed in "E-stonia".

[134] Office of Cyber Security and Information Assurance, https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.

And with the new tensions and changes in international politics arising between the West and Russia, this small technological country of NATO has become crucial.

The Estonian “IT front” is coordinated since 2008 by an international military organization called CCDCOE (Cooperative Cyber Defence Centre of Excellence) used for research and study on the themes of war and cyber security, whose headquarters is in a military base in Tallinn. A center of excellence increasingly grown over the years which today sees the membership of 15 nations including the United States, Italy, Germany, France, Holland, England.

Preventing, monitoring and possibly respond to cyber terrorist attacks is their mission. The center employs about forty people from different countries and access to outsiders is strictly prohibited by the NATO’s security protocols.[135]

Since the 2007, the Estonian Information System Authority (RIA) is the central authority for cyber security: it coordinates powers over government efforts in cyber and related departments, such as the Department of Critical Information Infrastructure Protection.

RIA handles incident response, the protection of critical information infrastructures and serves as a platform for cooperation and the integration of efforts.

The military has a crucial role in cyber-defence, particularly regarding close cooperation with NATO through the CCDCOE.

In addition, there is the IT Crimes Office of the Criminal Police that sits within the Ministry of Interior. Also, within the Ministry are units dedicated to crisis management, cybercrime and

[135] L. Locatelli, *In Estonia, sul fronte della cyber guerra*, L’Espresso, 24 Settembre 2014, http://espresso.repubblica.it/plus/articoli/2014/09/22/news/in-estonia-sul-fronte-della-cyberguerra-1.181073.

critical infrastructure protection, which are responsible further for coordinating Estonia's information security.[136]

According to an interview to the Estonia's Defense Minister Hannes Hanso, Estonia is currently working under a 10-year defense plan, which will continue until 2022. Every four years are conducted reviews, i.e. the last one took place in 2016, and if changes are needed they will be implemented. The defense budget for 2016 was about €450 million.

Although this is modest by international standards, it is set to rise year-on-year by around 7%. The money spent on defense will be addressed to improving the defense infrastructure, investing substantially in military and improving the cyber resilience.[137]

Estonia's achievements in cyber security have also benefitted from a strong IT partnership between the public and private sector. This conjunction gave birth to the Cyber Defence League.

Among other offices, the Estonian Police and Border Guard also have their own Cyber Crimes Unit, to investigate and prosecute online criminal activity.

However, the real key to Estonian cyber security lies in the inherent safety and security built-in to every single Estonian e-Government and IT infrastructure system. Estonian citizens and businesses operate with confidence, knowing that their data is safe and their transactions are secure.

[136] N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security Threat Characterisation*, Rand Europe Report, page 14, RAND Corporation Publications 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf.

[137] G. O'Dwyer, *Interview: Estonian Defence's Minister Hannes Hanso,* DefenseNews, February 3, 2016. http://www.defensenews.com/story/defense/policy-budget/leaders/interviews/2016/02/03/interview-estonias-defence-minister-hannes-hanso/78845280/.

Indeed, the best kind of cyber security is one that everyday people never have to think about.[138]

3.3.4. United States of America

Speaking in terms of responsibilities and roles for what concerns cyber security in United States, it can be observed that there is a high level of distribution of power.

This country has a long history of "culture of defense" and the tragic events of terrorism that hit US have only had the effect of pushing the authorities towards an ever-increasing development of its defense architecture.

Obviously, in this architecture is comprised the cyber sector, which today has become crucial for spurring innovation, cultivating knowledge and increasing national economic welfare.

However, as already seen, the same infrastructure is the target of malicious activities, malfunctions, human errors or natural disasters. The collateral effects can be heavily destructive and can inflict huge losses.

The awareness that these "attacks" happen every day, has allowed United States to develop a whole-of-Government approach based on shared responsibilities, unity of effort within the Federal Government and close coordination between public and private sector.[139]

The US Federal Government's bureaucracy is extensive and complicated, thus the exact number of agencies, offices, boards, and commissions is unknown.

[138] Cyber Security, e-Estonia.com - The Digital Society, https://e-estonia.com/the-story/digital-society/cyber-security/.

[139] The White House, Office of the Press Secretary, Presidential Policy Directive PPD/41, *United States Cyber Incident Coordination*, July 26, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

All federal departments and agencies are in charge of the protection of their own ICT systems, and many have sector-specific responsibilities for critical infrastructure for which they are responsible.

The regulatory mandate of different departments and agencies varies; most departments have a generalized responsibility to regulate in their constituency, others have existing cyber security-specific regulations, while some don't have a clear authority to regulate cyber security.

Moreover, there are also cases in which cyber security strategy documents assign high-level roles and responsibilities to Federal Government entities, but leave the implementation details to the agencies' discretion.[140]

Thus, the following analysis is a brief summary of the most important leading authorities in US' cyber sector.

For what concerns military and capabilities, the Department of Defense is tasked to safeguard DoD's global information infrastructure from cyber attacks. DoD moreover has responsibilities for gathering foreign cyber threat information, securing national security and military systems, and investigating cybercrimes under military jurisdiction.[141]

Within DoD works the United States Northern Command (USNORTHCOM), which coordinates and provides forces for Defense Security Cooperation Agency operations. The United States Strategic Command (USSTRATCOM), through the United States Cyber Command (USCYBERCOM), is responsible for synchronizing, planning and executing cyber operations. USCYBERCOM directs the operations and defense of specified DoD networks and may conduct full-spectrum military cyberspace operations.[142]

[140] P. Pernik, J. Wojtkowiak, A. Verschoor-Kirss, *National Cyber Security Organisation: United States*, page 15, CCCDCOE Publications, Tallinn 2016. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf.

[141] Ibidem.

[142] N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security Threat Characterisation*, Rand Europe Report, page 30, RAND Corporation Publications 2013.

Then, there is the Department of Homeland Security (DHS): the primary institution responsible for cyber security within US borders.[143]

The DHS is entrusted of defensive actions for the government networks and it coordinates the nation's overall critical infrastructure protection efforts, including cyber infrastructure, by working also in cooperation with designated, sector-specific agencies within the Executive Branch through the National Cyber Security Center.[144]

Lastly, cannot be ignored the importance covered by the US Intelligence Community, headed by the Director of National Intelligence (DNI) is intrinsically linked to cyber due to the amount of information that flows throughout shared information technology infrastructures of the world.

The Office of the Director of National Intelligence coordinates 17 agencies and organizations, many of which are under the authority of DHS and DoD, and establishes objectives within the Intelligence community.

The National Security Agency (NSA) is the primary cyber security agency in the American national security sector, although other agencies also play significant roles. The Director of the NSA reports directly to the Director of National Intelligence.[145]

The Federal Bureau of Investigation (FBI) manages the National Cyber Investigative Joint Task Force (NCIJTF), which aggregates counterintelligence, counterterrorism, intelligence, and law

http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf

[143] P. Pernik, J. Wojtkowiak, A. Verschoor-Kirss, *National Cyber Security Organisation: United States*, page 15, CCCDCOE Publications, Tallinn 2016. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf.

[144] N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security Threat Characterisation*, Rand Europe Report, page 31, RAND Corporation Publications 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf.

