Department of Political Sciences

International Public Policies

Cybersecurity: The New Global Arena

A Franco-Italian Perspective

SUPERVISORS:

Prof. Raffaele MARCHETTI

Prof. Julien PIERET

MATTHIEU MAZERAT
Student Reg. No. 635592

CO-SUPERVISOR:

Prof. Roberta MULAS

Academic Year 2017-2018

Acknowledgements

First of all, I would like to thank my alma mater supervisor, Julien Pieret, to have helped me all along the way. His constructive suggestions and his commitment were always very appreciated and helped me unravel the complexity of my topic. He was also comprehensible and provided me with a critical look during the planning and development of this research work, which allowed to better grasp the essence of a thesis work.

Then, I would like to offer my special thanks to my Italian supervisor, Raffaele Marchetti, who accepted my project and provided with new elements which allowed me to shed a new light upon my work. He suggested the comparison of the French and Italian cases, which turned out to give my work more sense and range, especially within the framework of this double degree.

I would also like to extend my thanks to both LUISS and ULB staff, especially Pascale Meekers, Teresa Chiriatti and Camilla Vignanotti for their time and advice during the whole year, giving us the best conditions to enjoy this year.

I am particularly grateful for the assistance given by Emilien Paulis, who believed in my project from the beginning onwards and was to first to provide me guidance for this long-term hardship.

My gratitude goes also to Coralie, Jason and Géraldine. We started this joint endeavor as colleagues and ended up as friends. Sharing with them had a very important impact in the shaping this thesis and I am happy we faced these hard times together.

I want to extend my gratitude to my dearest friend Jamie who helped me in reviewing this work and provided me with precious advice and to Francois, without whom I would not even be studying political sciences. Thank you for bringing me back into the academic field.

To my better half, Anaïs, gracias por todo.

Finally, I wish to thank my parents and my family for their never-ending support and encouragement throughout my study. My gratitude towards them is endless as without them, all of this would not have been possible.

List of initialisms, acronyms and abbreviations

For the sake of clarity, I have listed here all the acronyms used in my work. The shortened version corresponds to the acronyms in the source language whereas the detailed version is the official translation.

AgID : Agency for Digital Italy
AIISI: Internal Intelligence and Security Agency
AISE: External Intelligence and Security Agency
ANSSI: National Information Systems Security Authority/ National Cybersecurity Agency of France (ANSSI)
CALID: Analysis Centre for Cyber Defensive Operations
CCDCOE: Cooperative Cyber Defence Centre of Excellence
CERT: Computer emergency response team
CINI: National Interuniversity Consortium for Informatics
CIOC: Joint Headquarters Cyber Operations
CIRC: Computer Incident Response Capability
CISR: Interministerial Committee for the Security of the Republic
CITDC: Interministerial Technical Commission for Civil Defence
CNAIPIC: Computer Centre for the Protection of Critical Infrastructure
CNCTR: Commission for the Control of Intelligence Techniques
COPS: Political Strategic Committee
CPCO: Planning and Operations Centre
DGA: Defence Procurement Agency
DGA-MI: Information Assurance Division of the DGA
DGRIS: Directorate General for International Relations and Strategy
DGSIC: Director of the Defence Information and Communication Systems
DICOD: Defence Communications and Information Delegation
DIS: Security Intelligence Department
ENISA: European Union Agency for Network and Information Security
LPM: Military Programming Law/Act
NATO: North Atlantic Treaty Organization
NISP: Interministerial Situation and Planning Unit
NSC: Cyber Security Unit
RCC: Cyber Military Civil (2013)
RCD: Operational Cyber Reserve (2016)
SGA: DGA delegate
SGDSN: Secretary General for Defence and National Security
SISR: Italy's Intelligence System for the Security of the Republic

Table of Contents

"*The weak point is located between the chair and the keyboard.*"
Anonymous, 2012

"For it is about mere words that men usually quarrel.
It is for the sake of words that they most willingly kill and are killed."
Anatole France, 1897

Introduction

From 1993 to 2012, the stance on cyberwar moved from "Cyberwar is Coming" to "Cyber War Will Not Take Place"(Arquilla and Ronfeldt 1993; Rid 2012). Why such a change in tone? Has the field of cybersecurity been studied so extensively in the past two decades that we can now just take our understanding for granted and move on? Indeed, a proper cyberwar leading to casualties and involving one state retaliating against another has not yet occurred. Nonetheless, if such a hard power scenario of cyberconflict has not taken place, new global issues point to the emergence of a subtler and softer form of cyber power (Nye Jr 2010). Indeed, information warfare, taking mainly the form of psychological warfare, plays a substantial role in our societies (Libicki 1995). In this regard, the recent unfoldings of the American, French, and Italian elections serve as a reminder that nowadays even the smallest unit in international relations - the individual - is subject to manipulation through the proliferation of distorted factual representations, namely the so-called fake news phenomenon that sows confusion on social networks. Thus, cyberwar, even though seemingly less lethal, has not disappeared from the horizon, but is rather taking various shapes affecting different actors on different levels. One of my former teachers, Dr. Rain Ottis, associate Professor in Tallinn University of Technology (Estonia), during his lectures on cybersecurity at the University of Jyväskylä (Finland), used to highlight that the human factor had to be considered in the cybersecurity equation. In other words, though a state may have the most powerful computers inside the most secure building in the world, it only takes one person to compromise a whole network. In fact, during recent years, social engineering implying hacking human behavior, has been one of the most recurrent components of attacks.

Topics related to the cyber-sphere have received much attention over the past decade. This sudden interest reflects shared feelings of both enthusiasm and fear. Indeed, while it can be said that the development of ICTs has brought about positive changes in our society, their ever-growing use and omnipresence raise a lot of concerns. All technologies relying on networks and more specifically on the so-called Internet infrastructure are bound to be, if it is not already the case, corrupted. An emblematic example of this pervasiveness occurred during April of 2007 in Estonia, whose whole national internet network was paralyzed (Dragosei 2007; The New York Times 2007; Hansen and Nissenbaum 2009:1159). For some, it even echoes as Web War One (Blank 2008).

While this statement can be discussed, the reactions it triggered within the international community speak for themselves. For example, the setting up of the North Atlantic Treaty Organization (NATO), the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in 2008, the creation of the European Union Agency for Network and Information Security in 2014, the drafting of two Manuals on the International Law applicable to cyberwarfare and cyberoperations, respectively in 2013 and 2017 [1]. Yet, while these international initiatives received public attention, within states, governments also pushed forward laws and national strategies taking this new cyber threat landscape into account. As a matter of fact, as presented by Baumard, most national cybersecurity strategies were implemented during the 2006–2016 period (Baumard 2017:12). These implementations have been studied in many ways by tacticians, thinks tanks and political science researchers. Nonetheless, we can point to two main methodologies.

The first methodology draws upon various approaches, borrowing concepts from traditional international relations theories and law. Based on hard facts, it mainly consists in listing the capabilities of a state, both offensive and defensive, following a framework built for that purpose (Ball 2011; Cavelty 2014; Baumard 2017) or rely on non-scientific comparative analysis frameworks. Overall, this comprehensive method has proved beneficial in the comprehension of conventional warfare analysis. Yet, its main shortcoming is the inability to take into account the cyberspace pluridisciplinary. The second central methodology draws upon constructivist theories, especially Securitization theory of the Copenhagen School, which explains how an issue becomes protected through discourse (Buzan, Wæver, and De Wilde 1998). Most of the time, researchers noticed that national interest was put forward in the constructivist discourse to uphold political or military actions or explain states' behavior. In that regard, the securitization of cyberspace is not an exception and follows the same pattern (Kempf 2012:190).

From a general point of view, the cyberissue raises many questions: How does the cyber element push states to rethink their national defense strategy? What does it add to the equation? Does it constitute a new "cybersecurity dilemma" (Council 2007; Buchanan 2017)? What about the attribution of this attack (Tsagourias 2012)? In terms of results, they are two opposite sides to these questions: on one side, researchers tend to consider that this cyber element does not change the rules of the game and only adds a new modality to warfare in general and does not

[1] NATO-commissioned initiative without endorsement of the views reflected within.

justify any changes from both states and the international community. On the other side, with whom we concur, the cyber as a new domain increases the complexity on the battlefield and brings up a whole series of new considerations to the fore, which justify rethinking the way we traditionally perceive warfare. All of these considerations help and push states to undertake strategies encompassing cyberspace. That being said, the research question around which our work will be revolved is the following:

To what extent does cyberspace constitute a way to reaffirm a country's national interests through the implementation of its cyberstrategy? The aim of this research is to show to what extent States remain locked within a realist paradigm - in which the pursuit of the national interest remains crucial - while simultaniously reshaping the way they conceive modern warfare, and particularly by securitizing their cyberspace to better cope with new challenges. To do so, we will conduct a comparative analysis between France and Italy.

Therefore, the very interest of our work lies in the way states construe cyberspace and shape a discourse fitting their interests. To that end, reports, white papers on cyberdefence and bills from the two governments will be used to complete different frameworks. As Baumard illustrated, the year 2007 was a turning point in the way states think their cyberstrategy (Baumard 2017:13). Thus, the period concerned goes from 2008 to 2018. As far as the year 2018 is concerned, this corresponds to the latest publication of the French government (Légifrance 2018), hence the selection of this date.

The relevance and aim of this thesis can be summed up in four points. Firstly, the cases selected for this comparative analysis (France and Italy) and the domain (securitization of the cyberstrategy) have not been studied together so far, at least not to our knowledge and not in this fashion. Secondly, the frameworks used for conducting the analysis have been updated, including not only the original criteria but also new inputs built especially for this analysis, drawing upon both realist and constructivist theories. Not only does such a mix allow to provide more tools to portray the reality, it also contributes to the development of the cybersecurity field. Thirdly, political science literature on cybersecurity does not present many studies using a realist-constructivist framework coupled with a discourse-theoretical approach. Thus, adopting a crossover theoretical approach will give a new perspective to general international relations studies and shed a different light upon a current phenomenon, and better explain state behavior as far as (cyber-) national defense is concerned. Fourthly, the operationalization of the concepts provided to answer the research question is twofold. The first step is dedicated to causative factors, drawing upon Baumard's typology of national cyberdoctrines (Baumard

2017:69–72) and a framework updated by our care. The second step relies on stating the concrete actions undertaken by states and is more descriptive. As a matter of fact, the dual qualitative-quantitative approach has already been applied for the securitization of the American cyberspace (Hjalmarsson 2013:5). Though, unlike Hjalmarsson, we plan on using a lexicometry software whose relevance has already been put forward (Mayaffre and Poudat 2013; Borriello 2017).

In summary, the aim of this thesis is to compare the implementation of the cyberissues inside the national defense strategies of France and Italy using a crossover approach: applying a constructivist analysis of both national cyberstrategy, underpinning the underlaying realists' interests involved in the discourse.

It goes without saying that such method can raise some criticism. One could argue for instance that the work is limited to two cases only and cannot help in detecting trends or decision patterns that could be applied to any country. However, inferring such a thing would be to mistake the primary aim of this work. Indeed, the intention of our study is to find a correlation between the securitization of cyberspace through the implementation of cyberstrategy and the lexical field/built categories put forward to achieve it. Thus, the mix between qualitative and quantitative appears justified and relevant. On the one hand, our dominant approach is qualitative and is therefore perfectly suitable to a restrictive number of cases, as it allows to focus on specific factors (Coman et al. 2016:34). On the other hand, the dual approach, an extensive comparison analysis and a comparison of the priorities highlighted through the discourse, allows to support our hypothesis. Nevertheless, the use of the quantitative approach, namely the lexicometry software TXM, only comes into play to corroborate our hypothesis. Then, the lack of a unified framework allowing "systematic and comparative empirical analysis" within the Copenhagen School is sometimes pointed out (Stritzel 2007:358). However, by drawing upon Baumard, Klingova as well as Hanssen and Nissenbaum's frameworks, we offset these critics.

The outline of this thesis is as follows. The first part is dedicated to a broad literature review on cyber-related topics and on the research, taking into account both national strategy and cyberspace as a whole. After these two sections, we introduce the typology of national cyberstrategy upon which this research draws. Thereafter, we move on to the theoretical framework that structures this work and allows us to develop and present our hypothesis. The fourth part establishes the methodological framework: the cases selected, the operationalization

of our concepts and the two-pronged process envisioned to test our hypothesis. The next part is the center of our work, namely the analysis and the presentation of our findings. Finally, we conclude and sum up the impact of our results on the cybersecurity studies as well as explain how our modus operandi broadens the appeal for the field of cybersecurity studies and begs further research questions.

1 - Literature review

Unlike many other topics belonging to the fields of political science and international relations, cyber-related topics and their origin can be misleading if the researcher does not take the time to explain their meaning in more detail. Therefore, this literature review will be divided into two sections. In the first section, we trace back the roots of this flourishing sub-discipline sometimes called cybersecurity or cyberconflict studies, and put forward the origin of its mysterious prefix – cyber - highlighting by the same token how traditional international relations have tackled the topic so far. In the second section, modern views of the topic of national cyberstrategy are introduced, emphasizing the most contemporaneous theories.

1.1. The Historical Evolution of the Prefix *Cyber*

By looking at the entry "cyber" in the dictionary, we can already see that this prefix is actually a shortened form of a Greek adjective *kubernētēs* meaning "to steer/steersman" (Oxford Online Dictionaries 2018). However, its meaning is still far from our modern conception. Indeed, the first word we are familiar with only comes up in 1834 under the form *cybernétique* and refers to "the means for a government to govern" (Ampère 1834). One century later, the two notorious World Wars occurred. The multiplication of the theaters of war (air, land, sea) coupled with their intensity compelled tacticians to stretch their imagination in order to increase the efficiency on the battlefield and improve coordination between war actors. Eventually, these changes led to major breakthroughs in warfare technology and communication. This interaction between war and technology brought about the American mathematician and philosopher Norbert Wiener to introduce in his 1948 book , *Cybernetics or control and Communication in the Animal and the Machine* (Wiener 1948), the "long-lasting analogy between computing machines and the nervous system; envisioning 'numerical machines' (digital computers) as a founding stone of a self-organizing society" (Baumard 2017:2). Thereafter, another key concept was coined: "cyberspace", which emerged from the field of science fiction (Gibson 1984). Eventually, the term "cyberwar" came up in the mid-nineties, as the information and telecommunications technologies (ICTs) sector was booming (Arquilla and Ronfeldt 1993).

1.2. Cyber: The Birth of a Field

From that moment on, a cybersecurity field started emerging, as captured by the Bourdieusian field theory (Bourdieu 1979), namely as a sub-setting within the social setting where an array of different actors fight for the dominant position. Since the field has been relatively linked to the emergence of ICTs and the development of networks connecting the world, realism and neorealism theories have not been the dominant approach to tackle the subject (Dunn Cavelty 2012:106). Indeed, until 2006, Eriksson and Giacomello reported "political science literature on cyber-security—and closely related sub-issues such as cyber-crime, cyber-terrorism, or cyber-war—remains policy-oriented and does not communicate with more general international relations theory, not even neo-realism" (Dunn Cavelty 2012:106). Still, a noteworthy initiative is the one of American researcher Nazli Choucri, who targeted a more comprehensive approach encompassing cyberspace within globalization as an integrated system, adding a fourth level of analysis to the neo-realist theory of Kenneth Waltz (Waltz 1959). Indeed, the basic structural approach brought about by Waltz was only made up of three levels of analysis which are the individual, the state and the international community (Waltz 1959). Furthermore, she applies the lateral pressure theory to these four levels of analysis (Choucri 2012; Choucri and Clark 2013; Vaishnav, Choucri, and Clark 2013). Originally, this former theory refers to the trend by which states must diffuse their model beyond their borders and consequently influence international interactions. It was conceptualized by Nazli Choucri and Robert C. North in order to explain the relationship between internal growth and international activities (Choucri 2012:17).