[145] P. Pernik, J. Wojtkowiak, A. Verschoor-Kirss, *National Cyber Security Organisation: United States*, page 15, CCCDCOE Publications, Tallinn 2016. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf.

enforcement information and activities from several federal agencies in order to predict and prevent cyber attacks.[146]

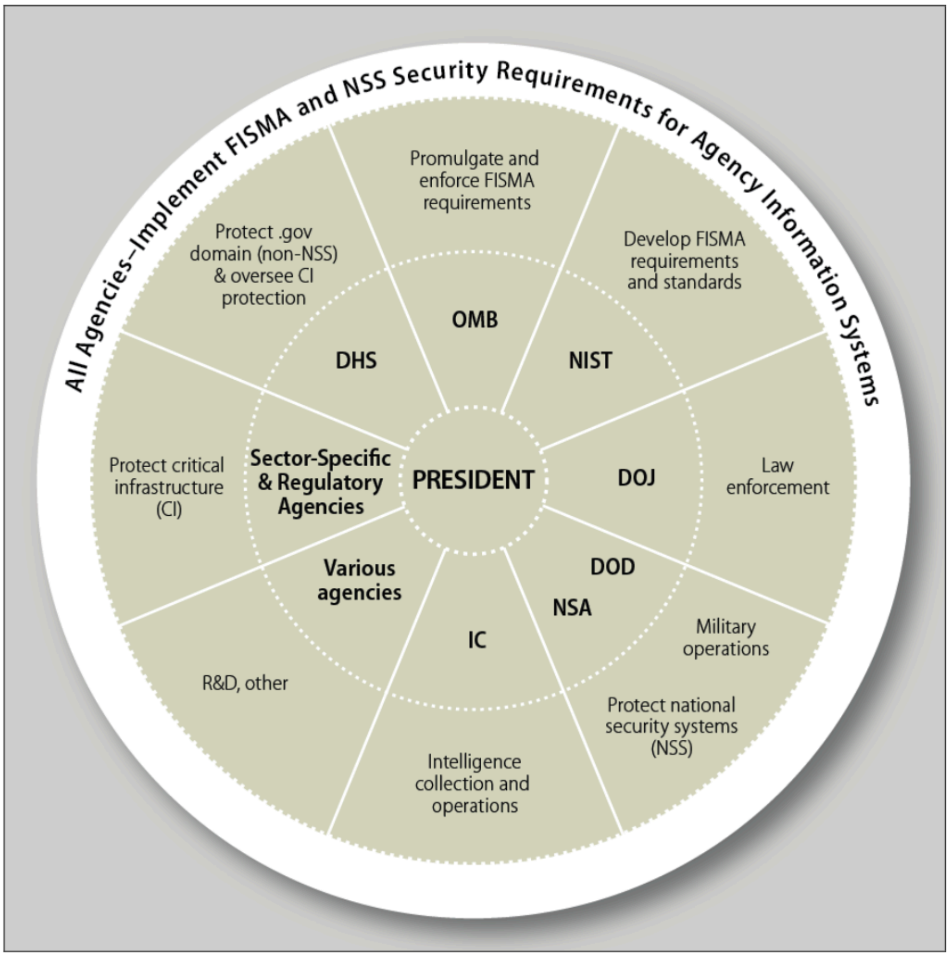
Furthermore, the Intelligence Community provides and secures the intelligence technology for the armed forces.[147]

[146] U.S. Department of Justice, The Federal Bureau of Investigation (FBI), *'National Cyber Investigative Joint Task Force (NCIJTF)'* http://www.fbi.gov/about-us/investigate/cyber/ncijtf.

[147] U.S. Coast Guard, *'United States Coast Guard Cyber Strategy'*, p.21, Department of Homeland Security, 2015 https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf; U.S. Central Intelligence Agency, 'Executive Order 12333', 1981 https://www.cia.gov/about-cia/eo12333.html.

In the Figure 1 below there is a simplified schematic diagram of major agency responsibilities in cyber security.

Figure 1. Simplified Schematic Diagram of Federal Agency Cybersecurity Roles


All Agencies–Implement FISMA and NSS Security Requirements for Agency Information Systems
Promulgate and enforce FISMA requirements
OMB
Develop FISMA requirements and standards
NIST
Law enforcement
DOJ
Military operations
DOD
NSA
Protect national security systems (NSS)
Intelligence collection and operations
IC
R&D, other
Various agencies
Protect critical infrastructure (CI)
Sector-Specific & Regulatory Agencies
Protect .gov domain (non-NSS) & oversee CI protection
DHS
PRESIDENT

Source: CRS.

Notes: DHS: Department of Homeland Security; DOD: Department of Defense; DOJ: Department of Justice; FISMA: Federal Information Security Management Act; IC: Intelligence Community; NIST: National Institute of Standards and Technology; NSA: National Security Agency; OMB: Office of Management and Budget; R&D: Research and development.

Source: E. A. Fischer, *Cybersecurity Issues and Challenges: In Brief*, Congressional Research Service Report, Aug. 12, 2016.

https://fas.org/sgp/crs/misc/R43831.pdf.

The amount of resources US planned to invest in cyber security is remarkable: according to the Cybersecurity National Action Plan released by Obama’s Administration in February 2016, has been proposed a $3.1 billion Information Technology Modernization Fund to enable the retirement, replacement, and modernization of legacy IT that is difficult to secure and expensive to maintain, as well as the formation of a new position, such as the Federal Chief Information Security Officer, to drive noteworthy changes in terms of cyber security across the Government.

Moreover, in order to implement these changes which will make United States a leading country in the fight against cyber crime, the Federal Government retained appropriate to invest additional resources which have been translated in the 2017 Budget's allocation of more than $19 billion for cyber security – a more than 35% increase over the 2016 enacted level.

These resources should enable agencies to raise their level of cyber security, help private sector organizations and individuals to better protect themselves, disrupt and deter malicious activities, and respond efficiently to incidents.[148]

3.3.5. Canada

In the Canada's Cyber Security Strategy is clearly stated that discussing about an ambiguous issue such as cyber security requires clarity, otherwise the risk of succumbing to inefficiency could be very high. For this reason, roles and responsibilities are distinctly enunciated.

Public Safety Canada coordinates the implementation of the Strategy. Based on a whole-of-Government approach, it provides central coordination for assessing emerging complex threats and developing and promoting comprehensive and efficient approaches to address risks within the Government and across Canada.[149]

[148] The White House, Office of the Press Secretary, *FACT SHEET: Cybersecurity National Action Plan*, February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[149] Ministry of Public Safety, Government of Canada, *Canada's Cyber Security Strategy*, 2010. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

Within Public Safety Canada, the Canadian Cyber Incident Response Centre deals with threats-monitoring activities and leads activities aimed at raising public awareness and improving public safety.

Under the guidance of the Ministry of Defence there is an independent agency with high expertise in the field: the Communication Security Establishment Canada, which detects and discovers threats, provides intelligence and cyber-security and responds to threats against government systems.[150]

The Canadian Security Intelligence Service (CSIS) analyzes and investigates domestic and international threats to the security of Canada.

The Royal Canadian Mounted Police's role is to investigate suspected domestic and international criminal acts against Canadian networks and critical information infrastructure.

The Treasury Board Secretariat is responsible to support and strengthen cyber incident management capabilities across Government, through the development of policies, standards and assessment tools. Furthermore, it's responsible for information technology security in the Government of Canada.

Foreign Affairs and International Trade Canada is a Department entrusted to advise on the international dimension of cyber security and work for developing a cyber security foreign policy that will strengthen the coherence of the Canadian government in its engagement abroad on cyber security affairs.

[150] N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security Threat Characterisation*, Rand Europe Report, page 10, RAND Corporation Publications 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf.

And lastly, the Department of National Defence and the Canadian Forces are in charge of defending their own networks and to exchange information about cyber best practices with allied militaries.[151]

The economic resources allocated to the cyber field are substantial and mirror the Canadian willingness to further build up its systems and networks. According to the Strategy, $36.4 million were pledged over five years, starting with $3 million only in 2015.

On top of the $36.4 million promised, the Canada's budget referring to cyber-security also included details of a planned $58 million five-year investment to protect the Government of Canada's "essential cyber systems and critical infrastructure" against cyber attacks.[152]

Thus, the aforementioned document added: " (…) to better defend and protect these systems, the Government is taking action by upgrading critical cyber systems, such as Internet network paths and connections that are used on a regular basis to provide services to Canadians.

Taking these measures will ensure that the Government is able to continue to detect and repel infiltration attempts on the Government's cyber systems and identify malicious actors that seek unauthorized access".[153]

3.4. Achieving Efficiency: the Current Italian Challenge

Comparing Italy with what has been studied and shown so far, it turns out a multifaceted framework.

[151] Ministry of Public Safety, Government of Canada, *Canada's Cyber Security Strategy*, 2010. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.

[152] A. Martin, *Canada commits $36.4 million to cybersecurity measures in 2015 budget,* We Live Security, April 22, 2015. http://www.welivesecurity.com/2015/04/22/canada-commits-36-4-million-cybersecurity-measures-2015-budget.

[153] Government of Canada, 2015 Budget. http://www.budget.gc.ca/2015/docs/plan/ch4-3-eng.html.

Certainly, the cyber security challenge has been fully accepted by Italy, and countless efforts have been already made and continue to be carried out, to put the country up to the task.

However, there are still many problems that require a greater commitment on the behalf of the Institutions in order to let Italy reach levels of protection, competitiveness and development equal to those of other developed countries.

Firstly, it can be noticed that today Italy still suffers of obvious deficiencies: official documents relating to cyber security strategies don't mirror a clear vision as that adopted by other countries such as Canada, the US, Britain or Estonia.

And even if only recently (2015) a national CERT has been activated, the absence of national emergency plans such as those, for i.e., provided by United States, is an additional obstacle to the improvement of the security system.

Contrary to the other previously investigated countries, Italy does not have a single document where it is exposed in a clear and straightforward way the national strategy. But there are two comprehensive documents from which it can be deduced the strategic direction of the country in terms of cyber security.

Today, the same strategy may be defined as partially operational, because the objectives to achieve continue to clash with the country’s structural problems, especially in the long term. These difficulties are closely related to a stagnant economic growth, low productivity rates and a high unemployment rate.

Although several government measures have been implemented to reinvigorate the country's economy, it is still quite difficult to stay within budget and at the same time invest heavily in the security sector.

From the official documents illustrated, it can be assumed that Italy has a very broad concept of threat and surely prefer to adopt a defensive rather than an offensive posture in cyber security. Precisely because of this consideration there should be an increase in the amount of resources allocated in both cyber and Research & Development sectors, but without forgetting the substantial investment of € 150 million that the government has already approved in 2016.

For Italy cyber security is one of the three priority threats to address -after terrorism and migratory issue- but it's still not equivalent to the threat of terrorism. This, for example, is another big difference with countries like Great Britain or the United States: the latter, for instance, have even predict that in the near future the threat posed by the cyber domain will likely surpass the terrorism issue.

Nevertheless, Italy does not underestimate the issue but certainly the walking path ahead is still long: regarding e-crime and law enforcement, for example, Italy has amended and strengthened its Criminal Code in order to include coverage of computer crimes and e-crimes since the early 1990s, however has yet to implement all of the cross-border assistance options contained in the Council of Europe Convention on Cybercrime, ratified by Italy in 2008.

Italy’s participation in various law enforcement training programs is undeniable as much as his involvement in many partnerships to increase cooperation in cyber security, information sharing, border security and surveillance.

The Italian Postal and Communications Police Service, is the main law enforcement entity responsible for cyber crime prevention in Italy and since 2005 is responsible for law enforcement initiatives against cyber attacks on critical information infrastructure. It is assisted by other law enforcement entities such as the Italian Police, the so-called Guardia di Finanza and Carabinieri.

Another topic of discussion concerns the structure of responsibility and roles in cyber defense.

Italy has somehow a fairly centralized power structure and this carries its own consequences. Surely, other particularly “decentralized” defense structures, such as that found in United States, are not guarantee of efficiency as well.

Taking in consideration the American case, for i.e., cyber security strategy documents have assigned high-level roles and responsibilities to multiple entities but have left important details unclear. Several GAO (Government Accountability Office of United States of America) reports have likewise demonstrated that the roles and responsibilities of key agencies charged with protecting the nation’s cyber assets are inadequately defined.[154]

Furthermore, several federal agencies have not demonstrated an ability to coordinate their activities and project clear policies on a consistent basis and they still suffer from redundant activities and lack of trust, thus translating in inadequate information sharing mechanisms.[155]

Basically, Italy delegates the responsibility firstly to the office of the Prime Minister, who in turn coordinates the various offices hierarchically subordinate.

Much of the work is done by the governmental agencies of domestic and external security (AISI and AISE), but still nowadays arises the question whether the Italian system is too complicated and intricate or not. Many are the stakeholders involved that have to play their part, each with its own role and responsibilities, and above all they must dialogue.

Thus, the question that follows is: does this structure create delays and overlaps or not?

[154] United States Government Accountability Office, Report to Congressional Addressees, *CYBERSECURITY: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, February 2013. http://www.gao.gov/assets/660/652170.pdf.

[155] United States Government Accountability Office, Report to Congressional Requesters, *CYBERSPACE: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, July 2010. http://gao.gov/assets/310/308401.pdf.

Although currently there are no regulatory changes expected about the Italian defense structure, quoting the words of Gen. Carmine Masiello, it could be “always better to have a reserve: redundancy is not necessarily bad, it can also be a guarantee of operation continuity”.[156]

[156] P. Licata, *Come migliorare la sicurezza cyber in Italia. Le idee di Masiello (Palazzo Chigi)*, F! Formiche, 5 Agosto 2016. http://formiche.net/2016/08/05/come-migliorare-la-sicurezza-cyber-italia-le-idee-di-palazzo-chigi.

Conclusion.

In my thesis, I wanted to approach the study of the cyber challenge by creating a generalized comparative profile of the most advanced countries.

The countries chosen for comparison are those countries that, to date, can be considered groundbreaking in terms of cyber security and that are equipped with the most sophisticated technologies.

I have highlighted in order the following cases: United Kingdom, Estonia, United States of America and Canada. I have included in the study even a brief overview on Europe in the second chapter, as it is a paramount supranational entity that legally binds its Member States.

Undoubtedly the final result allowed bringing out more clearly, from the international context, the Italian framework.

For what concerns United Kingdom, I have shown that cyber security is considered a vital topic.

This emerges clearly from the National Cyber Security Strategy of the country, considering several measures adopted: the equalization – in terms of risk and impact – of cyber threats to terrorism or military conflict; the establishment of a Cyber Permanent Committee composed of various government members from different government departments, remarking the will of the central government to work collaboratively; a multiplicity of authorities responsible for the management of the cyber issue; finally, the massive investment of £ 1.9 billion for the defense of the systems and infrastructure, deterrence of adversaries and development of whole-society capabilities.