1.3.The Securitization of Cybersecurity

In the mid-90s, the constructivist movement took off and gave researchers new tools. From this moment on, the focal point was put on the discursive practices involved in the construction of states' cyberspace, especially the link between national security and cyberspace (Bendrath 2001; Bendrath 2003; Cavelty 2007; Cavelty 2008; Hansen and Nissenbaum 2009; Lawson 2011; Lawson 2012). From 2010 on, the securitization of cyberspace becomes the logical solution for some states to answer the challenges posed by cyberattacks and the potential emergence of a cyberwar (Gorr and Schünemann 2013).

In the same fashion, the 2000s were also a critical juncture because of the emergence of the internet as a global network, spreading quickly to consumers, and bringing about a new paradigm for crime and conflicts. Suddenly, long-standing crimes became intertwined with cyberspace. This fusion gave birth to a plethora of meta-issues rapidly addressed by political scientists, such as cybercrime, cyberespionage (Marchetti and Mulas 2017:39–46), cyber-harassment, cyberextortion (Cavelty 2016), cyberweapons, cyberdeterrence (Lupovici 2011; Jensen 2012). It must be reminded that these new issues did not come out of nowhere. Indeed, the triggering factors were the wave of conventional cyberattacks on Estonia (2007)[2], Georgia (2008)[3], Ukraine (2014)[4] but also new forms of attacks, the advanced persistent threats (APT)[5] such as Stuxnet (Le Monde.fr 2010) and Shamoon (Perlroth 2012) to name the most emblematic.

On the same timeframe, European integration was pursuing its way and the field of cyberspace/security gathered momentum as the Council of Europe decided to get to grips with cyberspace-related issues. This first resulted in the adoption of the Budapest Convention on Cybercrime on 23 November 2001, which tackled the issue of cybercrimes, intended as infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security (Council of Europe 2018). As far as the European Union is concerned, its first milestone was also achieved the same year with the creation of the European Union Agency for Network and Information Security (ENISA) (EUR-LEX 2004). Later on, former High Representative of the European Union for Foreign Affairs and Security Policy Catherine Ashton pushed for further cooperation in the domain of cybersecurity strategy and called for an open, safe and secure cyberspace (Commission 2013).

[2] After the relocation of the Bronze Soldier of Tallinn, which was a symbol from the Soviet-era, unrests led by Russian minorities hit the country and wave of cyberattacks, presumably coming from Russia, targeted and paralyzed Estonian administrations (Dragosei 2007).

[3] Also known as the Russo-Georgian War, this notorious conflict lasted five days and ended with the loss of Abkhazia and South Ossetia for Georgia. During this period, cyberwarfare has been used extensively. (Swaine 2008; Vendil Pallin and Westerlund 2009:400)

[4] Back in November 2013, in the midst of negotiations with the European Union on one side and with Russia on the other side, Ukraine's authorities decide to leave the discussion on a agreement with Brussels in favor of Moscow. The population feels betrayed and starts demonstrating. Again, information warfare played a role (Lee 2014; Maurer and Geers 2015).

[5] An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).(Joint Task Force Transformation Initiative 2013)

1.4.The Shift from National Strategy to National Cyberstrategy

This formerly mentioned and peculiar event in Estonia was really the trigger pushing the field of cyberstrategy to emerge, but it would not have known such an expansion without the work carried out by pioneers (Ventre 2011; Dossé, Kempf, and Malis 2013; Ventre 2015; Ventre 2016). While the sector was quickly gaining the status of strategic interest, it also became instrumental to the eyes of some people interested in the legislation cyberwar/informational warfare and Cyberoperations (Czosseck and Geers 2009; Schmitt 2013; Pipyros et al. 2016; Schmitt 2017). Indeed, due to the peculiar nature of the cyberspace network, relying both on logical and physical infrastructures, the issue of attribution remains problematic for research (Clark and Landau 2010; Roscini 2015) and is also a reminder that the state, seen as a delimited and physical territory, is the space where everything originates: infrastructure is after all physical.

Nowadays, cyber-related studies are growing more and more especially, in broader domains as they impact not only the private but also the public sphere. Cyberespionage, protection of data, IoTs (Internet of things), and, generally speaking, all issues linked to the Web, are now considerations at the center of states' preoccupations.

This naturally led to the expansion of comparative studies, first highlighting the causes and mechanisms of previous cyberattacks (Gamero-Garrido 2014) and then putting forward solutions envisioned by organizations (EU & NATO (Joubert and Samaan 2014)]) or states (Silva 2013; Samantha Adams et al. 2015). In addition, we also find single case studies on the more relevant actors of the cybersphere such as the US (Lynn 2010; Samaan 2010), China (Hachigian 2001; Ball 2011; Inkster 2010), Europe (Davì 2010; Lukin 2012; Fahey 2014; Backman 2016), Estonia (Cardash, Cilluffo, and Ottis 2013; Crandall 2014; Crandall and Allan 2015) and Russia (Thomas 2009; Gvosdev 2012; Thomas 2014), and to some extent Israel (Al-Rizzo 2008) and North Korea (Haggard and Lindsay 2015). Surprisingly, despite the pervasiveness of cybersecurity, research on single European countries is not as widespread, yet Estonia, for example, provides us with a wealth of literature.

Could the underlying reason for this scarcity be its *domaine reservé* nature standing for a new means to reassert one's state legitimacy, bringing the state back to the center of international relations (Chapaux et al. 2015)? As a matter of fact, these questions are not meant to be answered as such, but rather, to show the extent of the range of questions brought about by the

field of cybersecurity. Nonetheless, what is certain is that cyberspace covers so many issues that it is rare to find studies covering every aspect encompassed by this reality. One can also wonder if this non-interest does not reflect the willingness of actors to better adopt a regionalist perspective as envisioned by some authors (Telò 2013). Or perhaps, the Web of actors is so complex that the solution requires a comprehensive initiative, involving every actor – states, international organizations (both intergovernmental and non-governmental), civil society and private companies, but also individuals as they can, at their scale, be the origin of huge damages on the networks. The most compelling evidence of this need of cohesion between actors is the recent call on governments to cooperate by Microsoft, that called for a Digital Geneva Convention (Microsoft 2017). Private interests aside, such call shows to what extent we are now all entangled.

1.5. Looking for a Common Cybercapabilities Assessment Framework

In any case, if researchers did not focus their attention on the subject, numerous actors of the private sector and some international organizations have already developed assessment tools to analyze in depth the cyberinfrastructure put in place by states with the aim of implementing a global regional framework. A few examples are the ENISA framework (Liveri and Sarri 2014) or its National Cyber Security Strategies Implementation Guide, or the Alliance think tank framework of cybersecurity landscape[6] (Alliance 2015). The most promising work is about to be released by the International Telecommunications Union (ITU) that has undertaken the elaboration of an ITU National Cyber Security Toolkit[7], merging a series of current assessment tools to provide the most comprehensive National Cyber Security toolbox ever done. With a release expected during the year, it will entail the following tools: ITU – National Cybersecurity Strategy Guide (2011); Oxford Martin School – Cyber Capability Maturity Model (2014); CTO – Commonwealth Approach For Developing National Cyber Security Strategies (2014); Microsoft – Developing a National Strategy for Cybersecurity (2013); CCDCOE - National Cyber Security Framework Manual (2012); OECD - Cybersecurity Policy Making at a Turning Point (2012) and OAS – Cyber Security Program (2004).

Throughout this literature review, we notice how the interest in cybersecurity studies has grown over the past three decades. This growing interest highlights how instrumental it has become

[6] Cf. Appendix 1.
[7] Cf. Appendix 2.

for states to secure their cyberspace. Discourse is a way of achieving the safety of this field. However, most of the studies carried out so far consider too many countries and only reflect material differences rather than ideological ones. Furthermore, as the last section on common cybercapabilities assessment framework shows, the spectrum that cyberspace covers is so considerable that it takes a whole range of tools to provide for a comprehensive framework, which has not yet been released.

2 - Theoretical Framework

As stated in the introduction, the theory used to elaborate our national cyberstrategy framework and thus answer our research question borrows from both realism and constructivism for the first part, and on speech analysis for the second part. The first section is dedicated to a short description of the realist paradigm, as some of its principles will be used for the framework construction in order to confirm our hypothesis. The second section introduces the concept of discourse and text analysis. The third section deals with securitization and how cybersecurity can be analyzed through this lens.

2.1.Realism

The roots of realism trace back hundreds of years, with authors such as Thucydides, Hobbes or Machiavelli forming the basis of this theory. As Telò explains, even though realism was born in Europe, it became quite famous over the Atlantic after the Second Word War (Telò 2009:35).

Realists hold several principles: (1) the anarchical structure: from within, states are stable through a "social contract", by which people give up part of their liberty in exchange for protection. Hobbes tried to apply the so-called domestic analogy beyond the state, namely transposing "the domestic oppositions between state of nature and state of reason, disorder and order, anarchy and stable peace" (Telò 2009:15) at the internal level. Yet, the lack of Leviathan, or authority above states, makes the peace and the stability at an international level impossible; (2) the state-centric paradigm: realists consider that states are the most important actors on the international system and are driven by survival or self-defense. While other actors can exist, they are seen as non-autonomous and deriving from states; (3) the balance of power context: the lack of supranational entity implies a perpetual state of anarchy, and at the international level there is a natural balance between stronger and weaker powers; (4) the prevalence of power and foreign policy: one the one hand, for some states maximizing power is central, and as stated above, the system is anarchical and only pure power can allow states to survive. On the other hand, some states only seek power to pursue their national interest. Power is here intended as hard power based on population, territory and capabilities; (5) the prevalence of "high politics" over "low politics": some issues are viewed as priorities for states but the highest one remains security. Indeed, states feel insecure all the time because of the so-called "security dilemma". For example, if a neighboring country adopts a rearmament policy, your state has to

follow because there is a pending uncertainty concerning its intentions; (6) the rational choice theory rationale: in order to achieve their national interest, states think about their actions in terms of a costs benefits calculus. This calculus is the only factor that explains its foreign policy, which incidentally dominates the domestic one. (Telò 2009:35–36; Choucri 2012:17).

In addition to these principles, we would like to underline Morgenthau's vision of national interest. In his masterpiece Politics Amongst Nations, he highlights that "since the world is characterized by conflicts of interest, the best conceivable scenario is achieving a balance of interests" (Telò 2009:32). Furthermore, he considers that the understanding of international politics goes through the reading of "main signposts" which are/he depicts as "interests interpreted in terms of power" (ibid.).

Thus, far from being an extensive explanation of the realist theory and its substrates, this overview provides us key concepts necessary to establish our own tools and integrate them into a discourse analysis framework. In that matter, the concepts of security and national interest provide us with a starting point for the elaboration of a new framework.

The Concept of National Interest

The topic of national interest has been a topic of much discussion in the realm of political science. Traditionally, we have been associating national interests with geopolitical and economic interests (Telò 2009:26). However, that does not mean that "interests are not always rooted in material factors" (Telò 2009: vii). Telò adds that "they can be oriented towards the short-term or the long-term […] highly conflictual ("zero-sum") or assume the benefits of cooperation; […] be altered by institutional context; and […] be changed by ideas about values or about causality*"* (ibid.).

If we follow the classic realist theory, Morgenthau highlighted that a nation "thinks and acts in terms of interests, defined as power" (Morgenthau 1993:15). Kempf's explanation of interests goes in the same direction. He argues that "in a multipolar system, actors keeps on taking decisions fitting their own interests before the ones of system" (Kempf 2012:191). He further adds that "the system is the result of this way of thinking and that actors define themselves in terms of interests of powers" (ibid.). Besides, Kempf affirms "interests are no more rooted in material or territorial factors but in assets and information" (ibid.). [8]

[8] free translation for the ideas of Kempf.

Interests are therefore at the center of the definition of cyberstrategy. Indeed, "[T]he human element, including national interests, is playing an ever-increasing role in cyber security and certainly the current set of international standards and best practices is not comprehensive enough to secure cyberspace" (Von Solms and Van Niekerk 2013:101). In our case, the human component would be the decision maker that implement policies to securitize cyberspace. To stay within the crossover theoretical framework we adopted, we thus consider interests as the main signposts of securitization and are "generally defined in terms of threats to the sovereignty or survival of the state" (Buzan, Wæver, and De Wilde 1998:56).

Thus, the national interest refers to an all-encompassing idea. When the concept is uttered, the state calls upon this joker that enables to resort to every means possible to protect what is intended as belonging to this national interest and consequently ensuring the nation to thrive. (see concept of cyberspace).

The Concepts of Security and Cybersecurity

From the beginning of this work, we have been mentioning the terms security and cybersecurity. Yet, their meaning is subject to change according to which school of thought or conceptualizations we embrace.

We begin with security. Valverde provides us with a comprehensive definition, namely "[t]he abstract noun 'security' is an umbrella term that both enables and conceals a very diverse array of governing practices, budgetary practices, political and legal practices, and social and cultural values and habits" (Valverde 2001: 90). Security is therefore pluridisciplinary and can either be seen as an objective state, a subjective state, a pursuit or a symbol (Zedner 2009:9–25). To Zedner, security "conveys many meanings and has many referent objects, ranging from the individual to the state to the biosphere"(Zedner 2009:10). In other words, security, as an abstract concept, is informed by an array of actors and refers to an object influenced by a series of factors.

As far as Cybersecurity is concerned, the same observation applies. The securitization of cyberspace is thus done through cybersecurity, which encompasses several referent objects. A relevant definition for us stems from the work of Von Solms and Van Niekerk who worked on the differentiation of information security and cybersecurity, they argued that:

> [*C*]*yber security can be defined as the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace* (Von Solms and Van Niekerk 2013:101).

Despite the fact that this definition fits well to our work, we have to add an additional dimension to it, which is securitization. As Dunn Cavelty, we will also view cybersecurity as "a combination of linguistic and non-linguistic discursive practices from many different "communities of actors" (Dunn Cavelty 2012:108).

2.2. Cyberspace and Cyberdoctrines

The Concept of Cyberspace

There are several ways to consider Cyberspace: from a military point of view (NATO), from a legal point of view (Tallinn Manual) or from an academic perspective (Dunn Cavelty 2012; Kempf 2012). The NATO terminology website presents the view of each of its member states on the matter. However, to better portray this concept and to not favour one national view over another, we will therefore try to combine the three perspectives.

First of all, Dunn Cavelty argues that there are two ways of conceiving cyberspace: the first way excludes the physical infrastructures, while the second integrates them (Dunn Cavelty 2012:107). We believe it is more adequate to choose the second path and integrate them, as they form the basis of the system.

The Tallinn manual, which is an attempt to codify cyberspace on the international level, defines it as "[t]he environment formed by physical and non-physical components, characterized by the use of computers and electromagnetic spectrum, to store, modify and exchange data using computer networks" (Schmitt 2013). This view depicts three of the layers on which cyberspace relies well: the material layer ("physical components" or hardware), the logical layer ("non-physical component": the "software") and the information layers ("non-physical component": information transiting through the networks) (Kempf 2012:10–15) (see Figure 5 below).

A similar definition was elaborated from the merging of the Tallinn Manual's definition of cyberspace and the one indicated in the national documents and policies. It views cyberspace as

> *a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources* (Mayer et al. 2014:1).