Estonia, known for the cyber attacks endured in 2007, gave birth to a framework purely imbued on resilience. Since 2009, a number of important decisions that have been taken have allowed Estonia to become today one of the reference countries with regard to progress in the cyber security field.

The central body that deals with cyber security is the RIA (Estonian Information System Authority) and it is also noteworthy its close cooperation with NATO CCDCOE of Tallinn, through which play a crucial role in cyber defense.

The main objectives are improving Estonian defense of critical infrastructure, investing substantially in the military, and improving resilience. Although, the defense budget for 2016 was fairly modest, it is set to rise year-on-year by around 7%. Estonia's achievements in cyber security have also benefitted from a strong IT partnership between the public and private sector.

This conjunction gave birth to the Cyber Defence League.

However, the real key to Estonian cyber security lies in the inherent safety and security built-in to every single Estonian e-Government and IT infrastructure system. Estonian citizens and businesses operate with confidence, knowing that their data is safe and their transactions are secure.

Indeed, the best kind of cyber security is one that everyday people never have to think about.[157]

For the United States, although the problem is not unknown nor has recent origin, it has long been at the center of debates. The same American concept of cyber threat has changed a lot over time, going hand in hand with the attacks and events that involved the country over the years.

The emphasis has shifted from non-state terrorism to state actors' activities, and predominantly from a political to an economic matter. Terrorism has always been a top-priority threat to address for United States, but the improvements made in the digital field have brought US to reconsider the security's global framework giving to cybercrime the proper credit. The same

[157] Cyber Security, e-Estonia – The Digital Society, https://e-estonia.com/the-story/digital-society/cyber-security/.

former President Obama has identified cyber threats as one of the more serious economic and national security challenges of all times.

Although the US governmental architecture assigned to cyber security is very complex and bureaucratically articulated, with an unspecified number of agencies, offices, commissions, boards, the federal effort to protect US communications and information infrastructure and securing America's digital infrastructure is remarkable as the amount of resources planned to invest in cyber security.

However, the major hindrances to development continue to be the wide dispersion of power among the various stakeholders and the persistent lobbying activities carried out by those opposing the regulation of private networks to facilitate the protection of critical information infrastructures, because it's considered profitless.

Regarding Canada, I have observed a fairly linear frame: Canada has a perception of cyber threats roughly like that of other countries.

However, Canada is a country heavily economically dependent by the massive use of technology. This applies to the use of IT systems made by both citizens for every-day activities and the government. Thus, the primary objectives of the country are securing government systems, partnering to secure vital cyber systems outside the federal government and helping Canadian to be secure online.

Cooperation is the keyword of the whole discourse and in order to achieve efficiently their goals, roles and responsibilities are distinctly enunciated and cooperation among governmental bodies and agencies that work in the security field is mandatory.

Following what has been analyzed from an international perspective, I would like to conclude with few comments on the Italian cyber security landscape.

Some premises are necessary: the digitalization process is an unavoidable path, which in Italy has started to take off around the 90s, thus having acceleration towards the 2000s.

In the recent past, one of the most significant causes of the Italian delay was the fragmentation of interventions that led to duplications and inefficient use of resources. Although with the adoption of the "National Strategic Framework for Cyberspace Security" and the "National Plan for Cyberspace Protection" and with the issuing in 2015 of the "Strategy for the Digital Growth 2014-2020", Italy has greatly remedied.

It is true that in our country, government intervention is required to a greater extent than in other countries, to transform the public administration into an ally of citizens and businesses, to develop our cities into smart communities and to evolve our industrial system so that it will be able to meet the challenge of digital competitiveness.

However, the objective of these strategic measures adopted is not only protection but also to represent a new way of understanding the role of the Government as a market booster and helper of the citizens.

Additionally, the Italian delay is rooted in a cultural problem with strong generational and geographic features: the Italian population, of which a large percentage are elderly, it does not use the internet services and in Southern Italy, both enterprises and citizens, have more deficient digital skills than the rest of country.

Even smaller companies reveal levels of use of network services lower than those of families. This is a deficit that undermines the competitiveness of our country.

In light of this, it should be positively remembered the personal commitment of the former Prime Minister Matteo Renzi in matter of cyber security.

The first evidence of this commitment is definitely the Directive of 1 August 2015, which has found a place in the cyber security architecture elaborated by its predecessor, the Prime

Minister Mario Monti, urging the institutional players to fully implement it, and adding to that cyber security architecture new and shared objectives.

In a nutshell, the Directive identified the following guidelines:

- The strengthening of the ability to identify attacks and react appropriately (starting with the National CERT's and CERT-PA's actions).
- The coordination between institutions to respond to systemic events, recognizing in this context the special role of DIS for the coordination of intelligence activities in cyber security, and renewing the commitment in an adequate Selection & Hiring process and training of the staff.
- The public-private partnership involving strategic companies and managers of critical infrastructures (with a particular role of the CISR).
- A boost for each administration, to take on their proper role in the international meeting tables with cyber security as subject of discussion, such as those of NATO and EU.
- A focus on research and development, in collaboration with universities and research centers.

Already in 2015, the first steps towards the implementation of these strategies have been taken, for example the activation of the National CERT and CERT-PA, and the enhanced activity of DIS in cyber security.

Worthy of mention is the renewed relationship between DIS and universities and public research centers, gathered in the Laboratorio Nazionale di Cyber Security CINI.

Does this mean that everything is proceeding perfectly and smoothly? Of course it doesn't, everything is perfectible, and also our country is involved in recovering at least a ten-year delay on the issue of cyber security readiness.

However, Italy has shown a willingness to improve and to have fully accepted the cyber challenge, and this can be seen by the significant progresses made: Italy has clearly established a vision, a purpose, objectives and priorities to be pursued, following a risk assessment approach; it has responded to cyber threats by developing a clear governmental structure, carrying out a survey of policies, regulations and already existing capabilities.

Moreover, Italy's participation at exercises organized at national, European, or international level, increased at the general level of procedures and capabilities. Indeed, Italy regularly engages in exercises organized by NATO, as for example "Cyber Coalition 2013",[158] Tallinn's CCDCOE and ENISA. Italy also participated to the exercise "CybIt 2013", in which for the first time the private sector was involved as well.[159]

Digital is synonymous with efficiency, transparency, growth, tax evasion's fight, but it is especially the door that opens up to our future. For this reason is also important to allocate resources on Research & Development, and improving the quality of education programs about cyber security, making them available for the people.

That's why it was a positive surprise to witness the former Prime Minister's direct commitment to this issue, assigning approximately 150 million Euros to cyber security through the Italian Stability Law n. 208/2016.

Nowadays, Italy is endowed with professionals and researchers of outstanding value, who work with tenacity and even in objectively difficult conditions, due to the scarcity of public and private investments in the sector, but being still able to produce valuable results.

[158] Ministero della Difesa, *Cyber Coalition 2013: conclusa l'esercitazione NATO di Cyber Defence*, 29 Novembre 2013, http://www.difesa.it/SMD_/Eventi/Pagine/CyberCoalition2013.aspx.

[159] Claudia Cencetti, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014, pag. 105. http://www.iai.it/sites/default/files/iaiq_12.pdf.

Many of our professionals hold important roles in the cyber security industry in the most important companies in the world; and many are those who teach and do research both in Italy and abroad in the most prestigious institutions.

Therefore, Italian Research & Training in cyber security do not require the importation of "*Number Ones*" from abroad. Instead, require greater attention to the university tissue, which is the "nursery" of all Italian skills, and is made up of respected professionals and experts who would gladly put their passion and their knowledge to the service of the country.

The absence of a digital policy in a country may produce very serious damages in the short and medium term, exposing the country to the risk of losing important opportunities of growth, such as skilled jobs in all sectors of industry and services, university and private research, *know-how* production, innovative companies and startups.

Thus, IT security should not be regarded as an unnecessary cost, or worse a general activity's slowdown; on the contrary, it is an indispensable precondition for its exercise. This would be immediately translated in businesses' advantage in terms of competitiveness.

The spread of an information security culture, then, is a decisive factor for the country, not only in a defensive key but also for stimulating economic growth.

References

Bibliography

- Ann Brown K., *Critical Path. A Brief History of Critical Infrastructure Protection in the United States*; Spectrum Publishing Group, Inc. 2006.
- Brunner M. and Suter, E. M., *International CIIP Handbook 2008/2009*. Center for Security Studies, ETH Zurich, 2008.
- Collins, A., *Contemporary Security Studies*, Third Edition, Oxford University Press 2013.
- Gadi, E., *Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War*, Georgetown Journal of International Affairs, Winter/Spring 2008.
- Tikk E., Talihärm A., *International Cybersecurity Legal & Policy Proceedings*, CCD COE Publications, 2010.

Technical Papers

- Auti S., *Resilience against Cyber Attacks, Protecting Critical Infrastructure Information*; WIPRO Ltd Publications, 2014. http://www.wipro.com/documents/resilience-against-cyber-attacks.pdf.
- Baldoni R., *TENACE PROJECT, Critical Infrstructure Protection: threats, attacks and countermeasures*, Research Report, 2014. http://www.dis.uniroma1.it/~tenace/deliverables_eng.php?lang=eng&section=0.
- Cencetti, C., *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014. http://www.iai.it/sites/default/files/iaiq_12.pdf.
- EastWest Institute, *International Pathways to Cybersecurity*. Report of Consultation, Brussels: EastWest Institute, 2010. http://www.ewi.info/system/files/CyberSummaryReport.pdf.
- EIC creates unit for defence of critical information systems. Press release by the Estonian Informatics Centre, 30 Sept. 2009. http://www.ria.ee/eic-creates-unit-for-defence-of-critical-information-systems.
- Fischer, E. A.,*Cybersecurity Issues and Challenges: In Brief*, Congressional Research Service Government of Canada, 2015 Budget. http://www.budget.gc.ca/2015/docs/plan/ch4-3-eng.html.
- Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F., *Italy Cyber Readiness at a Glance*, Potomac Institute for Policy Studies Publications, November 2016. http://www.potomacinstitute.org/images/CRI/PIPS_CRI_Italy.pdf.

- ICDRM, *Emergency Management Glossary of Terms*, Institute for Crisis, Disaster, and Risk Management, The George Washington University, January 2009. https://www2.gwu.edu/~icdrm/publications/PDF/EM_Glossary_ICDRM.pdf
- Klimburg A., *The Whole of a Nation in Cyberpower*; http://journal.georgetown.edu/wp-content/uploads/2015/07/171_gj124_Klimburg-CYBER-2011.pdf.
- Klimburg A., *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.
- Klimburg A. and Mirtl P., *Cyberspace and Governance – A Primer (Working Paper 65)*, Austrian Institute for International Affairs, Spetember 2012, http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Cyberspace_and_Governance_-_Working_Paper_65_2.pdf.
- Maulny, J. P., and Sarraf, S., *Assessment and Prospects of Security Threats*, Report of Institute de Relations Internationales et Stratégiques, April 2016. http://www.iris-france.org/wp-content/uploads/2016/04/TAC-Report-2016-ENG-V3.pdf.
- Pernik,P.,Wojtkowiak, J., Verschoor-Kirss, A., *National Cyber Security Organisation: United States*, page 15, CCCDCOE Publications, Tallinn 2016.
- Potter, E. H., *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, McGill Queen's University Press, page 7.
- Rattray, G. and Healey, J., *Categorizing and Understanding Offensive Cyber Capabilities and Their Use, in Proceedings of a Workshop on Deterring Cyberattacks. Informing Strategies and Developing Options for U.S. Policy*, ed. National Research Council (Washington, DC: The National Academies Press, 2010).

- Robinson, N., Gribbon, L., Horvath, V., Robertson, K., *Cyber-security Threat Characterisation*, Rand Europe Report, page 27, RAND Corporation Publications, 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf
- Setola, R., Rapporto di Ricerca 2011, *La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici*, Centro Militare di Studi Strategici CEMISS, http://www.masterhomelandsecurity.eu/wp-content/uploads/2012/08/Protezione-infrastrutture-e-risorse-critiche_Setola.pdf.

Official Documents

- Canada's Cyber Security Strategy, 2010, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf.
- *Chancellor Speech: Launching the National Cyber Security Strategy*, from HM Treasury and the Hon. Philip Hammond MP, November 1, 2016, https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy
- Commissione Europea, *Sicurezza delle Reti e dell'Informazione: proposta di un approccio strategico europeo*, COM 2001/298, 6 Giugno 2001.
- Consiglio dell'Unione Europea, *Un Europa sicura in un mondo migliore. Strategia Europea in materia di sicurezza*. 12 Dicembre 2003, pag. 2.
- Consiglio dell'Unione Europea, *Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione* (S407/08), 11 Dicembre 2008.
- Decreto del Presidente del Consiglio dei Ministri, 24 Gennaio 2013, http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.
- Directive (Eu) 2016/1148 of the European Parliament and of the Council of 6 July 2016. http://eur-lex.europa.eu/legal-content/EN-IT/TXT/?uri=CELEX:32016L1148&from=EN.
- Directive of the council on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection. COM (2006) 787, Brussels, 2006.

- Directive on security of network and information systems (NIS Directive), July 2016. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
- Direttiva 1 Agosto 2015, Sistema di Informazione per la Sicurezza della Repubblica. https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html.
- Dutch Ministry of Housing, Spatial Planning and the Environment, Handreiking Security Management, (The Hague: Dutch Ministry of Housing, Spatial Planning and the Environment, 2008), http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2010/11/26/handreiking- security-management/11br2008g225-2008613-154851.pdf.
- ENISA, National Cyber Security Strategies. Practical Guide on Development and Execution. December 19, 2012. https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.
- *Estonian Cyber Security Strategy 2014 – 2017*, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.
- European Union Directive 2008/114/EC, 2008.
- *Fact Sheet: The Department of Defense (DoD) Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf.
- Ministero dell'Economia e Finanza, Legge di Stabilità 2016, 8 Gennaio 2016, http://www.mef.gov.it/focus/article_0014.html.