What changes with this definition is the range; it is considered as a "global domain" which consequently affects us all, and here the destructive power enabled by this domain is put forward. But, this definition does not provide us with the full picture of cyberspace. Therefore, the same authors included a list of elements making up cyberspace, namely:

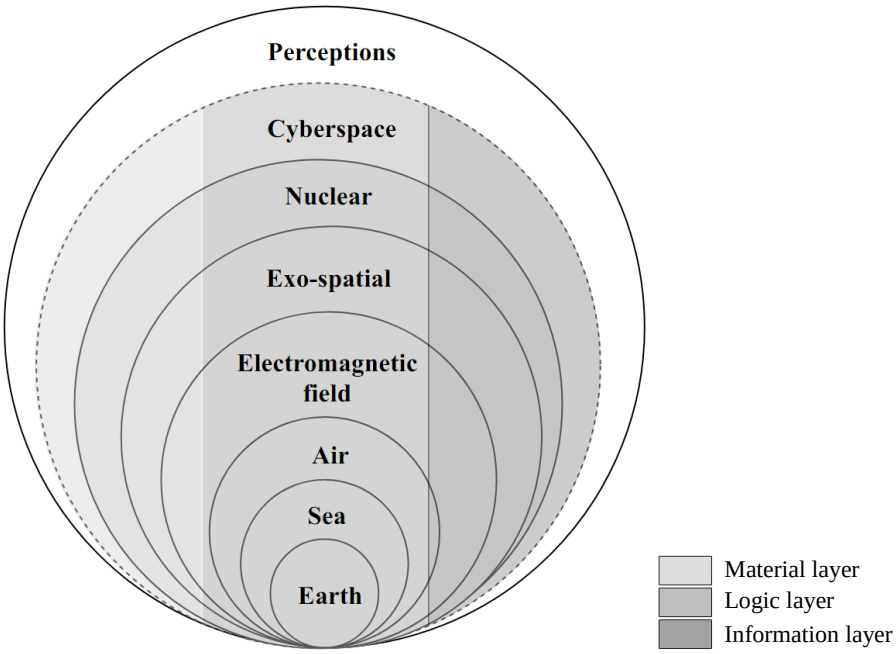
> *a) physical infrastructures and telecommunications devices that allow for the connection of technological and communication system networks, understood in the broadest sense ([Supervisory Control and Data Acquisition (SCADA)] devices*[9]*, smartphones/tablets, computers, servers, etc.*[10]*); b) computer systems (see point a) and the related (sometimes embedded) software that guarantee the domain's basic operational functioning and connectivity; c) networks between computer systems; d) networks of networks that connect computer systems (the distinction between networks and networks of networks is mainly organizational); e) the access nodes of users and intermediaries routing nodes; f) constituent data (or resident data)* (Mayer et al. 2014:2).

This list is rather complete, yet one element characterizing cyberspace is missing. We find this element by following the definition of Kempf, namely "[c]yberspace is the space made of all kind information computer systems connected by a network and enabling the social and technical communication of information by individual or group of people" (*translation ours*) (Kempf 2012:16). Again, cyberspace is endowed with a "space" but what is relevant here is to mention the fact that the agent is specified. Indeed, cyberspace can be used by a single user or a group. Besides, the space to which Kempf refers, should be seen as a strategic sphere. Here is the figure with the strategic spheres and the layers mentioned above.

[9] "Computer systems and instrumentation that provide for monitoring and controlling industrial, infrastructure, and facility-based processes, such as the operation of power plants, water treatment facilities, electrical distribution systems, oil and gas pipelines, airports, and factories" (Schmitt 2013:262).

[10] We come back to the here above mentioned physical infrastructures, that is "submarines cables, data centers and other physical infrastructures" (Kempf 2012:11–12).

Figure 1 Strategic Spheres and the three layers



Note: elaborated from the Figure in Kempf (2012:61)

Eventually, it would be suitable to just add these two elements: the agent element and the strategic element to the last provided definition. Thus, drawing on the whole set of views (Kempf 2012; Schmitt 2013; Mayer et al. 2014), we suggest our own comprehensive definition of cyberspace, that is : the global and dynamic changing space formed by physical, both material and living life, and non-physical components covering all strategic spheres, characterized by the use of computers and the electromagnetic spectrum, to store, exchange, share, extract, use, eliminate, disrupt or defend information and physical resources.

We use the "space" and mention the attack and defend possibilities (disrupt/defend) because it is easier to adopt such a stance in the view of securitization. Indeed, a space linked to tangible infrastructures is easier to securitize and to explain to the audience. In addition, we included ourselves, humans, inside cyberspace because, as we explained earlier (p. 16), there is a double-edged agency in cyberspace, which makes us both agents and potential victims inside the cyberspace.

The Concept of Cyberthreats

Generally speaking, the term denotes "a rather vague notion signifying the malicious use of information and communication technologies either as a target or as a weapon"(Cavelty 2008:21–22). However, this conception is rather unclear and does not provide us with a

comprehensive explanation of the phenomenon. The problem arising from defining [cyber]threats is that, if we remain within the framework of securitization, what is framed as being a threat for a country that may not be perceived as such by another one. This operation called "threat framing" consists of a determined agent, or for us, securitizing actors, in "develop[ing] specific interpretive schemas about what should be considered a threat or risk, how to respond to this threat, and who is responsible for it."(Cavelty 2008:21).

Therefore, it is useful to refer to a classification of cyberthreats to better frame the concept afterwards. In that matter, Nissenbaum identified three categories of threats looming large in the field of cybersecurity (Nissenbaum 2005:64). The first category is made of "threats posed by the use of networked computers as a medium or staging ground for antisocial disruptive, or dangerous organizations and communications", which refers to the broad coordination of various crimes using ICTs technologies. The second category is the "attack on critical societal infrastructures, including utilities, banking, government administration, education, healthcare, manufacturing and communications media". Here, we find the critical infrastructures already captured in the idea of national interest and cyberspace. The last category entails "threats to the networked information system itself ranging from disablement of various kinds and degrees to – in the worst case – complete debility", which are all cyberattacks that do not specifically aim at critical infrastructures but could reach them while attacking the whole system.

From Nissenbaum's typology, we can abstract our own definition which is: cyberthreats are threats looming over the cybersecurity network, relying partially or totally on cyberspace and which targets, both living and non-living entities, and can vary from the single individual to the whole network.

The concepts of cyberstrategy and cyberdoctrine

In part 2.4 dedicated to the four typologies of Baumard, we introduced the notion of cyberdoctrine. So far, we have been using cyberdoctrine and cyberstrategy equally because we think they convey the same meaning. For the sake of clarity, we concur with Baumard's stance and assume that cyberstrategy and cyberdoctrine can be used interchangeably. As far as Baumard's cyberdoctrines types are concerned, namely "Social order" (I), "Technocrat" (II), "Societal Resilience" (III) and "Power- sovereign" (IV), we do not detail them as they were fully presented in part 2.4. Moreover, Kempf's opinion goes into the same direction when he

argues that "the doctrine is a discourse, often national, on the implementation on [a] strategy" (Kempf 2012:161).

Still, we need an operational definition of cyberstrategy. Betz defines cyberstrategy as "the reciprocal interaction of human choice in conflict" (Betz 2017). Its choice reflects the old classic paradigm, that is the "interaction between states", and consequently individuals in times of conflict. Despite embracing the securitization theory, we do think some realist concepts prevail. Here, we refer to the security dilemma that becomes the cybersecurity dilemma. A state deploying its [cyber]strategy will think in terms of security dilemma for its strategic spheres[11] in order to build enough [cyber]deterrence [12] capability to feel safe (Kempf 2012:161). Nonetheless, this conceptualization does not give us the full picture of cyberstrategy.

The problem is that, as it is the case for other concepts, such as cyberthreats, cyberstrategy falls into the category of concepts shaped by the discourse of domestic officials and legitimate actors.

Yet, Kempf suggests a broad definition: "[C]yberstrategy is the part of strategy dedicated to cyberspace, conceived as a space where conflicts prevail amongst a series of actors including states, groups and individuals" (*translation ours)* (Kempf 2012:7). Nonetheless, Kempf also talks about a strategic calculus that is involved in the cyberstrategy conception and which is dependent on three features: space, time and actors (Kempf 2012:103). Furthermore, in his conclusion on cyberstrategy, he includes the underlying element of these three components that is the theory of the strategic spheres, which highlights the double nature of cyberspace: on the one hand it is a space of its own, on the other hand, it encompasses and is intertwined with all other spheres on the three different layers (see Figure 5) (Kempf 2012:208–211).
Thus, taking these features into account, we decided to keep the definition provided by Kempf but we changed the space to strategic sphere to remain within our framework, which gives us : "[C]yberstrategy is the part of strategy dedicated to cyberspace, conceived as a strategic sphere where conflicts prevail amongst a series of actors including states, groups and individuals" (Kempf 2012:7). The advantage of such definition is that it is as neutral as possible, and it can therefore encompass the most issues possible, as it neither mentions the means to achieve the strategy nor the actors putting it in place.

[11] Please refer to Figure 5.
[12] For more information on cyberdeterrence, refer to Kempf (2012:164-65).

As we have seen, the difficulty of naming and conceptualizing ideas surrounding cyberspace relies on the very fact that as a sphere it can encompass almost everything. The direct consequence of this is either a lack of consensus of the definition or no definition at all. Nevertheless, following the logic of securitization, we rather keep the definition as open and neutral as possible to better label decisions implied by discursive practices later.

Typology of cyberdoctrines

Although no proper comprehensive framework exists to assess all the sectors encompassed by cyberspace, there is a framework aiming at organizing countries in different categories reflecting their military priorities. This framework was developed by Phillipe Baumard and is called typology of national cyber-doctrines (Baumard 2017:70). Developed as a response to the lack of guidelines and framework for the study of National Cyber Security Strategies (NCSS), it was based on 35 public national cyber-doctrines and national cyber security strategies (Baumard 2017:3).

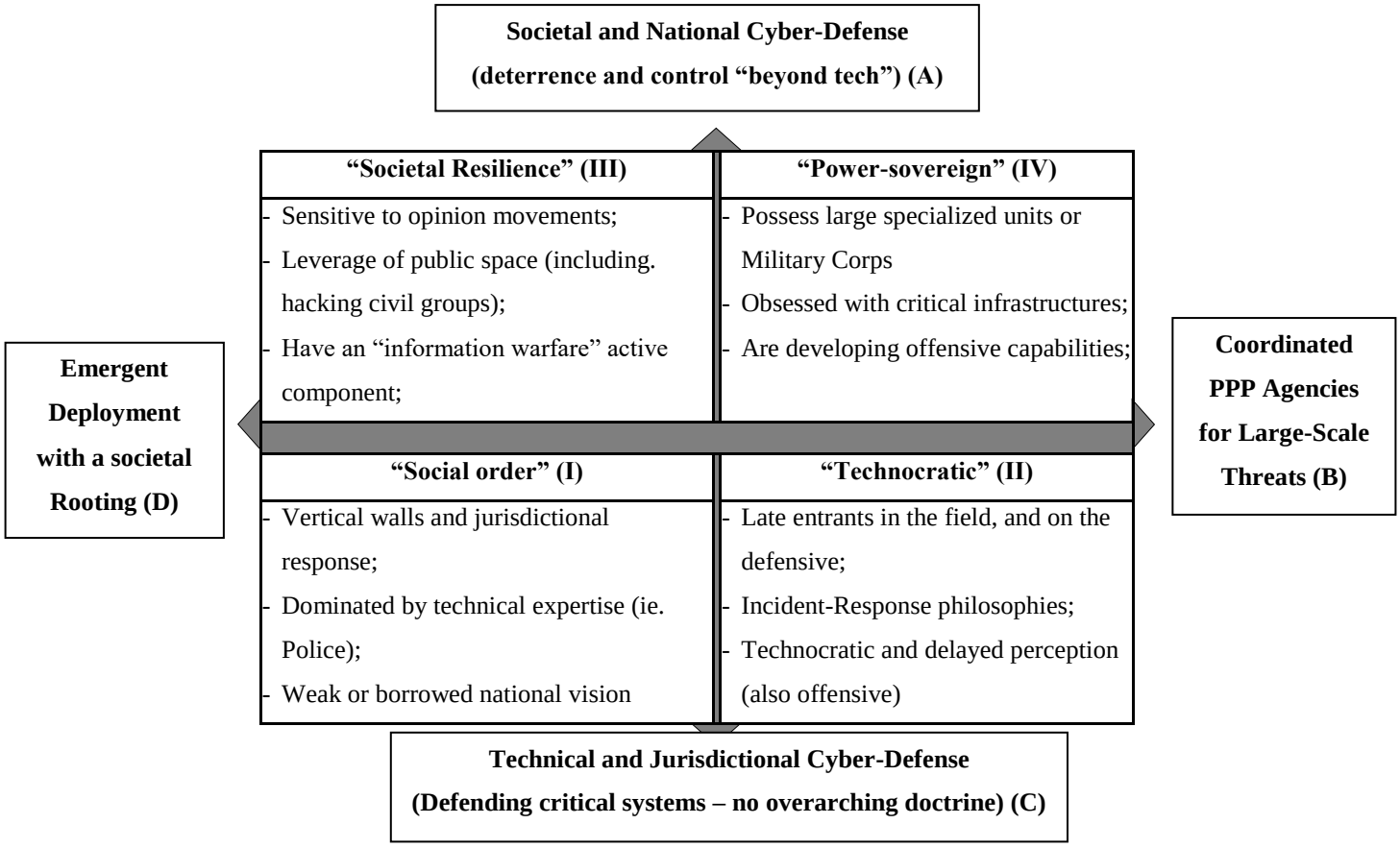
Baumard established four different categories called *class*. The first class "Social order" (I) relies on a control at the source exerted by technical expertise (like the police) more than on a national vision, which if there is any, is often borrowed from another state. The second class is the "Technocrat" (II), which unlike the previous class aims at exerting a control by a normalization of the outputs. States that adopt this stance are mostly latecomers on the field and suffer from a delayed perception of technology change, still mainly inspired by an incident-response philosophy. The third class "Societal Resilience" (III) tends to focus their offensive capabilities on information warfare, monitoring and controlling the public sphere where opinion movements can appear (civil hacktivist groups for instance). The fourth class "Power-sovereign" (IV) gather states obsessed with critical infrastructures. In order to protect them, they usually invest in large specialized units that can withstand state-sponsored cyber-attacks thanks to sustainable deterrence policies. However, when facing pattern changes or emerging hacking movements, this class can seem unprepared as its whole structure is rather rigid and does not foster reactivity to "distributed cognitive warfare" (Baumard 2017:69)**.**

On top of that, as you can see from the adapted version of Baumard's typology (on the next page – Figure 4), different classes can also fall into the same category. Two different oppositions, delimiting four axes, can be inferred from the typology table:

(1) conventional physical infrastructure defense only (C) versus comprehensive defense encompassing both physical and psychological control (A)
(2) Coordinated Private Public Partnerships (PPP) for large threats (B) versus implication of the civil society for targeted threats (D)

Classes III and IV view the digitalization of society as fostering and threatening at the same time cyber-development and cyber-defense. Thus, they put the emphasis on the deterrence and control "beyond tech" which refers to the protection of infrastructures through the protection of information warfare. They are said to be following a type (A) stance; while other states (classes I&II) tend to adopt a defense, which is only based on physical infrastructures such as submarine cables, data centers and other physical infrastructures (Kempf 2012:11–12), and follow an approach of type (C), deprived from any doctrine or if they have one, it is often borrowed from another state. In the same fashion, states pursuing a close cooperation with the private sector (II&IV) engage in type (B) stance, while states relying more on public society (I&III) follow a type (D) approach. (Baumard 2017:69).

Figure 2 *Baumard's typology of national cyber doctrines*



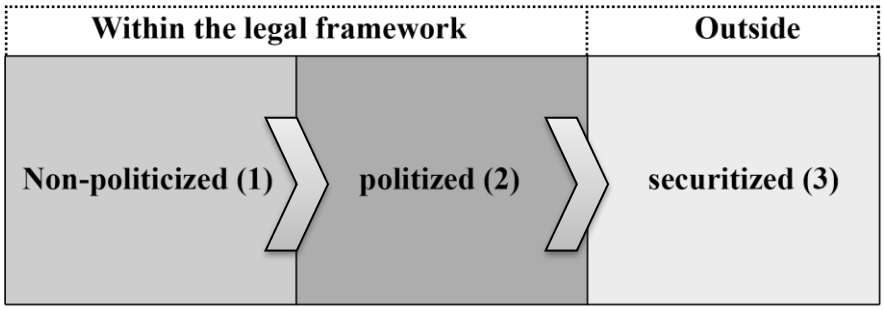
Note: Table elaborated from the data contained in the 2 x 2 matrix (Fig. 4.2. in (Baumard 2017:70)).

2.3.Securitization theory

The term securitization finds its roots in the broader concept of security. But what does security refer to according to theorists of securitization? There are two views on the topic: on the one hand, the traditional old military and state-centered realist view that tends to see security as a given, generated by military issues and the use of force (as depicted in the previous subpart); on the other hand, the broadened and modernist view that envisions security as potentially applied to an "ever wider range of issues" (Buzan, Wæver, and De Wilde 1998:1). Securitization theory embraces this latter view and stems from the so-called Copenhagen School (CS), which is at the crossroads of three theoretical approaches: Security Studies, the speech act theory and the classical Schmittian understanding of the state and security policies (Hansen and Nissenbaum 2009:1158).