- Ministero della Difesa, *Cyber Coalition 2013: conclusa l'esercitazione NATO di Cyber Defence*, 29 Novembre 2013, http://www.difesa.it/SMD_/Eventi/Pagine/CyberCoalition2013.aspx. Per maggiori informazioni, si veda ISO/IEC 27001 – Information Security Management, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.
- National Security Strategy and Strategic Defence and Security Review 2015, *A Secure and Prosperous United Kingdom.* November 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf.
- National Security Concept of Estonia 2010, available at https://www.eda.europa.eu/docs/default-source/documents/estonia---national-security-concept-of-estonia-2010.pdf.
- Office of Cyber Security and Information Assurance, https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.
- Presidency of the Council of Ministers, *The National Plan for Cyberspace Protection and ICT Security*, December 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf.
- Presidency of the Council of Ministers, *The National Strategic Framwork for Cyberspace Security*, December 2013, page 12 https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf.
- Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza*, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/relazione-2013.pdf

- Public Safety – Canada, Canada's Cyber Security Strategy, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx.
- Presidenza del Consiglio dei Ministri, *Strategia per la Crescita Digitale 2014 – 2020*, Marzo 2015. http://www.agid.gov.it/sites/default/files/documentazione/strat_crescita_digit_3marzo_0.pdf
- Regolamento (CE) n. 460/2004 del 10 marzo 2004, che istituisce l'Agenzia Europea per la sicurezza delle reti e dell'informazione, art. 1.1.
- *The DoD Cyber Strategy*, 17 April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
- The White House, Office of the Press Secretary, *FACT SHEET: Cybersecurity National Action Plan*, February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.
- The White House, Office of the Press Secretary, Presidential Policy Directive PPD/41, *United States Cyber Incident Coordination*, July 26, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
- U.K. National Cyber Security Strategy 2016 – 2021, page 17. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
- U.S. Coast Guard, *'United States Coast Guard Cyber Strategy'*, p.21, Department of Homeland Security, 2015 https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf; U.S.

Central Intelligence Agency, 'Executive Order 12333', 1981 https://www.cia.gov/about-cia/eo12333.html.

- U.S. Department of Commerce, *Cybersecurity, Innovation, and the Internet Economy (Green Paper)*, (Gaithersburg, MD: NIST, 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.
- US Department of Homeland Security, National Incident Management System, (Washington,DC: FEMA, 2008), http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.
- U.S. Joint Chiefs of Staff, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, (Ft. Belvoir, VA: DTIC, 2012), http://www.dtic. mil/doctrine/new_pubs/jp1_02.pdf.).
- United States Government Accountability Office, Report to Congressional Addressees, *CYBERSECURITY: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, February 2013. http://www.gao.gov/assets/660/652170.pdf.
- United States Government Accountability Office, Report to Congressional Requesters, *CYBERSPACE: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, July 2010. http://gao.gov/assets/310/308401.pdf.

Journal and Newspaper Articles

- Gayathri, A., *Iran To Shut Down Internet Permanently; 'Clean' National Intranet In Pipeline',* International Business Times, 9 April 2012.
- Gorman, S., and Barnes, J. E., *'Cyber Combat: Act of War',* The Wall Street Journal, 30 May 2011.
- Internazionale, *Cos'è il Datagate e come è cominciato*, 25 Giugno 2015, http://www.internazionale.it/notizie/2015/06/25/datagate-snowden-spionaggio.
- *Il Futuro della Cyber Security in Italia*, 18 Novembre 2015, https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/il-futuro-della-cyber-security-in-italia.html.
- *La Sicurezza del Cyberspazio Come Priorità Strategica*, 25 Novembre 2015, https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-sicurezza-del-ciberspazio-come-priorita-strategica.html.
- Licata, P., *Come migliorare la sicurezza cyber in Italia. Le idee di Masiello (Palazzo Chigi)*, F!, http://formiche.net/2016/08/05/come-migliorare-la-sicurezza-cyber-italia-le-idee-di-palazzo-chigi/.
- Locatelli, L., *In Estonia, sul fronte della cyber guerra*, L'Espresso, 24 Settembre 2014, http://espresso.repubblica.it/plus/articoli/2014/09/22/news/in-estonia-sul-fronte-della-cyberguerra-1.181073.
- Martin, *Canada commits $36.4 million to cybersecurity measures in 2015 budget,* We Live Security, April 22, 2015. http://www.welivesecurity.com/2015/04/22/canada-commits-36-4-million-cybersecurity-measures-2015-budget.

- O’Dwyer, G., *Interview: Estonian Defence’s Minister Hannes Hanso,* DefenseNews, February 3, 2016. http://www.defensenews.com/story/defense/policy-budget/leaders/interviews/2016/02/03/interview-estonias-defence-minister-hannes-hanso/78845280/.
- Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K., Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, pages 11-25, December 2011.
- We Need to Talk about Cyber Security; http://www.airport-business.com/2014/06/need-talk-cyber-security/.
- Zeltser, L., *The Big Picture of the Security Incident Cycle*, Computer Forensics and Incident Response, 27 September 2010.

Sitography

- Associazione Italiana esperti in Infrastrutture Critiche AIIC; http://www.infrastrutturecritiche.it/aiic/.
- Centre for the Protection of National Infrastructure; http://www.cpni.gov.uk/Templates/CPNI/pages/Default.aspx.
- CIO; http://www.cio.com.
- Critical Infrastructures Protection and Resilience EUROPE; http://www.cipre-expo.com.
- Critical Infrastructure Protection in the EU; CEPS Centre for European Policy Studies https://www.ceps.eu/content/critical-infrastructure-protection-eu.
- Cyber Security, e-Estonia.com - The Digital Society, https://e-estonia.com/the-story/digital-society/cyber-security/.
- Cyber Security, Republic of Estonia, Ministry of Economic Affairs and Communications, available at https://www.mkm.ee/en/objectives-activities/information-society/cyber-security#cyber-crime1.
- Department of Homeland Security U.S.; https://www.dhs.gov.
- DISA Vice Director talks cybersecurity, jointness; http://www.c4isrnet.com/videos/military-tech/show-reporter/disa-forecast/2015/11/04/75045812/.
- *EU International Cyberspace Policy*, https://eeas.europa.eu/topics/eu-international-cyberspace-policy_en.

- European Commission website, Critical Infrastructure Section, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm.
- Federal Emergency Management Agency, FEMA; http://training.fema.gov/emi.aspx.
- George Mason University, Center for Infrastructure Protection and Homeland Security; http://cip.gmu.edu.
- National Cyber Security Centre, https://www.ncsc.gov.uk/about-us.
- National Security Agency / Central Security Service NSA/CSS, https://www.nsa.gov/index.shtml.
- NATO Cooperative Cyber Defence Centre of Excellence; https://ccdcoe.org.
- Sistema di Informazione per la Sicurezza della Repubblica; https://www.sicurezzanazionale.gov.it/sisr.nsf/index.html.
- *The Comprehensive National Cybersecurity Initiative,* The White House, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.
- *The importance of safety, security and justice*, GSDRC, Applied Knowledge Services. http://www.gsdrc.org/topic-guides/safety-security-and-justice/concepts/the-importance-of-safety-security-and-justice
- The Information Warfare Site; http://www.iwar.org.uk.
- U.S. CyberSecurity in the 21st Century; http://www.cfr.org/united-states/us-cybersecurity-21st-century/p37192.
- U.S. Department of Justice, The Federal Bureau of Investigation (FBI), *'National Cyber Investigative Joint Task Force (NCIJTF)'* http://www.fbi.gov/about-us/investigate/cyber/ncijtf.

Miscellaneous

- Public Private Partnerships for Critical Infrastructure Protection; http://csis.org/files/publication/130819_PPP.pdf

Executive Summary

Today, the challenge posed by cyber security is a topic widely discussed and of significant importance.

The cyber domain is still a largely unexplored area and this has consequences that cannot be underestimated.

With the advent of the Internet, the increasing development of technology and the increasing role they take on in the daily life of every individual, protecting while ensuring the continuous operation of the cyber space, it becomes imperative.