The CS actually provides a more complete definition of security, namely: "the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics" (Buzan, Wæver, and De Wilde 1998:23). To better capture the idea of the process in which a political issue moves from non-politicized to securitized, we elaborated a table showing what the fathers of securitization call "extreme politicization" (ibid.).

Figure 3 *From legal to securitized: the spectrum of issues*



Note: table made using the description provided in Buzan, Wæver, and De Wilde (1998:23)

On the left part, the public issue is either ignored from the political agenda (1) or is currently part of a public policy (2). In both of these steps/status, (political) actors are abiding by the rules defined by the legal framework. On the right, the public issue moved towards the status of existential threat (3), which may require measures or legitimatize actions happening outside the

normal bounds of political procedures (Buzan, Wæver, and De Wilde 1998:24). The success of the securitization relies on the "intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects" (Buzan, Wæver, and De Wilde 1998:25). Indeed, "[a] successful securitization thus has three components (or steps); existential threats, emergency action, and effects on Interunit relations by breaking free of rules" (Buzan, Wæver, and De Wilde 1998:26).

Buzan, Wæver and De Wilde prescribe to study the securitization through "discourse and political constellations" (Buzan, Wæver, and De Wilde 1998:25). But why through these means? Following the Austinian tradition, the process of securitization corresponds to what is called a speech act in the language theory (Buzan, Wæver, and De Wilde 1998:26). In other words, the simple fact of uttering the word amounts to the performance of the act itself, just like making a promise, it therefore possesses a performative effect (Austin 1975:88). As far as the security discourse is concerned, for the agent, the process goes as follows: an issue is labeled as (a) security (issue) and then, a right to resort to extraordinary means appears legitimate (Buzan, Wæver, and De Wilde 1998:26). This whole thought process fits in the textual analysis, understood in the security field as assessing through discourse analysis if a securitization is successful or not (ibid.).

This speech approach theory involves three key units : the referent objects (1), that is the issue/sector threatened having a "legitimate claim to survival"; the securitizing actors (2), namely the agent stating which referent object should be securitized; and the functional actors (3), conceived as "actors who affect the dynamics of a sector" (Buzan, Wæver, and De Wilde 1998:36).

In addition to these three components, an important element of the theory is the audience, which is the population being convinced of the necessity to securitize the referent object (Buzan, Wæver, and De Wilde 1998:41). Indeed, the audience per se does not exist, it is the result of dichotomy constituted within the security discourse between "the 'we' on whose behalf they [securitizing actors] claim to speak, and the 'you' who are simultaneously addressed by the linking of fears and threats to 'feelings, needs and interests' ". Eventually, the success of the speech act in the securitization theory also depends on facilitating conditions:

> *(1) the demand internal to the speech act of following the grammar of security, (2) the social conditions regarding the position of authority for the securitizing actor—that is, the relationship between speaker and audience and thereby the likelihood of the audience accepting the claims made in a securitizing attempt", and (3) features of the*

> *alleged threats that either facilitate or impede securitization* [13] (Buzan, Wæver, and De Wilde 1998:33).

Nonetheless, there is not a sole theory of securitization but a set of theories that developed over the time (Balzacq 2015:103). For the sake of clarity, Balzacq identified "the constellation of concepts associated with securitization" and elaborated an "ideal type" that we will use as the reference for our framework analysis (Balzacq 2015:105)[14]. In the operationalization section, we will further explain how we use the three components: "existential threats, emergency action, and effects" through the analysis of "discourse and political constellations" (ibid. pp.25-26).

2.4. Securitization applied to Cyberspace

Securitization can be applied to numerous "sectors" - military, environmental, economic, societal and political (Buzan, Wæver, and De Wilde 1998:21–23). These sectors represent "sub-forms" or "grammars of securitization" which "tie referent objects, threats, and securitizing actors together" (Hansen and Nissenbaum 2009:1163). However, in their seminal security framework, the Copenhagen School authors did not include the field of cybersecurity as a significant sector to be securitized (Hansen and Nissenbaum 2009:25). Indeed, the fathers of the securitization theory ruled it out as they consider it had " no cascading effects on other security issues", except on the computer field (Buzan, Wæver, and De Wilde 1998:25). This statement proved to be true at the end of the nineties, but, with the development of ICT technologies and the growing cyberattacks, its relevance was slowly put into question. The cyberattacks on Estonia led Hansen and Nissenbaum to undertake an update of the securitization framework in order to "identify and locate cybersecurity as a particular sector on the broader terrain of Security Studies" (Hansen and Nissenbaum 2009:1157).

Thus, they designed a framework to assess the extent to which Estonia had securitized its cybersecurity sector. This process entailed addressing three questions:

> *What threats and referent objects characterize cyber security; what distinguishes it from other security sectors; how may concrete instances of cyber securitizations can be analyzed; and what may critical security scholars learn from taking cyber discourse seriously?* (Hansen and Nissenbaum 2009:1157).

[13] These features can be materials elements already inspiring a threat: tanks, weapons or hostile sentiments for instance.
[14] Cf. appendix 6.

To answer these questions and analyze the securitization of the cybersecurity, Hansen and Nissenbaum considered three modalities that apply specifically to the cyber-sector: (1) hypersecuritization, (2) everyday security practices and (3) technification.

Hypersecuritization (1) refers to what Buzan called "a tendency both to exaggerate threats and to resort to excessive countermeasures" (Buzan 2004:172). However, Hansen and Nissenbaum decided to remove the term "exaggerate" from their definition and only view it as "an expansion of securitization beyond a 'normal' level of threats and dangers", hence resorting to extraordinary measures (Hansen and Nissenbaum 2009:1164). Besides, they decided to focus on specific features of the cybersecurity discourse. For them, the power of hypersecuritization does not only stem from the act of securitization but also from the underlying potential of the threat to bring down with it an array of "other referent objects and sectors", because it mobilizes the "specter of the future" (ibid.). Thus, we can sum up these characteristics as "instantaneity and inter-locking effects (Denning 1999:xiii). Indeed, just as the environmental discourse, cybersecurity discourse relies on irreversibility, which implies that if the system is destroyed, there is no turning back (Hansen and Nissenbaum 2009:1164). In that matter, two features are specific to cyberspace. The first feature is the swiftness of threats, as cyberthreats draw their intensity from the cascading effects they produce instantaneously. The second feature is the difficulty to picture the potential damages that cyberthreats could create as there is a lack of prior major disasters. 15

Everyday security practices (2) imply a twofold process that involves the influence of securitizing actors, including private organizations and businesses, over "normal individuals' lives: on the one hand, the protection of network's security aims at securing the "individual's partnership and compliance" and on the other hand, "linking elements of the disaster scenario to experiences familiar from everyday life" contributes to making "hypersecuritization scenarios more plausible" (Hansen and Nissenbaum 2009:1165). In other words, securitization discourses are integrated more easily if their impact and content reflect the audience's life.

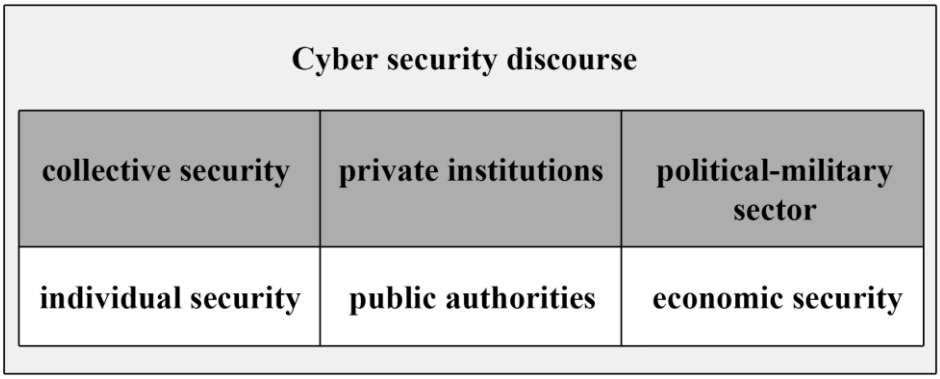
It is true that elements of daily life can be found in other sectors, but cybersecurity presents two features that make it even more relevant. The first one is the pervasiveness. Indeed, what is peculiar with cyberspace is the pervasiveness of any activity in the field (see Figure 2): even people unequipped with computers or technologies linked to the network are bound to feel the

[15] This echoes to our previous remark that up to now no cyberwar, intended as causing human casualties, has ever happened.

"consequences of digitization" because our world relies on ICTs and networks (Hansen and Nissenbaum 2009:1165).

The second feature is what we call double-edge agency. As Hansen and Nissenbaum explain, individuals act on the network as both active partner in the fight for a better and more secure network, but also as the potential liability given that a single click can compromise the whole infrastructure (Hansen and Nissenbaum 2009:1166). The combination of the two leads to the so-called hypercascading scenarios mentioned earlier. Moreover, the need for security in everyday life provides governments "with the discursive and political legitimacy to adopt radical measures, the question becomes at which point and how these strategies, and their harmonious constitution of state-society relations, can become contested."(Hansen and Nissenbaum 2009:1166)

Figure 4 *Interlocking feature of the cyberdiscourse*



Note: Elaborated following the RAND remarks (Hansen and Nissenbaum 2009:1161).

The table above reflects the pervasiveness of the cybersecurity discourse well. As Ronald J. Deibert (2002) and Diana Saco (1999) have argued, "cyber security is a terrain on which multiple discourses and (in)securities compete" (Hansen and Nissenbaum 2009:1162).

Just like securitizations, technifications (3) work as speech acts and produce a performative effect. However, using this framework of securitization presupposes that technology serves a "politically and normatively neutral agenda" (Hansen and Nissenbaum 2009:1167). Indeed, the discourse constructed depends on technical and expert knowledge, and is meant to work outside the political realm. In that matter, a privileged role is dedicated/allocated to experts within the cyber security discourse: if cyber security is so crucial, it should not be left to amateurs (Hansen and Nissenbaum 2009:1167), for the mastery of cybersecurity is not within the reach of anyone. Cybersecurity experts are thus legitimized as the securitizing actors of the field because they

are endowed with skills, and because using technifications enables "distinguishing themselves from the 'politicking' of politicians and other 'political' actors"(Hansen and Nissenbaum 2009:1167). Moreover, the securitization task behooves experts because the future of the field is hypothetical and therefore leaves much space to the technical and expertise. On top of that, the sector is evolving at a strong pace, with attacks and technology taking new forms, reinforcing the legitimacy given to the technical discourse and the epistemic community (Hansen and Nissenbaum 2009:1166).

Interestingly, computer scientists tend to disagree on the likelihood of cyberattacks. These divergent opinions come from the nature of the cybersecurity field and give birth to a paradoxical situation. While some people envision a world fully developed where technology surrounds us, and underestimating the underlying nascent threats, others expect the worst-case scenario. This dual vision further facilitates the implementation of such technification discourse. In addition to the general cloudiness surrounding cyberspace, the military factor adds another layer of opacity to the field (Hansen and Nissenbaum 2009:1167).

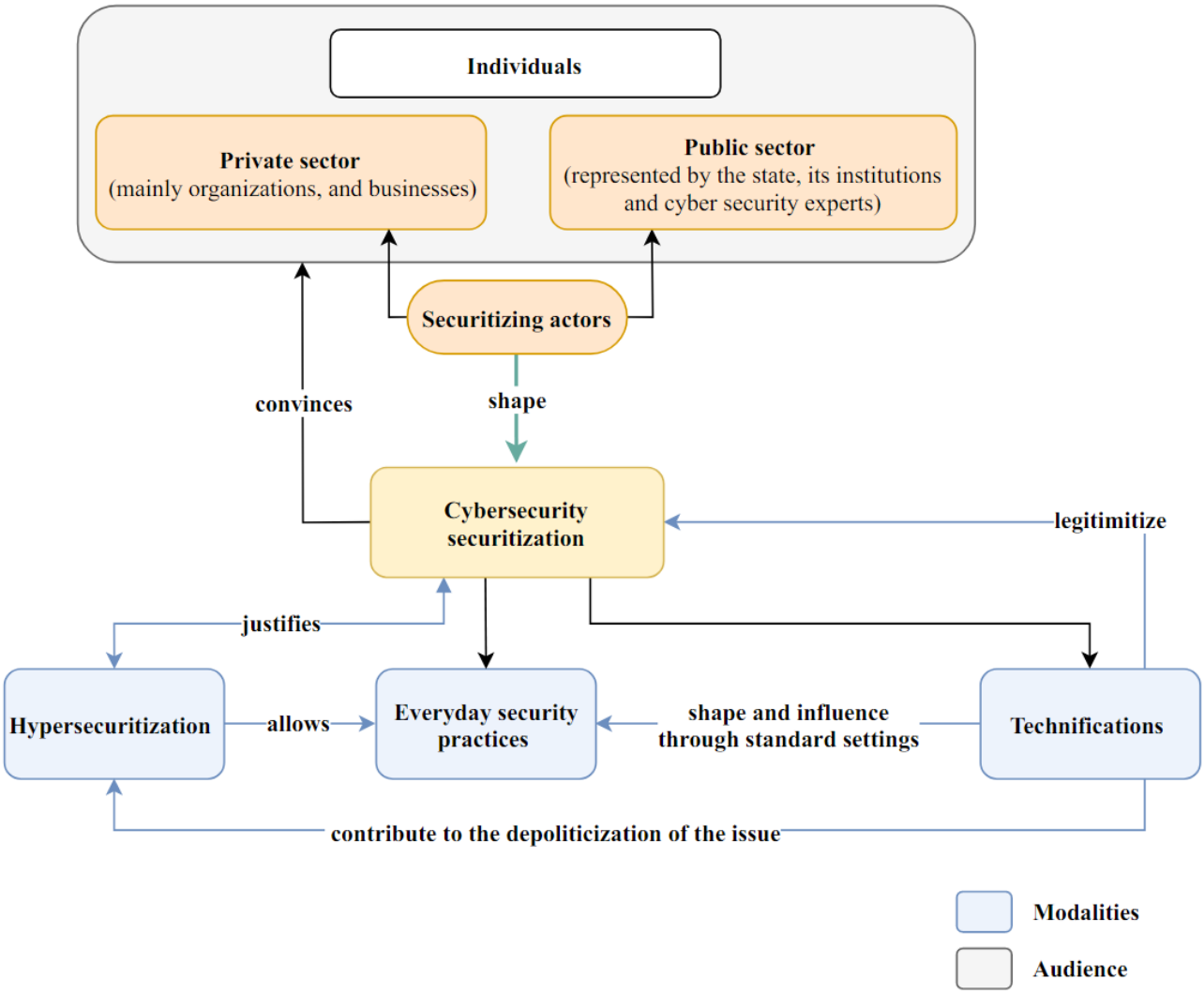
Eventually, the grip of experts on a field is "not exclusive to the sole cybersecurity sector", yet in this case, cybersecurity experts succeeded in gaining a privileged position (Hansen and Nissenbaum 2009:1168). This stronghold on cyber technifications entitles them to declare what "is 'good' knowledge and 'bad' knowledge" (Hansen and Nissenbaum 2009:1167). This capacity is for instance reflected in the establishment of good practices for companies and users or through the institutionalization of the field, but also through the informing of hacker's image (ibid.).

Last but not least, unlike the process of desecuritization, understood by the CS "as the movement of an issue out of the realm of security and into the realm of the politicized", technification aims at depoliticizing an issue, depriving its opponents of any possibility of contesting or debating it (Hansen and Nissenbaum 2009:1168). Again, this reinforces the hypersecuritization.

On the next page lies a blueprint of the model we introduced. It summarizes the cybersecurity securitization by putting forward the three modalities - hypersecuritization, everyday security practices and technification - their ties and the securitizing actors of the cybersecurity sector.

Amongst these actors, we find two categories: public and private sectors. For the former, we perceive the state as the main actor because it controls every other institution such as the Ministry of Defense, the military forces (land, marine, air, cyber) and so on. For the latter, we include private organizations that can play a role in the decision-making, but above all businesses such as ICTs businesses.

Figure 5 *The cybersecurity securitization*



Note: graph created from the content in Hansen and Nissenbaum (2009)

2.5.Speech Analysis Theory and Lexicometry

The Concept of Speech/Discourse Analysis and Cyberdiscourse

The first relevant clarification is the difference between language analysis and speech analysis. While the language analysis aims at pointing at "rules of conformity that can be found within grammars and dictionaries" (*translation ours*) and is rather descriptive, speech analysis, more analytical, is not only based on "rules governing the language but also on the combination of circumstances in which the medium is written or delivered and how it is delivered"(*translation ours*) (Charaudeau 2005:30). Besides, Charaudeau also indicates that "speech [is a place] where meaning is labeled, witnessing beliefs and knowledges' systems to which individuals and social groups adhere" (*translation ours*) (Charaudeau 2009:41).

As we indicated in the theoretical framework, we will adopt the logic of securitization and therefore be attentive to discursive practices as we think they convey more than just words but also beliefs. We will find these inside what we see as the cybersecurity discourse. To Dunn Cavelty,

> *the cybersecurity discourse is about more than one threat: ranging from computer viruses and other malicious software to cyber-crime activity to the categories of cyber-terror and cyber-war. Each subissue is represented and treated differently in the political process and at different points in time. Consequently, cyber-security policies contain an amalgam of countermeasures, tailored to meet different, and at times conflicting security needs.*(Dunn Cavelty 2012:105)

Indeed, "cyber security is a terrain on which multiple discourses and (in)securities compete" (Hansen and Nissenbaum 2009:1162) at "different points in time", as is underlined above. Nonetheless, we again only have features concerning the concept. Consequently, in our view, cybersecurity discourse or speech is the set of discursive practices that are reflected in the various documents that make up the cyberdoctrine.

Lexicometry and TXM

Given that our analysis includes a part dedicated to speech analysis, and especially lexicometry, we will also borrow a theory from the field of speech analysis. The resort to methods for processing pieces of information automatically is not new and goes back to the automatic speech analysis (ASA) developed by Michel Pêcheux (Leimdorfer and Salem 1995:131). ASA

relied on the codification of key themes, a method itself based on the syntax approach of Zellig Harris (ibid.).

Thus, drawing upon Pecheux's work, Salem designed the software Lexico (Salem 1987), which consisted in a statistical analysis of a text (Leimdorfer and Salem 1995:132; Lebart and Salem 1994). Later on, TXM, an open source software, was created by four French universities (Université de Lyon & Lumière Lyon II; Université de Nice Sophia Antipolis; Université Sorbonne Nouvelle - Paris 3 and Université de Franche-Comté) a Canadian university (Université du Québec in Montréal) and a British university (Oxford) (Heiden 2010:2). Its aim is to provide a software dedicated to textometry, which is a textual data methodology. In the words of the authors, TXM:

> *tries to always combine various statistical analysis techniques, like factorial correspondence analysis or hierarchical ascendant classification, with full-text search techniques like kwic [key words in context] concordances to be able to always get back to the precise original editorial context of any textual event participating to the analysis.* (Heiden 2010:2).

Further on, the functions and strengths of TXM will be explained.

2.6. Hypotheses

Now that we have covered the theoretical framework and the literature review, we begin to witness how powerful the securitization tool can be to advance the state's agenda. Through the discourse, states achieve the politicization of an issue by bringing it under their control and, as the literature review has shown, cyberspace is no exception.

Although we are aware that numerous actors are implied in the decision-making regarding issues related to cyberspace of a state, we argue that the actor who gives the final decision is the state. Indeed, we deal with the security sphere, which is traditionally the exclusive domain of the state, and cyberspace and its security belong to this category. With that in mind, we should consider that states are by essence following what is best for their country, especially if it feels threatened. Moreover, as we have seen, the cyberdiscourse has the particularity of being intertwined with all other types of security discourses (Hansen and Nissenbaum 2009). Then, through the securitization of cyberspace, not only do states gain a new space to control, they are also endowed with an instrument which can influence every other type of discourse. Based on these assumptions and keeping our research question in mind, this brings us to our first hypothesis:

H1: *The securitization of French and Italian cyberspaces aims at asserting their national interest.*

Nowadays, international relations are still governed by states. Although the world has changed since the tenets of realism have been formulated, some of them still remain valid today and the pursuit of the national interest is the best example. As Kempf argued, "in a multipolar system, actors keep on taking decisions fitting its own interests before the ones of the system" (Kempf 2012:191). Nonetheless, states are aware that ICTs change the rules of the game, and that fights are no more conducted on single battlefields and following strict conditions. Indeed, conflicts are now also conducted remotely and on multiple theatres of wars. That being said, we should see securitization as a way to ease the implementation of actions and policies following the subsequent pattern, namely: first, the identification of the threats to the national interest components (population, territory [both public and private premises, but especially the vital infrastructures] and sovereignty); then, defining their impact on the referent object (living and non-living entities); and eventually, the adoption of actions. Even within this logic, the securitization actor remains the state most of time. That is why we adopt a stance we could see as a realist constructivism. Numerous studies point to the securitization of cyberspaces (Gorr and Schünemann 2013; Hjalmarsson 2013; Klingova 2013; Lobato and Kenkel 2015) and we don't see why it should be any different for France and Italy. Still, they do not delve into the relationship between national interest and cybersecurity matters, and above all, show that they are more than intertwined, they are one with another.

H2: *the French discourse on cyberspace leans towards hypersecuritization, meaning it belongs to the power-sovereign type.*

H3: *the Italian discourse on cyberspace leans towards technification, meaning it belongs to the technical type.*

Drawing upon the literature, we decided to merge Nissenbaum's framework and Baumard's typology to not only obtain the type of cyberdoctrine followed by a state, but also the prevalent cyberdiscourse that accompanies it. Although, we will go through our methodological process in the next section, we must mention a few elements to understand our choice of hypotheses. From the four categories introduced by Baumard, we only kept three: societal (I), technocrat (II), and power-sovereign (III). Each of these corresponds to a dominant cyberdiscourse, which are respectively (I) societal rooting, (II) technical and jurisdictional cyberdefence, and (III) national cyberdefence. It must be pointed out that the types chosen for each country are not

random, they derive from the analysis Baumard had done on national cyber-crime doctrines over the period 1994-2017 (see Appendix 8) (Baumard 2017:14). The only difference with what we want to demonstrate is that he positioned each document per year on the matrix, while we seek to spot a trend of the dominant cyberdoctrine for each country. Furthermore, even though we link a predominant cyberdiscourse to a cyberdoctrine, we may find elements of other modalities in the same cyberdiscourse, as all three make up the cybersecuritization discourse. Indeed, we should not forget that "cyber security is a terrain on which multiple discourses and (in)securities compete" (Hansen and Nissenbaum 2009:1162).

3 - Methodological Framework

Now that we have reviewed the literature on the topic, introduced the securitization theory and presented our research question as well as our hypotheses, we now move on to the methodological framework. This section is divided in five parts. In the first part, we present the approach retained for the data collection, namely the mixed method approach. As the name indicates, both qualitative and quantitative will be used. Thus, in the two subsequent parts, tools and frameworks for the qualitative analysis are first presented, and the software used for the quantitative part, TXM, and its features are explained. In the fourth part, we put forward our criteria selection methodology for our case study, highlighting why we chose the French and Italian national cyberstrategies, presenting by the same token the nature of the documents analysed. The fifth part deals with the operationalization of the concepts.

3.1. Research Design

3.1.1. Mixed Methodological Approach

The methodological approach retained for our work is based on both qualitative and quantitative methods. In the literature, there are various names that refer to this combination, but for the sake of clarity we will not only use a single appellation but also the framework attached to it, namely the mixed method approach (MMA) (Teddlie and Tashakkori 2003; Bryman 2006; Creswell and Creswell 2009).

MMA relies on four main factors to consider when elaborating the research strategy: timing, weighting, mixing and theorizing (Creswell and Creswell 2009:203–24). As you can see from the table below, our research scheme falls into the second case of the possible MMA scenarios.

Table 1 *Aspects to Consider in Planning a Mixed Methods Design*

Timing	Weighting	Mixing	Theorizing
No Sequence concurrent	Equal	Integrating	Explicit
Sequential-Qualitative first	Qualitative	Connecting	
Sequential-Quantitative first	Quantitative	Embedding	Implicit

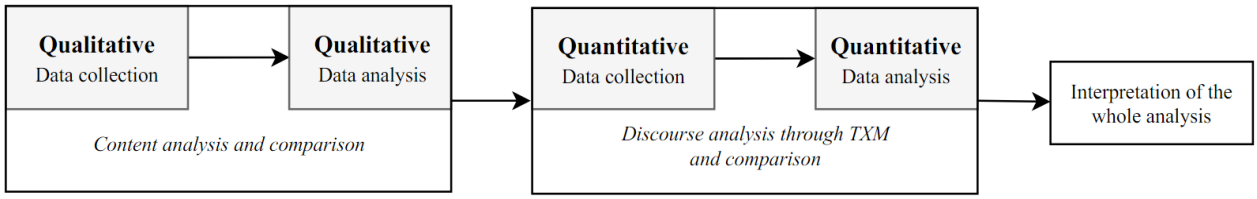
Note: Adapted from Creswell et al. (2003) in Creswell and Creswell (2009:207) from Figure 10.1

Indeed, the data will be collected following a series of sequences. In a first part, we will conduct a qualitative data collection and in a second part, we will perform a quantitative data collection. In our case, the analysis order does favor one method over the other: the qualitative has more

weight in the analysis. This corresponds to what Creswell calls a connected mixing, which implies that a researcher wants to connect the two results of his data collection and mix them between the "data analysis of the first phase of research and the data collection the second phase of research." (Creswell and Creswell 2009:208). The precise outcome of this integration will be detailed below, in the section explaining how the different frameworks are mapped together and how our main theory of securitization is linked to it.

Yet, such method comes with a variety of challenges. Nonetheless, Creswell devised an array of strategies to follow in order to ease the process. Among the six major strategies suggested, one fits perfectly with our research design and is called sequential exploratory design (Creswell and Creswell 2009:210).

Figure 6 *Sequential Exploratory Design*



Note: Adapted from Creswell (2009:210) from Figure 10.2 (b)

As you can see from the graph above, the approach follows two steps. The first phase is dedicated to the qualitative data collection and analysis, while the second phase introduces the quantitative tool (here TXM). The second phase builds on the results found in the first one, hence the name exploratory (Creswell and Creswell 2009:211). As our work involves two countries, the final stage also involves a comparative analysis.

Our main interest in selecting this method lies in the fact that it enables us to explore a phenomenon and to "develop an instrument" when there is none available (Creswell and Creswell 2009:212). In our view, it means being able to create a framework suited to analyze states' cyberstrategy. Furthermore, the benefits of this mixed approach are twofold. First, the procedure is quite straightforward, qualitative then quantitative, which makes it easy to implement. Second, using both data collection allows "to expand the qualitative findings" and offset the weaknesses of each method (ibid.). Indeed, while some authors argue that it is better to use different data for the qualitative analysis part and the quantitative part (Teorell and Svensson 2007:84), we function differently, putting forward that qualitative and quantitative

methods are two different data collections. They do not reflect the same outcome, but together they can bring about diverse visions on the same phenomenon.

Yet, MMA poses several methodological issues. What we mentioned above as challenges are the following: "the need for extensive data collection, the time-intensive nature of analyzing both text and numeric data and the requirement for the researcher to be familiar with both quantitative and qualitative forms of research" (Creswell and Creswell 2009:205). As time is the main challenge for us, the period and the corpus are defined.

3.1.2. The Case Study Method

Even though we chose to adopt a mixed method approach, our main aim is to compare the implementation of the national cyberstrategies in France and Italy. We thus draw upon a traditional case study method, intended as "both within-case analysis of single cases and comparisons amongst a small number of cases" (Sprinz and Wolinsky-Nahmias 2004:21). Indeed, we will study the two countries to compare them afterwards.

Using the case study method presents an array of advantages. The first being the operationalization of qualitative variables which can guarantee "high levels of conceptual validity". Then, while one can rely on previous works to improve them, new variables can be set up. The third advantage is especially valid for researchers resorting to process tracing, as causal mechanisms can be unveiled. The fourth advantage is the construction of highly descriptive and detailed accounts, as the method demands an extensive analysis. The fifth advantage is the "analysis of complex causal relations through contingent generalizations and typological theories in instances of equifinality and path dependency"[16] (Kacowicz 2004:108).

Notwithstanding, the case study method is not exempt of drawbacks. First, there can be a case-selection bias and thus, results abstracted from these methods cannot provide us with generalizations. Second, the findings can result in a "potential indeterminacy" due to the variable selection imposing a tradeoff between representability and accuracy. Third, for a single case study, the results can bear limited range as the researcher can take into account every covariation and causal effects (Kacowicz 2004:108).

[16] For a more detailed account on case study benefits, see Bennett (1999,3; 2000); Collier (1993); Bennett and George (1997c, 8, 12); Eckstein (1975, 80); George (1979, 61); Ragin (1994, 81); Maoz (2002, 2–3).

In his work on "Case Study Methods in International Security Studies" (2004), Arie M. Kacowicz describes case studies as a middle ground to provide a "methodological bridge" between neorealists and constructivists (Kacowicz 2004:109). While this statement seems convincing, he also argues that constructivists tend to adopt a comparative method "usually neither structured nor focused" (Kacowicz 2004:111). Since we rely mainly on constructivism, through securitization theory, and to some extent realism, we will indeed not provide the mode of comparison, such as the most similar system design, but directly move to the comparative framework.

3.1.3. A comparative framework

What is peculiar in our case is the fact that our comparative framework is embedded in the MMA approach.

The comparative analysis is an old-fashioned method but has proved to be useful in numerous studies. Among its main advantages, we find a predilection for studies including small number of cases (Lijphart 1971:684), which fits to the first part of our work, where the unit of analysis is the state. Moreover, going for a comparative analysis implies selecting few variables, hence our choice of mixing here the two above explained frameworks, which allows us to classify states into specific categories. This choice will enable us to discover what Lijphart calls "general empirical propositions" (Lijphart 1971:682–683). He adds that "with an intermediate number of cases, a combination of the statistical and comparative methods is appropriate" (Lijphart 1971:685). This is where our choice of MMA proves interesting. While in the first part, we fit it to the few cases analyses, we are also able to fit the second category of intermediate range analysis, thanks to the series of documents used in the second part.

This is not the only drawback that our approach allows, if not to avoid, at least to circumvent. Usually, there are two main criticisms addressed to researchers adopting the comparative analysis method: (1) the difficulty of tackling several variables because it does not possess the exhaustiveness provided by large-case analysis, resorting to a statistics method and (2) "the fallacy of attaching too much significance to negative findings" (Lijphart 1971:684–686). Again, MMA will help to rectify the potential bias as a result of the second part that comes as the validating or invalidating factor. Nevertheless, as we have seen in the previous section, MMA is not exempt of criticism.

Regarding the comparative method, Lijphart points to several paths to offset the weaknesses entailed in the comparative method. A first path consists in increasing "the number of cases as much as possible", which in our case is not possible for the first part but applies to the second part. A second path aims at reducing "the 'property-space' of the analysis" - which means combining similar variables - and corresponds to our adoption of the mix between Baumard's typology and securitization's framework. A third path has to do with the analysis of similar and "comparable" cases that makes it easier to discover partial generalizations and control the other variables (Lijphart 1971:686–688).

3.2. The qualitative tools

As said above, the first part of the analysis will be dedicated to the qualitative analysis. This part is divided in two phases, one rather descriptive, and the second one more analytical.

During the first phase, we will introduce the main features of each document, highlighting them and the undertaken actions. In the second phase, we conduct an extensive content analysis. Indeed, drawing upon a framework realized by our care, a first qualitative assessment of both countries, France and Italy, will be undertaken, providing us with a firsthand knowledge of the cybersecurity landscape. The period covered will range from 2008 to 2018.