Governments around the world, but especially those of the most advanced countries, are facing an issue that grows hand in hand with technological development. Technological progress could become then a double-edged sword if adequate measures are not adopted.

In the present study will be analyzed several aspects related to cyber security, to be read in a comparative perspective with the Italian situation.

In the first chapter will be provided a set of basic definitions: the importance of the critical infrastructure for the proper functioning of industrialized societies and their growing interdependence.

Then it will be explained how this interdependence makes them targets vulnerable to cyber attacks and thus why it is crucial that each country considers the protection of critical infrastructure as a key objective to achieve.

Firstly, in order to protect critical infrastructures from cyber attacks it should be made a proper distinction of both the types of attacks that can be perpetrated and the actors who can be held responsible for such attacks. Each attack has its own modality, its own specific goal, and the responsible/s behind the attack it belongs always to a specific typology of actors driven by a

number of precise reasons.
All these parameters cannot be ignored otherwise the risk is of missing the ultimate goal, which is the protection and at the same time assurance of the operational continuity of critical infrastructures.

The concept of cyber security has always been linked to the problem of information: the interdependence between different software-based control systems has always been a sensitive target that required appropriate protection for allowing to the post-industrial economies continuous and reliable operation as well as for ensuring national security.

Then, from this consideration, the critical information infrastructures emerged as a referent object.

Information, in turn, has always been an aspect related to power, diplomacy and armed conflict. Therefore, in light of this, the cyber domain falls perfectly into logics of geopolitics and international competition.

Providing the population of a country an access to a safe space where information can be safely exchanged or kept is a priority and intrinsic to national security.

The concept of national cyber security will be explained in section 1.3.

In the second chapter, the investigation adopts a broader perspective to look at the issue: the cyber threat is a global problem. Each country decides to avail itself of a series of tools in countering cyber crime.

How countries decide to profit from these tools and the posture of a country towards the cyber issue are well explained in a comprehensive document that every country possesses and that will be fully explained, which is the National Cyber Security Strategy.

A National Cyber Security Strategy can be developed through a number of methods and should always be combined with adequate resources.

The principal mandates composing a National Cyber Security Strategy are the followings: Military Cyber Operations, Counter Cyber Crime, Critical Infrastructure Protection (CIP) & Crisis Management, Intelligence/Counter-Intelligence, and Cyber Diplomacy & Internet Governance.

This five mandates are exhaustively explained because they are indispensable for setting up the skeleton of a National Cyber Security Strategy, and they are also intertwined with four levels of government, namely the political/policy, strategic, operational and tactical levels, and with three so-called "*cross-mandates*": Information Exchange & Data Protection, Coordination as well as Research & Development and Education.

The importance to understand each of these mandates, to understand the differences among them but also the analogies, is pivotal to allow a more harmonized joint effort, which is directly linked to the powerfulness of a given National Cyber Security Strategy in achieving the prearranged goals.

The development of a National Cyber Security policy has to deal with many challenges both known and unknown. Furthermore, since both the national and international environment brings with it a large set of pre-existing treaties, the obstacles to the freedom of policymakers increase.

For this reason, it would be an optimum if all the cyber security policies would be connected to a homogeneous architecture, which is entitled to manage the Information Security System, and at the same time reducing redundancies and overlapping legislations.

In this regard, NATO has recently increased its focus on cyber security and its cooperation with non-NATO nations, the European Union and International Organizations as well. But, unfortunately, there is still a lot of work that has to be done before achieving the so long-wished smooth synergy between all actors involved in cyber security.

Moreover, in the second chapter, regarding the analysis of the National Cyber Security Strategy, the European Union has been considered as a subject of investigation too, because as a supranational institution that legally binds its Member States, could not be ignored. Indeed, the effects of European policies in cyber security, along with other field's policies, easily spill over the legal frameworks of the Member States.

Four countries have been selected as case studies: United Kingdom, Estonia, United States of America and Canada.

These countries have been taken as examples of *best practices* based on their high level of development in this field, as well as their implementation of top quality strategies and more sophisticated cyber-responses.

For what concerns United Kingdom, I have shown that cyber security is considered a vital topic.

This emerges clearly from the National Cyber Security Strategy of the country, considering several measures adopted: the equalization – in terms of risk and impact – of cyber threats to terrorism or military conflict; the establishment of a Cyber Permanent Committee composed of various government members from different government departments, remarking the will of the central government to work collaboratively; a multiplicity of authorities responsible for the management of the cyber issue; finally, the massive investment of £ 1.9 billion for the defense of the systems and infrastructure, deterrence of adversaries and development of whole-society capabilities.

Estonia, known for the cyber attacks endured in 2007, gave birth to a framework purely imbued on resilience. Since 2009, a number of important decisions that have been taken have allowed Estonia to become today one of the reference countries with regard to progress in the cyber security field.

The central body that deals with cyber security is the RIA (Estonian Information System Authority) and it is also noteworthy its close cooperation with NATO CCDCOE of Tallinn, through which play a crucial role in cyber defense.

The main objectives are improving Estonian defense of critical infrastructure, investing substantially in the military, and improving resilience. Although, the defense budget for 2016 was fairly modest, it is set to rise year-on-year by around 7%. Estonia's achievements in cyber security have also benefitted from a strong IT partnership between the public and private sector. This conjunction gave birth to the Cyber Defence League.

However, the real key to Estonian cyber security lies in the inherent safety and security built-in to every single Estonian e-Government and IT infrastructure system. Estonian citizens and businesses operate with confidence, knowing that their data is safe and their transactions are secure.

Indeed, the best kind of cyber security is one that everyday people never have to think about.[160]

For the United States, although the problem is not unknown nor has recent origin, it has long been at the center of debates. The same American concept of cyber threat has changed a lot over time, going hand in hand with the attacks and events that involved the country over the years.

The emphasis has shifted from non-state terrorism to state actors' activities, and predominantly from a political to an economic matter.

Terrorism has always been a top-priority threat to address for United States, but the improvements made in the digital field have brought US to reconsider the security's global framework giving to cybercrime the proper credit. The same former President Obama has identified cyber threats as one of the more serious economic and national security challenges of all times.

[160] Cyber Security, e-Estonia – The Digital Society, https://e-estonia.com/the-story/digital-society/cyber-security/.

Although the US governmental architecture assigned to cyber security is very complex and bureaucratically articulated, with an unspecified number of agencies, offices, commissions, boards, the federal effort to protect US communications and information infrastructure and securing America’s digital infrastructure is remarkable as the amount of resources planned to invest in cyber security.

However, the major hindrances to development continue to be the wide dispersion of power among the various stakeholders and the persistent lobbying activities carried out by those opposing the regulation of private networks to facilitate the protection of critical information infrastructures, because it’s considered profitless.

Regarding Canada, I have observed a fairly linear frame: Canada has a perception of cyber threats roughly like that of other countries.

However, Canada is a country heavily economically dependent by the massive use of technology. This applies to the use of IT systems made by both citizens for every-day activities and the government. Thus, the primary objectives of the country are securing government systems, partnering to secure vital cyber systems outside the federal government and helping Canadian to be secure online.

Cooperation is the keyword of the whole discourse and in order to achieve efficiently their goals, roles and responsibilities are distinctly enunciated and cooperation among governmental bodies and agencies that work in the security field is mandatory.

The chapter concludes with a glance to the Italian landscape, the guidelines followed and the challenges that Italy is tackling.