To achieve a comprehensive framework, we came back to the previous frameworks presented namely in Baumard's typology (Social order (I), Technocrat (II), Societal Resilience (III), Power- sovereign (IV)) and Hansen's cyber security framework analysis (discourses on (1) hypersecuritization, (2) everyday security practices and (3) technification). By analyzing the two frameworks we concluded that elements were missing to adapt them to our work. The whole process demonstrating the creation of our framework will be explained in the operationalization of the qualitative tools.

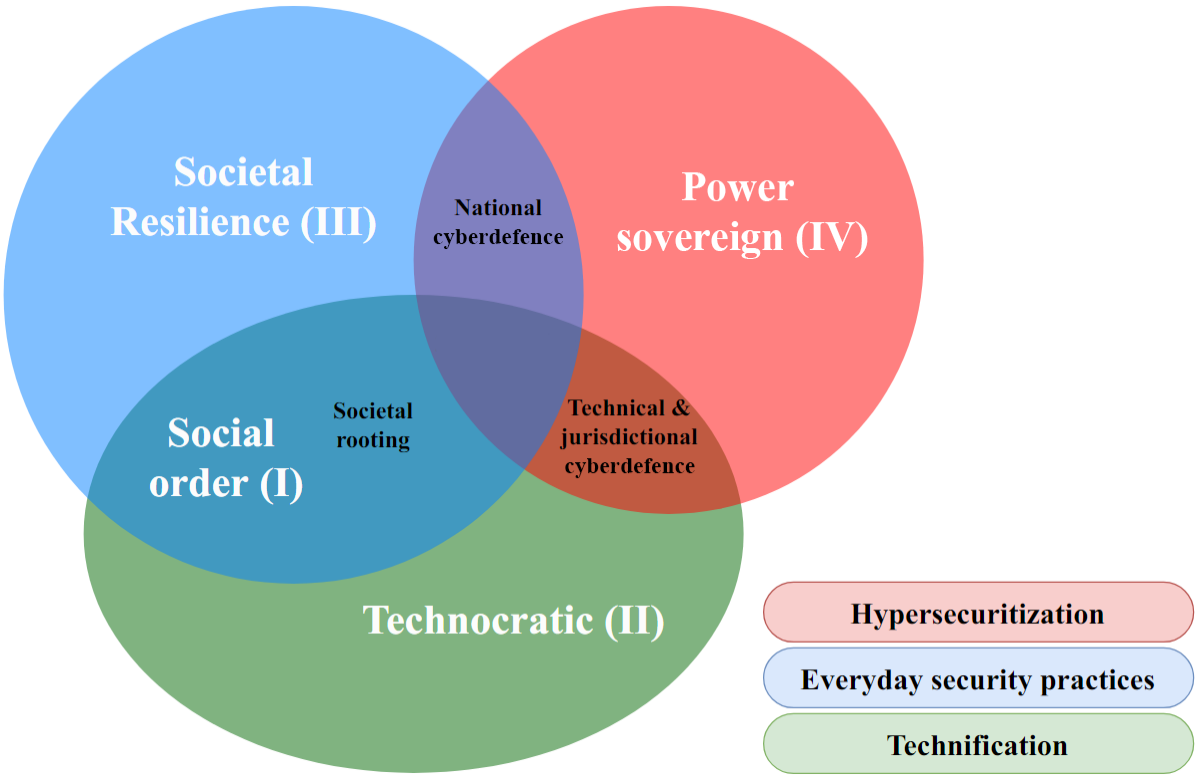
Let us have a look at Baumard's work first. Despite providing a thorough analysis, he does not provide any guidelines or steps that could be used by others to apply the analysis to other countries. Moreover, in his results he classifies the national documents per year. We want to position the country in average over 10 years to better reflect long-term trends. On top of that, he only considers formal documents (white papers) in his matrix; however, we think that the cyberstrategy/doctrine is also influenced by the legislative (bills) and other government

officials' statements. Therefore, our selection of documents is broader[17]. As far as Hansen and Nissenbaum's framework is concerned, it is sufficiently complete on its own but like Baumard's work, it has to be integrated into a more detailed framework.

That being said, we chose to mix the two frameworks by juxtaposing their criteria and we were able to abstract a set of rules by mixing the two frameworks, namely:

- Countries fitting to type I tend to adopt a mix between technification and everyday security practices discourses;
- Countries fitting to type II tend to adopt a discourse leaning technification;
- Countries fitting to type III tend to adopt a discourse leaning towards everyday security practices.
- Countries fitting to type IV tend to adopt a discourse leaning towards hypersecuritization;

Figure 7 *Mixed securitization framework*



[17] For the first part of the analysis.

The mixed securitization framework provides a double outcome. Indeed, by the end of our qualitative analysis, we should be able to classify France and Italy in one of Baumard's categories and, consequently, detect the prevailing discourse's modality used by both countries.

3.3. The quantitative tools

After drawing conclusions from the first part, the second step consists in conducting a quantitative data collection. Following the MMA approach, findings of the first part will influence the second one. Nevertheless, the quantitative part also draws upon two tools which are intertwined.

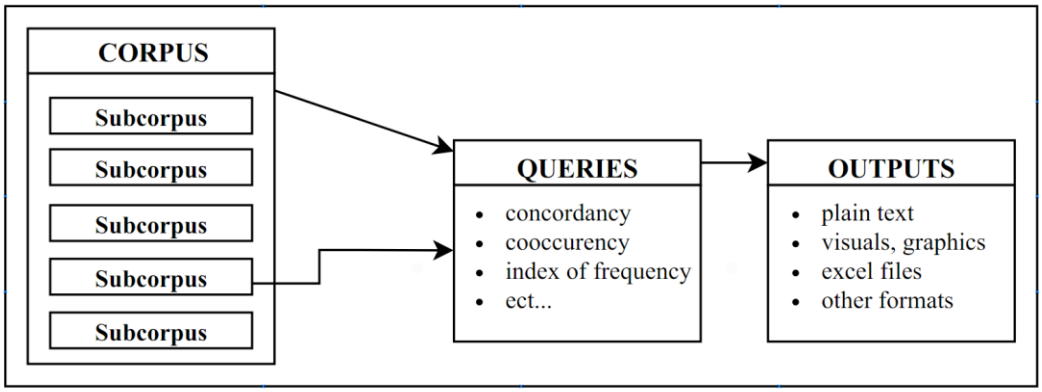
The first tool comes from a general empirical observation given by Teorell and Svensson, arguing that "in finding a balance between the automation and sophistication, there is bound to be a tradeoff between reliability and validity (Teorell and Svensson 2007:269)" (as cited in Hjalmarsson 2013:5). This observation implies the building of a systematic framework. In our case, this entails building a codebook (divided in the three types of discourses highlighted in the here above figure 7) that will be fully explained in the operationalization.

It is possible that the first qualitative analysis reflects the incomplete character of this framework. However, this version already constitutes a strong basis for the analysis as such. Moreover, each word listed in the codebook should be seen as a concept per se, that is, it might probably refer to multiple words when we index all the word frequencies. Indeed, without the mapping of the word frequency and proper software, the codebook does not really help us. This is why we use a lexicometry software used in the academic world called TXM (Heiden 2010). In order to understand the reason why we use this software, we must first understand TXM's rationale.

The strength of TXM is to provide researchers with a set of functions to analyze a series of text, called corpus, which divides it into groups of texts, called subcorpora. It performs different kinds of operations, called queries, that allows us to retrieve words, syntagma and compare them with each other. The queries can be either applied to the whole corpus or to a defined subcorpus. What is especially interesting for us is the use of taggers and lemmatizers which are plugins that enable the software to tag corpora 'content from other languages. Language is thus not a barrier as far as lexicometry is concerned.

There are a few key concepts that will be used in our lexicometry analysis: the corpus and sub-corpus have already been mentioned above; the specificity analysis, which is a process highlighting the frequent use of a word or the contrary; the cooccurrences, which are also known as collocations in English, refer to words that are frequently used together; the concordance, which displays every phrase in a text where a selected word appears; and the hierarchical index or index of frequency, which aims at listing the most frequent words used in a corpus.

Figure 8 *Ecosystem of TXM*



Note: Elaborated from the description provided in Heiden (2010).

The table above summarizes the workings of TXM. It is interesting to notice that the software allows multiple output formats that can be easily adapted for our research. We will mainly use the following functions: concordancy, coocurency and the index of frequency.

Eventually, before moving on to the cases, we would like to highlight a quote putting forward another reason to employ lexicometry in the framework of securitization discourse analysis:

> *Discourse analysis is not the exclusive method securitization studies. a complete analysis will also include more traditional political analysis of "the units interacting, facilitating conditions, and all of the other dimensions of security complex theory. But to see whether securitizations are separate or are defined by each other, a study of the actual phrasing of the securitizing moves seems appropriate.* (Buzan, Wæver, and De Wilde 1998:177)

Thus, the main interest of using TXM is to empirically show the direct link between the cyberdiscourse and securitization. Indeed, by looking closely at the iterations of words and collocations, we will be able to gather elements improving the validity of our findings from the first quantitative analysis. Moreover, quantitative data present a double advantage. On the one hand, data can be presented through both numeric and visual representations. On the other hand,

quantifying data allows to better understand how these iterations can be used to detect and predict decision patterns.

3.4. Cases Selected

In the previous sections, we have explained how the analysis is structured. We now move on to the presentation of the cases and the documents used. As already mentioned, we focus on two countries, France and Italy, and their implementation of cybersecurity policies during the period going from 2008 to 2018. First, the choice of the timeframe is explained. Second, the two cases are presented, putting forward their similarities and differences. Third, the academic purpose of studying these two cases is presented. Fourth, the documents on which the analyses rely are briefly introduced.

First, the temporal choice was shortly brought up during the introduction, which spans from 2008 to February 2018. The reason is quite simple. As far as the start of the period is concerned, a wave of cyberattacks struck Estonia in April 2007, as highlighted by numerous authors (Dragosei 2007; The New York Times 2007; Hansen and Nissenbaum 2009:1159). It sounded the alarm throughout the EU and urged the countries still deprived from a real cyberdoctrine, like our two countries, to adopt one. The end of the period, namely February 2018, corresponds to the release of the two last major documents shaping priorities for the two countries.

Furthermore, France and Italy are two very similar countries in multiple regards. First, their location. Both countries are rooted in the European continent and possess a common history. Then, they have a similar population size. Besides, not only are the two countries democracies sharing the same currency, they also both belong to the same institutional arrangements at a regional (Council of Europe, OSCE, EU) and international level (OECD, WTO, NATO). Finally, unlike the United Kingdom, Germany or the United States, France and Italy were both late comers in the adoption of a cyberdoctrine (Romani 2007:32–34).

Table 2 *Similarities between the cases*

Features	**France**	**Italy**
Political system	*democracy*	*democracy*
Values	*European*	*European*
Genesis of their Cyberstrategy	*2008*	*2012*
Members of the same organizations	✓	✓

Despite these similarities, several sources, both academic (Kempf 2012; Baumard 2017) and non-academic (ITU 2018), show that the two display different cyberpower capabilities (Kempf 2012:174–175). Indeed, the cyberpower intended by Kempf corresponds to the power in terms of economical, technological and military capabilities linked with cyberspace. It is divided in five criteria: the digitalization of the society, the existence of telecommunications, information, communications and internet-linked companies in the country, the presence of a cyberdefence, a written cyberdoctrine and the cooperation with other actors several characteristics. Each of these criteria is divided in indicators.

Table 3 *Cyberpower indicators*

Features	Indicators
Digitalization of the society	• Computer per capita • Phone per capita • Smartphone per capita • Revenue linked to e-commerce
Telecommunications, information and communications as well as Internet-linked companies	*Not indicated,* but Kempf accounts probably for the number of them within the country
Presence of a cyberdefence	• Budget dedicated to the sector • Existence of links between the actors of cyberspace • Economic intelligence service
Cyber doctrine (white papers or official statements)	• General action both at domestic and international levels • Willingness to act on the three layers
Cooperation with other actors	• On equal basis (centralization or development) • Or third-party relations (sales and foreign aid)

Note: Elaborated from the description provided in Kempf (2012: 174-75)

Drawing upon what he knows from the classical rankings of power, Kempf suggests a ranking of cyberpowers, putting in a first group - United States, Russia, China, Israel, the United Kingdom, Germany, France, Japan and India; and in a second group - South Korea, Taiwan, Australia, Canada, Brazil, Italy, Sweden, Singapore, Finland, Estonia. However, Kempf adopts a careful stance in his estimations, arguing that these lists may prove incorrect and incomplete. Indeed, in his book, he does not provide any data backing up this statement, but he indicates that countries tend to hide a part of their power to avoid arms races and also to keep an advantage over their neighbors (Kempf 2012:175).

As we said above, non-academic sources also mentioned the difference in Cyberpower between France and Italy. The international telecommunications Union (ITU) has built up a Global

Cybersecurity Index (GCI) over the past year. It is based on five pillars (legal, technical, organizational, capacity building and cooperation) and in the 2017 GCI report, out of the 193 ITU members, it ranked France at the 8th and Italy at the 31st (ITU 2017). Though, if we compare the two countries in terms of world military expenditure in 2016, France is at the 6th rank while Italy is at the 11th rank (Tian et al. 2017). Again, these two instances only have the aim to underline a difference between the two countries and justify an extensive case study of the two.

As we mentioned before, just like France, Italy is a latecomer in the cybersecurity field. However, the gap described in official studies seems to underline that there may be another factor influencing such differences. This is where we introduce the securitization of cyberspace.

The interest for the research lies in several points. The first one is the method we use. Indeed, the mix-method analysis will enable us to provide information on the latest developments occurring in both countries, confront this data and being able to support the results with the qualitative tool. The second point is the fact that it is rather rare to find studies on France and Italy, especially from a comparative perspective. The third point connects with the second insofar, as far as we know, the securitization of the French and Italian cyberdiscourse have never been studied together, nor in this fashion. The fourth point is the access to the source, the mastery of the two languages implied in the study allows to provide a firsthand account that would not be possible otherwise.

Both analyses are based on the same type of documents that is French and Italian reports, bills, national strategy white papers[18]. The main documents that define the cyberdoctrines carry various names but few of them are identified as white papers or national strategy. For the first part of the analysis, every type of document will be mobilized whereas in the second part, we will only use documents of the same nature as this is one of the requirements of speech analysis, but also because preparing each document requires more time and space.

[18] Cf. appendix 13 and 23 for the complete list.

3.5. Operationalization of the Concepts

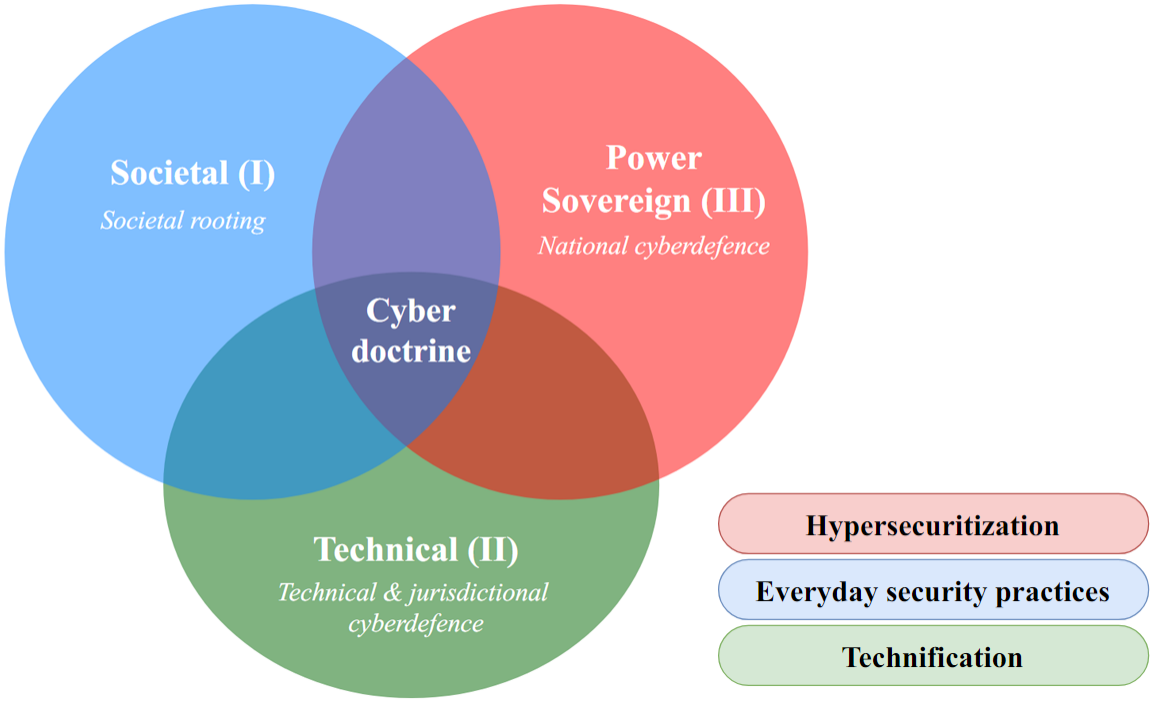
Before moving on to the analysis, we need to explain how we mobilize the concepts explained in the previous sections. This section will be divided in two parts. In the first one, we explain how we mobilize Baumard's typology of national cyberdoctrines (Baumard 2017:69–72) to list the concrete actions undertaken by the states, and class them in a framework elaborated by our care. In the second part, we detail the operations that will be using a lexicometry software which relevance has already put forward.

3.5.1. Qualitative cyberdoctrine framework

For the first analysis, we perform an extensive analysis and draw upon a series of documents including white paper on defense, reports, decree, bills. In order to both respect the securitization and speech analysis theories, we must define a few parameters. We consider the state, represented by the head of state in each country, as the sole securitizing actor, as he has the last word on the decision-making process. The other actors are thus viewed and will be referred as sub-actors or called by the name of their function. This could be the case for the Ministry of Defence, the Ministry of the Interior or the Prime Minister. Then, although all documents are not fully written by the head of the state in the two cases, we also assume that since he is the one commissioning its drafting, the state is the legitimate author of the texts. Eventually, speech analysis requires the analysis of documents of the same nature. This is the reason why we consider all the types mentioned above as included in the type of strategic policy papers.

The framework we mobilize was inspired by the work of a few authors (Gorr and Schünemann 2013; Hansen and Nissenbaum 2009; Baumard 2017). To determine the type of cyberdoctrine embraced by the two states, we used the four categories - Social order (I), Technocrat (II), Societal Resilience (III) and Power- sovereign (IV) – in the methodologic part. However, since Baumard did not specify the steps to follow to obtain these four categories, we decide to merge the two social to only get one Societal category. Should one of the countries fall into that category, we can determine later if the country leans more toward the Social order or the Societal resilience.

Figure 9 *Qualitative cyberdoctrine framework*



Note: Elaborated by our care.

This merging allows us to get a perfect match of our two frameworks presented above, namely the cyberdoctrine and cyberdiscourse frameworks. Thus, we obtain three categories: Societal (I), Technocrat (II), and Power sovereign (III). Each of which following different decisions pattern: (I) societal rooting, (II) technical and jurisdictional cyberdefence and (III) national cyberdefence.

Nonetheless, this does not tell us how to rank each country's behavior. To that end, we operationalize our main concepts for the qualitative part. The first concept of cyberdoctrine is made up of three dimensions: Societal (I), Technocrat (II) and Power-sovereign (III). To measure each of these dimensions, we take into account the actions falling into the categories of societal rooting for the first dimension, of technical and jurisdictional cyberdefence for the second dimension and of national cyberdefence for the third one. Again, since Baumard did not really give any concrete examples, we will give indicators we consider fitting to these categories.

Table 4 *Operationalization of the qualitative concepts*

Concepts	Dimensions	Indicators
Cyberdoctrine	Societal (I)	Actions falling under the societal rooting such as • Sensitive to opinion movements; • influence of the public space actors (including. hacking civil groups) to a certain extent Europe; • Have an "information warfare" active component; • Weak or borrowed national vision • Inclusion of the society through awareness campaign or good practices diffusion • Education
	Technocrat (II)	Actions falling under the technical and jurisdictional cyberdefence • incident-Response philosophies; • technocratic and delayed perception (also offensive) • domination of the technical expertise (ie. Police); • vertical walls and jurisdictional response;
	Power-sovereign (III)	Actions falling under the national cyberdefence: • Creation or expansion of large specialized units or military corps; • Obsessed with critical infrastructures; • development of offensive and defensive capabilities;
National interest		Definition of the national interest or Delimitation of the geopolitical, economic and information assets of a country viewed as critical sectors Threats to: • components of the State, • the sovereignty, • survival of the state, • cyberspace and its components,

Note: Elaborated by our care.

Nota bene: As we have seen in the concept, national interests encompass the other concepts, which is why it may be probable to find decisions that can fall in the categories of defense of the national interest and one of the cyberdiscourse. With that in mind we will classify for each document every decision under the national interest category specifying the threat and then specify to which cyberdiscourse it corresponds.

3.5.2. Quantitative cyberdiscourse framework

We now come to the quantitative operationalization. First, we will explain how we will prepare the texts for the lexicometry software TXM. Second, we will move on to the operationalization of our quantitative framework.

Although all the queries executed within the software TXM are programmed, we still have to prepare and "clean" the text. This step consists of putting all the files in the right format supported by the software. The entiere content is then put into small caps, ready to be processed. These steps are very important as they can distort the results if not done properly.

To obtain applicable results, we will only work on the longest documents and the more relevant documents that set cyberspace strategy doctrine for each country. For France, these are the White Paper on National Defence and Security of 2008; the France's Information System Defence and Security of 2011; the White Paper on National Defence and Security of 2013, the French National Digital Security Strategy of 2015 and the Defence and National Security Strategic Review of 2017. For Italy, these are the 2013 National Plan for Cyberspace Protection and ICT Security and the 2017 National Plan for Cybernetic Protection and Information Security.

The data being presented, we can now explain how we conceptualize it. To that end, we will draw upon a codebook elaborated by Katarina Klingova in her work on the "Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia" (Klingova 2013:42). By following this pre-existent codebook, we can construct a model before analyzing the primary sources and improve it after the first qualitative data collection. In this way, we will focus on the main areas of interests and avoid getting lost in superficial word counting.
It is important to notice that these lists are not complete and will be modified after the first part of the analysis.

Table 5 *Codebook for securitization discourse*

Concepts	Dimensions	Indicators (occurrences of the words or words linked)	
Securitization	Everyday security practices	Society Population Community Individual Vital activities Goods Privacy of data Society as a network Dialogue/consensus Collaboration	Training/education Awareness Public/private sector Freedoms Rule of law Interdependence Connectivity (social dependence) Competence (individual as well as global)
	Technification	Specialists Computer experts Network Disruptions Software/Hardware Malware Standards of information/norms Vulnerability reduction Incident response Interoperability	System management/ provider/operator Prevention Capacity building Intrusions/disruptions Access/connectivity User-end Stakeholders Intellectual property/data
	Hypersecuritization	Nation State Government State authority War Hostile aggression/attack Armed conflict Defense Destruction Command	Deter/defend Global issue Terrorists Organized crimes Cascading effect Military/armed forces Catastrophe Cold War analogies Critical infrastructures Escalation
National interest		Delimitation of the geopolitical, economic and information assets of a country viewed as critical sectors Threats to: - the sovereignty, - survival of the state, - cyberspace and its components,	

Note: Adapted and borrowed from Klingova (2013:42).

Thus, we will look at the different occurrences by indexing the 300 first forms of each text and then sort out the words fitting to the three categories to represent the types of cyberdiscourse employed within each state.

4 - Analysis

We now enter the center of our work. As indicated in the previous section, this analysis will be twofold, both qualitative and quantitative. In a first part, the two French and Italian national cyberstrategies will be analyzed separately from 2008 to 2018. Then, in a second part, we confront the results of the two analyses to compare the national cyberstrategy construction. The country's analysis per se is divided into three steps. The first step aims at going back to the chronology of the country's implementation of cyberdefence national strategy, looking at how the cyberthreat is perceived, who the main actors and priorities are, and finally, what the concrete actions undertaken to tackle the issue are. The second step is dedicated to the quantitative analysis through the lexicometry software TXM in which we will check if our findings are confirmed or not. The two steps are complementary as the first one helps us to compile data to build a framework available in the appendixes for each country and add new words for the second step. The third and final step shows which realist scenarios or principles are used by states in their representatives' discourses to push forward their agendas, and what kind of cyberdiscourse is used by states throughout the devise of their strategy.

4.1.French and Italian national cyberstrategies (2008 to 2018)

4.1.1. French Case

4.1.1.1. *First step (Descriptive)*

The protection of information systems, what we would encompass in the cyberspace, was already a concern before 2008. Kempf informs us that the French member of parliament (MP), Pierre Lasbordes, issued a report in 2006 called *La sécurité des systèmes d'information – Un enjeu majeur pour la France* (Information systems security – a major concern for France) which aimed at assessing not only the information systems security but also the critical infrastructures as well as the business world (Kempf 2012:194). His results pointed to several weaknesses: a lack of cohesion and autonomy of the different actors of the sectors as well as insufficient means and vulnerable companies (ibid.). But, the wake-up call was the series of attack that occurred in Estonia in 2007 as French authorities/infrastructures had also been targeted to be spied on (Romani 2007:5). In this context, a white paper was mandated by the former French president Nicolas Sarkozy in a letter released in 2007 (Commission du Livre blanc sur la défense et la sécurité nationale 2007).

- *French White Paper on Defence and National Security 2008*

The 2008 French white paper is a milestone in the conception of the national cyberstrategy. The whole white paper is divider in chapters, but we can distinguish three main themes that are relevant for us: the definition and the assertion of national interest's elements, the changes and actions to be implemented; and the dedicated financial means.

First, an interesting element to be underlined is the French definition of the national security strategy, which aims at "provid[ing] responses to 'all the risks and threats which could endanger the life of the Nation'"(Mallet, France, and France 2008:301). The underlying consequence of this statement is to denote the threats and risks for its national interest. The simplest way to do it is to distinguish around which topics the word interests is used. In the protection chapter (XI), they are designated as "vital" or "national interests", while in the intervention chapter (XII), French representatives talk about "strategic" or "security interests".

The former interests refer to the population and the territory, we even have a map of the defense and security zones covered, namely seven national zones and five overseas areas (see Appendix 5) (Mallet, France, and France 2008:172). In addition to these zones, the white paper indicates which sectors are considered as critical infrastructures. In that regard, the regulation of 2 June 2006 includes the following: "civil activities of the state; judiciary activities; military activities of the state; food; electronic communications, audiovisual and news media; energy; space and research; finance; water supply; industry; health and transport" (Mallet, France, and France 2008:179). The cyberspace is not entailed here but with the 2008 white paper, things change as "the internet will need to be considered as critical infrastructure and considerable effort will be made to improve its resilience" (Mallet, France, and France 2008:174).

For the latter interests, France's goal is to "maintain the force projection capability necessary to defend its security interests and responsibilities" (Mallet, France, and France 2008:191). Nonetheless, a topic belonging to the protection of the nation does not appear here: the protection of sovereignty. We must go to the end of the white paper to read the following statement:

> *France must retain its areas of sovereignty, concentrated on the capability necessary for the maintenance of the strategic and political autonomy of the nation: nuclear deterrence; ballistic missiles; SSBNs and SSNs; and cyber-security are amongst the priorities.* (Mallet, France, and France 2008:306)

From this statement, it is clear that the cyber-security sector is a key domain for France to maintain its sovereignty. Moreover, if we associate this element with what we said above, we understand to what extent cyberspace became relevant for the French state from 2008 onwards.

Then, we move to the main measures envisioned by the national cyberstrategy. Here again, there are three different themes to be detailed: the protection of the national interest (population, territory and sovereignty) and consequently, the protection of the critical information, the technical actions and the cyberwarfare decisions.

As far as the population and the territory are concerned, these measures are the following:

> *develop the surveillance of national spaces and those in which France has interests, including outer space; acquire active, in-depth cyber-defense capability, combining the intrinsic protection of systems, constant monitoring of critical networks and a rapid response in the event of attack; [and] develop a new strategy and modernise population alert and information systems and crisis communication systems* (Mallet, France, and France 2008:190).

To understand how these actions would be implemented, we have to look at the intended actions for the protections of the critical information systems. Indeed, in the chapter related to protection (XI), the authors of the white paper again list actions aiming the cybersecurity sector. First, there is the setting up of a detection center aiming at detecting cyber-attacks thanks to "early-warning systems" (Mallet, France, and France 2008:174–175). Then, we can mention the conception of "security products and trust networks" which include "very high-security products to protect State secrets, as well as a range of guaranteed 'trusted products and services'" (Mallet, France, and France 2008:174–175). This basically amounts to the introduction of encryption among the secret states' services. In addition to these actions, there are other legal and symbolic statements. The most important decision being the setting up of a new agency in charge of the information systems security, which is known today as the National Cybersecurity Agency of France (ANSSI).

However, the technical side of this white paper should not be forgotten. One of the main aims of this document is to promote the expertise in the domain of information security systems. In practice, this means increasing the number of specialists in order "to create a reservoir of competencies". Pursuing along the same line, we can mention the establishment of information system security observatories in the defense and security zones we mentioned above ((see Appendix 5). The purpose of these observatories is to constitute a nationwide network of

experts (Mallet, France, and France 2008:174–175). It is interesting to notice that the French state talk about information systems and not cyberspace.

Eventually a whole part is dedicated to the offensive cyber-war and especially what is understood as such (Mallet, France, and France 2008:199). In other words, the 2008 white paper involves the definition "of an overarching concept incorporating all actions involved in cyber-war" but also the "formulation of a body of doctrine for offensive cyber-war capabilities (planning, execution, evaluation of actions". Nonetheless, the French state put a reserve, as "the concept must be compatible with the legal principles of French legislation and respect the principle of proportionate response, with the adversary's operational assets as its priority target"(Mallet, France, and France 2008:199). Thus, an important part of this white paper is to rethink warfare "to fully integrate digital transformation of defense"(Baumard 2017:56). For the political side, this is a task that will be carried out by the new Defence and National Security Council (Mallet, France, and France 2008:306), which set the defence and security aims. For the research side, the 2008 white paper also entails the creation of a "scientific interest grouping" (Groupement d'intérêt scientifique) which aims would be to "oversee projects and publications supported by a number of proactive universities and institutions"(Mallet, France, and France 2008:295). This will become the High Council for Strategic Education and Research (CSFRS) in 2009, which will include the state and its ministers but also the major French schools and companies to fulfil its mission (JORF 2009).

The 2008 white paper also advocates for a development of the "technological capabilities", emphasizing on the relevance of having an active and offensive cyberstance, particularly through "the development of defensive and offensive cyber-war capabilities but also the development of specialized tools (networked digital weapons, technical and operations laboratory, etc.)" (Mallet, France, and France 2008:200). Integrating these new technologies inside the defense sector implies training the personnel. The white paper also answers to this issue.

All these actions belong to a two-staged plan going from 2008 to 2025 (Mallet, France, and France 2008:206). What is important is to note that dealing with "cyber-war and networked operations" is part of the first stage, and consequently belongs to the top priorities. Most of these decisions point at the defense of the national interest and fall into the categories of technical and power-sovereign discourse.

Turning now to the finance part of this white paper. The first element backing the idea of a realignment of the French cyberstrategy is the following: the "funding of France's national security must be consistent with its analysis of its security interests, the risks France faces, and the definition of the necessary assets to confront those risks and prevail" (Mallet, France, and France 2008:273). In other words, France is willing to dedicate a part of its defense budget to the cyber-sector. To illustrate this, we see that the budget dedicated to the so-called "Defence Mission"[19] amounted to 36.8 billion Euros in 2008 and is intended to grow (Mallet, France, and France 2008:277).