The third and final chapter will dedicate more space to the Italian current situation. After having explained in broad terms what is the attitude of Italy towards cyber security, here, the aim of the research is to depict the Italian current profile in matter of cyber security through a comparison with the other countries previously studied and following three lines of enquiry.

These lines revolve around:

1) The concept of threat and how threat is characterized within the cyber security picture.

A great challenge for all those engaged in the cyber field is coming to grips with the fluidity of the cyber domain. This fluidity implies a multiplicity of definitions of the actors involved, the measures to undertake and even what constitutes a threat. Clarifying the concept of threat can certainly be useful in order to better assess the proper measures to undertake for countering crime. Indeed, at the bottom of every risk assessment strategy there is the cyber threat concept.

2) The level of prioritization attributed to cyber threats by each State.

The challenge posed by cybercrime has led the most developed countries to amend their legislations to better cope with this issue. Some countries have even equated the cyber threat to others identically significant such as terrorism, for example.
Thus, according to the level of prioritization assigned, each country has adopted the response measures deemed adequate

3) The identification of leading authorities responsible of policies, law enforcement, and their roles.

Establishing who has to be in charge of managing the cyber security of a country is a significant decision. There are countries that opt for a solution implying a centralized control system and others that prefer a decentralized structure. Both aspects carry along consequences in terms of benefits and losses.

After a concise overview of the governmental architecture designated to cyber security by each of the countries taken as case study, it will be deduced which one of the two aspects is better in relation to efficiency and resilience, or if a mixed approach would be more adequate. Resources allocation is another key topic in cyber security. Thus, it won’t be excluded from the discussion because it proves the concrete commitment of a country towards the issue and, of course, it gives a preview of the range of improvement that might occur in the field.

Even though in a comparative study there are many parameters that could be taken in consideration, these three are the selected ones to proceed with the study, because they have been considered important parameters that logically and prominently arose from the inquiry completed in the second chapter.
The last paragraph of the third chapter will illustrate the multifaceted framework in which Italy is entangled: following what has been analyzed from an international perspective, I have concluded with few comments on the Italian cyber security landscape.

Some premises are necessary: the digitalization process is an unavoidable path, which in Italy has started to take off around the 90s, thus having acceleration towards the 2000s.

In the recent past, one of the most significant causes of the Italian delay was the fragmentation of interventions that led to duplications and inefficient use of resources.

Although with the adoption of the “National Strategic Framework for Cyberspace Security” and the “National Plan for Cyberspace Protection” and with the issuing in 2015 of the “Strategy for the Digital Growth 2014-2020”, Italy has greatly remedied.

It is true that in our country, government intervention is required to a greater extent than in other countries, to transform the public administration into an ally of citizens and businesses, to develop our cities into smart communities and to evolve our industrial system so that it will be able to meet the challenge of digital competitiveness.

However, the objective of these strategic measures adopted is not only protection but also to represent a new way of understanding the role of the Government as a market booster and helper of the citizens.

Additionally, the Italian delay is rooted in a cultural problem with strong generational and geographic features: the Italian population, of which a large percentage are elderly, it does not use the internet services and in Southern Italy, both enterprises and citizens, have more deficient digital skills than the rest of country.

Even smaller companies reveal levels of use of network services lower than those of families. This is a deficit that undermines the competitiveness of our country.

In light of this, it should be positively remembered the personal commitment of the former Prime Minister Matteo Renzi in matter of cyber security.

The first evidence of this commitment is definitely the Directive of 1 August 2015, which has found a place in the cyber security architecture elaborated by its predecessor, the Prime Minister Mario Monti, urging the institutional players to fully implement it, and adding to that cyber security architecture new and shared objectives.

In a nutshell, the Directive identified the following guidelines:

• The strengthening of the ability to identify attacks and react appropriately (starting with the National CERT’s and CERT-PA’s actions).

• The coordination between institutions to respond to systemic events, recognizing in this context the special role of DIS for the coordination of intelligence activities in cyber security, and renewing the commitment in an adequate Selection & Hiring process and training of the staff.

• The public-private partnership involving strategic companies and managers of critical infrastructures (with a particular role of the CISR).

• A boost for each administration, to take on their proper role in the international meeting tables with cyber security as subject of discussion, such as those of NATO and EU.

• A focus on research and development, in collaboration with universities and research centers.

Already in 2015, the first steps towards the implementation of these strategies have been taken, for example the activation of the National CERT and CERT-PA, and the enhanced activity of DIS in cyber security.

Worthy of mention is the renewed relationship between DIS and universities and public research centers, gathered in the Laboratorio Nazionale di Cyber Security CINI.

Does this mean that everything is proceeding perfectly and smoothly? Of course it doesn't, everything is perfectible, and also our country is involved in recovering at least a ten-year delay on the issue of cyber security readiness.

However, Italy has shown a willingness to improve and to have fully accepted the cyber challenge, and this can be seen by the significant progresses made: Italy has clearly established a vision, a purpose, objectives and priorities to be pursued, following a risk assessment approach; it has responded to cyber threats by developing a clear governmental structure, carrying out a survey of policies, regulations and already existing capabilities.

Moreover, Italy's participation at exercises organized at national, European, or international level, increased at the general level of procedures and capabilities.

Indeed, Italy regularly engages in exercises organized by NATO, as for example "Cyber Coalition 2013",[161] Tallinn's CCDCOE and ENISA. Italy also participated to the exercise "CybIt 2013", in which for the first time the private sector was involved as well.[162]

Digital is synonymous with efficiency, transparency, growth, tax evasion's fight, but it is especially the door that opens up to our future. For this reason is also important to allocate resources on Research & Development, and improving the quality of education programs about cyber security, making them available for the people.

That's why it was a positive surprise to witness the former Prime Minister's direct commitment to this issue, assigning approximately 150 million Euro to cyber security through the Italian Stability Law n. 208/2016.

Nowadays, Italy is endowed with professionals and researchers of outstanding value, who work with tenacity and even in objectively difficult conditions, due to the scarcity of public and private investments in the sector, but being still able to produce valuable results.

Many of our professionals hold important roles in the cyber security industry in the most important companies in the world; and many are those who teach and do research both in Italy and abroad in the most prestigious institutions.

Therefore, Italian Research & Training in cyber security do not require the importation of "*Number Ones*" from abroad. Instead, require greater attention to the university tissue, which is the "nursery" of all Italian skills, and is made up of respected professionals and experts who would gladly put their passion and their knowledge to the service of the country.

[161] Ministero della Difesa, *Cyber Coalition 2013: conclusa l'esercitazione NATO di Cyber Defence*, 29 Novembre 2013, http://www.difesa.it/SMD_/Eventi/Pagine/CyberCoalition2013.aspx.

[162] Claudia Cencetti, *Cybersecurity: Unione Europea e Italia. Prospettive a confronto*, Quaderni IAI Pubblicazioni, 2014, pag. 105. http://www.iai.it/sites/default/files/iaiq_12.pdf.

The absence of a digital policy in a country may produce very serious damages in the short and medium term, exposing the country to the risk of losing important opportunities of growth, such as skilled jobs in all sectors of industry and services, university and private research, *know-how* production, innovative companies and startups.

Thus, IT security should not be regarded as an unnecessary cost, or worse a general activity's slowdown; on the contrary, it is an indispensable precondition for its exercise. This would be immediately translated in businesses' advantage in terms of competitiveness.

The spread of an information security culture, then, is a decisive factor for the country, not only in a defensive key but also for stimulating economic growth.