We have just seen that the main outcomes of this first white-paper were a reshaping of the national defense and national security that are seen as one. Its main aim was to answer and propose concrete actions to correct the weaknesses brought about by the Lasbordes and Romani's reports (Lasbordes 2006; Romani 2007). The protection of cyberspace, even if it is not referred to as such (information systems), not only became a key component of the two elements mentioned above, but also one of the top priorities to preserve sovereignty. Eventually, the new agency we mentioned is the unifying piece that will offset the lack of synergy exposed in the mentioned reports (Romani 2007:41).

Indeed, the National Information Systems Security Authority (ANSSI) was created the following year through the issue of a decree (n° 2009-834 of 7th July 2009), replacing a former organization dealing with the security of the information systems (Légifrance 2009). The ANSSI was attached to the Secretary general of Defense and National Security (SGDSN), which is under the authority of the Prime Minister and helps him in "fulfilling his responsibilities in matters of national defense and security" (for the ANSSI's organization chart see Appendix 7) (ANSSI 2018a). Two years after its creation, the ANSSI, under the authority of the SGDSN, released its first major publication.

- *France's strategy - Defense and security of the information systems – 2011 (p.24)*

This document was released by the SGDSN in 2011. It follows the directions that had been mentioned in the 2008 white paper and reasserts 4 strategic aims: (1) "be a cyberdefence world power"; (2) "safeguard France's ability to make decisions through the protection of information

[19] Excluding "expenditures of the Ministry, which come under Security in the case of the Gendarmerie, Veterans, National Memorials and Remembrance Policy, and Research and Higher Education as well as for the Ministry's contribution to the civilian research budget" (Mallet, France, and France 2008:277).

related to its sovereignty" [20] ; (3) "strengthen the cybersecurity of critical national infrastructures"; and (4) guarantee "security in cyberspace"(ANSSI 2011b:11–14). Indeed, among the major threats expected for the next 15 years that the French government dreads the most, we find high-scale attacks on national infrastructures, that is the critical and national infrastructure mentioned above (ANSSI 2011b:7). Thus, this document on the French strategy in terms of information systems supports the same set of decisions and actions decided in the 2008 white paper (indicated as (WP 08) before the same decisions), namely all the decisions related to the sovereignty and the critical infrastructures protection, but also the development of encryption and expertise. Nonetheless, although it summarizes decisions taken in 2008, and sometimes enhance/complete them, this document is not deprived of novelty. The first new elements affect the ANSSI. Not only was it equipped with an "operations room" to cope with the threats but also, and it may be one of the major change explained here, it is to endow with a new mission: the defense of the information systems (ANSSI 2011b:15). Then, as far the legal perspective is concerned, there is a willingness to strengthen or enact legal rules in cyberspace, both at national and international levels, but also to promote "international judicial cooperation on repression of offences committed on or through electronic communication networks" (ANSSI 2011b:14). This also goes the other way around, as French authorities also plan on transposing EU law to the national law (ANSSI 2011b:18).

Finally, an emphasis is put on the necessity to work in cooperation with other stakeholders as "confrontations in cyberspace know no boundaries"(ANSSI 2011b:11). In that matter, we can identify three types of stakeholders: the public administration, the private sector and the individuals. For the ANSSI, it is crucial to protect the public administration. This entails a first step which is rather technical, namely monitoring the updates and security breaches in software to anticipate danger (ANSSI 2011b:15). The second step consists in promoting safe and confidential way of communication in both administrations and public spheres (ANSSI 2011b:12). Two actions have been decided in that regard: the adoption of the General Security Framework (RGS)[21] (Légifrance 2010), which defines secured procedures to follow for safe communications in the administration, and the diffusion of good practices to individuals and companies (ANSSI 2011b:14).

[20] Understood as sensitive "diplomatic, economic, military, technical and scientific information" (ANSSI 2011a:12).
[21] From that moment on, all documents were put online and can be freely seen on the ANSSI's website.

In addition, two noteworthy actions can be mentioned about the cohesion between companies and French authorities. The first is the establishment of a public-private-partnership (PPP) to share state's expertise on threats analysis against new technologies, and protection from the private sector (ANSSI 2011b:17). The second is the strengthening of the industry sector, still in the field of information systems, using state resources, particularly through strategic investment funds. A last element mentioned was a project of a cyberdefence research center in collaboration with industrial partners.

While much of the strategic document is focused on the public and the private sectors, citizens are not in the least put aside. Indeed, if France hopes to solve the future challenges, it must prepare and trains its citizens accordingly. It is therefore fundamental "to ensure that the field of information systems security remains attractive for young graduates to prevent the gradual erosion of our expertise" and allow the expansion of "the pool of expertise available in the country" (ANSSI 2011b:12–16). To ensure this, it is necessary to " raise citizens' awareness of cybersecurity issues during the education process"(ANSSI 2011b:14).

Last but not least, this document stresses the importance for France to "strengthen its operational partnerships with its closest allies" and "share "essential data with foreign partners" (ANSSI 2011b:11–16).

It is interesting to see how the technical approach of the first white paper in 2008 was carried out by the ANSSI with this document, especially towards the private sector. Indeed, French authorities quickly understood that cyberspace was encompassing so many infrastructures, owned by both by public and private actors, and that progress and better protection of cyberspace would only be attained by working hand in hand with all the stakeholders. This inclusion, as we have seen, also affects individuals and future generations through education.

What is more, we quickly mentioned the research sector and cybersecurity. It turns out that an initiative was undertaken by various researchers and tacticians from the High Council for Strategic Education and Research (CSFRS)(Suchier et al. 2011). After the Defense and Security of the Information systems strategy paper of 2011, they quickly assessed the state of the French cyber-capabilities.

- *Report of the scientific council of the CSFRS – 2011*

Their findings showed numerous elements. The paper starts with the observation that France needs a comprehensive national cyberstrategy. Therefore, it must improve or reform his vision at three levels: the security, human resources and legal levels. For the first level, the main priority is to secure vital infrastructures and systems by designing "systems and protocols" specifically for them in order to improve their resilience (Suchier et al. 2011:48). The scientists continue advising to create a national observatory for cybersecurity:

> *whose mission will be to verify the implementation of security recommendations, to assess the cyber security level of society, to report major incidents, to give recommendations to public and private operators, and to make public the test results concerning the most critical system* (Suchier et al. 2011:48–49). [22]

This is congruent with the national network of observatories mentioned in the 2008 white paper. The other recommendation is the creation of a "national methodology for the evaluation of the security of information systems based on an internationally recognized standard" [23] (Suchier et al. 2011:48–49). The last security recommendation is to perform national cybersecurity exercises (Suchier et al. 2011:49).

Furthermore, the second level entails changing the way education and training are conceived. This encompasses a set of measures, namely creating a proper human resources branch, also reshaping the training of instructors; favoring a learning process focusing on single themes and adopting a transversal approach of the security problematics and build a common core of security knowledges (Suchier et al. 2011:49–52).

Finally, three recommendations can be uttered for the last level. First, loosening the legal framework for the researchers would not only allow them to carry out their research in better conditions, but would also attract candidates and talents from abroad. Second, France must continue to adopt an approach to security based on anticipation, as it has proven useful up to 2011. Yet, this condition can only be met if France and the different jurisdictions cooperate even more closely (Suchier et al. 2011:50–51).

If prima facie the CSFRS does not seem to only represent the state as we have seen in its presentation above, it was created to help the state provide it with answers to strategic

[22] as translated in Baumard (2017: 58).
[23] as translated in Baumard (2017: 58).

challenges. Therefore, not only does it play a substantial role in the conception of the national cyberstrategy, it will influence or inspire the main securitizing actor, that is the state. Thus, analyzing this paper within the framework of securitization seems relevant. It is thought-provoking to notice that the same month this report was released, a general officer for cyberdefence was appointed by the Department of Defense (Légifrance 2011).

- *Report Bockel – 2012*

Following these two documents, just like Lasbordes or Romani before, a new report was issued by the Senate (Bockel 2012). Again, this report provides a snapshot of the French situation in terms of cyberdefence which is not really positive. To better understand why such a stance is reflected in this report, we must take into account the fact that French infrastructures and political personalities had been attacked between 2011 and 2012, as the G20 summit was being held in Paris (Hollinger 2011). Therefore, this motivated senator Bockel, heading the Committee on foreign affairs, defense and armed forces, to launch a special inquiry on cyberdefence (Baumard 2017:60).

Ten priorities emerged from this report. We can mention an emphasis put on the ANSSI and the vital infrastructures. The first priority is to make cyberdefence and the protection of information systems a national priority. Numerous priorities are focused on the ANSSI, its organization and its role. In other words, the senator emphasizes the need to increase its workforce and its budget, and to amend the legal framework to give ANSSI more leeway in the exercise of its mission. Furthermore, it is also put forward that critical infrastructures and companies should report any attack to the ANSSI. Another set of priorities is dedicated to the companies and the researchers, which should embark on the cybersecurity field. Lastly, the senator stresses the importance of collaborating at bilateral and multilateral levels (Bockel 2012:5).

As was the case for the reports mentioned above (Lasbordes 2006; Romani 2007), the aim here was to raise the attention of the state, especially as the a new white paper as well as a the so called Military Programming Law (LPM) of 2014-2019, that is an official law planning the military expenses for the five following years (Légifrance 2013), were on track to be adopted.

- *French White Paper on Defence and National Security – 2013*

The response to the Bockel's report came one year later. At first glance, we notice a general change in the tone of the white paper. Indeed, this corresponds to a change of presidency, Nicolas Sarkozy to Francois Hollande, marked by a greater emphasis on Europe. From a practical point of view, we can point to numerous elements relevant for us in this white paper: the paradoxical view of international relations implied by France, its view on cybersecurity, threats and the national sovereignty; and eventually its previsions for the field of defense and cybersecurity.

First of all, French discourse leads the reader to believe in a different way it conceives its international relations, which seems to be a dual view. On one side, there are the European partners with whom France has developed neighbor relationships, and the NATO alliance which military command structures France has reintegrated in 2009 (DGRIS 2013:60). For the former partners, relationships are not even based on a "balance of powers" rationale anymore (DGRIS 2013:33). On the other side, it is not said that what is valid for European states is also valid for other nations. In other words, we should not rule out the idea that France may be still pursuing this balance of powers reasoning at a global level. Moreover, the peculiarity of the EU situation is confirmed a few lines further: "peace is often still underpinned by the balance of power between nations, and the European situation is exceptional in this respect"(DGRIS 2013:33). This conception of the international relations, or at least the way to describe them, remains anchored in realist terms.

Then, territorial integrity, protection of its citizens, continuity of the nation's major vital functions as well as improved resilience remain the priorities of France (DGRIS 2013:74). That does not necessarily mean that the protection of its "information systems" does not count as such, on the contrary, it should be seen as a sub-priority belonging to this set of priorities (DGRIS 2013:100). Still, France's vision of priorities stays rooted in the traditional realist components.

Similarly, it is highlighted that "sovereignty and international legitimacy are two essential and complementary pillars of strategy for defence and national security" (DGRIS 2013:19). However, when looking at the component of the national sovereignty, two surprising capacities are mentioned: (1) "to detect and protect ourselves against cyber-attacks and to identify those responsible for them" and (2) "to produce security systems, on a fully autonomous basis,

notably in the fields of cryptology and attack detection" (DGRIS 2013:100). This is the first proof that cyberspace components have a direct impact on national sovereignty. Actually, we will notice preserving its sovereignty is one of the main goals put forward by the 2013 white paper (DGRIS 2013:125).

What does it imply for the conception of danger and threat? The 2013 white paper comes back at numerous moments on the previsions made in 2008 and confirms they were right (Mallet, France, and France 2008; DGRIS 2013), indicating that information systems are "a new source of vulnerability", because our overreliance on such systems increases our weak spots but also given that cyberattacks are cheap to conduct (DGRIS 2013:43).

As far as cybersecurity and cyberdefence are concerned, the white paper mentions that some nations are currently dedicated to the development of "offensive IT capabilities that already pose a direct threat to essential institutions, companies and sectors for the Nations' life" (DGRIS 2013:37). Indeed, the French authorities argue cyberspace has become an "area of confrontation" (DGRIS 2013:43) and "the new importance of cyber-threats calls for developing our intelligence activity [identification] and the corresponding technical expertise in this area" (DGRIS 2013:71). Thus, a lot must be done to protect the information systems. French tacticians explain that the fight against cyber-threats entails "maintain[ing] the protection and defence capabilities" (DGRIS 2013:100) but also "offensive action capabilities"(DGRIS 2013:71). This means a "very substantial increase in the level of security and the means to defend [our] information systems", as well as a reinforcement of the human resources to catch up with Germany and the United Kingdom (DGRIS 2013:100). Finally, an instrumental element is the addition of cyberdefence to the national priorities and its incorporation within the armed forces (DGRIS 2013:89).

Nevertheless, as mentioned above, France is aware that to better protect its national territory, it also has to act on the international stage. Therefore, actions within the Europe Union and the North Atlantic space are important to achieve a common security framework (DGRIS 2013:51). In that regard, France aspires to "build[ing] a European approach in internal security" (DGRIS 2013:65). Indeed, threats of espionage or sabotage compel Europe to think about protecting "its vital infrastructure and its industrial, scientific and technical potential against attacks or cyberattacks"(DGRIS 2013:52).

All these ambitions have led to the implementation of concrete actions. First, the 2013 white paper provided for the creation of a cyber-defense unit, a sort of cyber military civil (RCC) within the operational reserve and under the supervision of the Ministry of Defence. The latter's aim is "to enhance cyber-defence capacity in the event of a major IT attack". (DGRIS 2013:114). Then, in the public-private field, the SGDSN has been tasked with "the establishment of a general, inter-ministerial contract defining the civilian capacities required for missions relative to national security" (DGRIS 2013:106) and the development of awareness-building policy. Those are "directed at decentralized state administrations, regional authorities and their public establishments and at the principal users of the cyberspace" (DGRIS 2013:101). Finally, the most detailed initiative is anchored in the technico-legal field, it is the national response policy in case of cyber-attacks. Based on a global approach, it consists of two complementary components:

> *the implementation of a robust and resilient posture to protect state information systems, operators of essential infrastructure and strategic industries, paired with an operational organisation to defend these systems, coordinated by the office of the Prime Minister and supported by close cooperation of the different state agencies, to identify and qualify as early as possible any threats to which our country is exposed*

and

> *a capacity for a global and appropriate governmental approach to attacks of varied nature and magnitude, relying initially on all diplomatic, judicial or police resources, but without ruling out progressive use of Ministry of Defence resources in the event that national strategic interests are threatened.* (DGRIS 2013:100)

More passive than the 2008 white paper, the 2013 looks more like a review white paper. If we take the context into account, this release occurred after the hardest years following the 2007 economic crisis and caution seems to be the guiding principle. Indeed, directly at the beginning of the white paper, we can read warnings on the "risks to our [French] economic dependence" and the need to find a balance between French priorities so that "defense and security arrangements are consistent with the need for fiscal consolidation" (DGRIS 2013:9). In addition to the vagueness, we can add that the few propositions are also blurrier than in 2008. Moreover, intervention, both at the domestic level and abroad, as well as nuclear deterrence seem to remain the top defense mechanisms to protect the national interest (DGRIS 2013). This whole overview begs the following questions: is it part of the French strategy not to display all its cards in order to keep a strategic advantage or does it suggest a lack of leadership and a follow-the-leader attitude (the USA through NATO in this regard)? It is hard to answer to such questions but necessary to put the French discourse into question.

- *Pact on Cyberdefence – 2014*

Following the release of the 2013 white paper, former Defence Minister Jean-Yves Le Drian commissioned the drafting of the so-called Cyberdefence Pact (Ministry of Armed Forces 2014). Drawing upon six main axis, it establishes fifty actions to undertake in order to improve the French cyberdefence. These axis are the following: (1) reinforcing the security level of the information systems as well as the defence and intervention assets of the Ministry and its major trusted partners; (2) preparing the future through an intensification of the research efforts in the technical, academic and operational domains, while supporting our industrial basis; (3) reinforcing the manpower dedicated to cyber defence and developing the associated career paths; (4) developing the cyber defence centre in Brittany for the Ministry of Defence and the national cyber defence community; (5) keeping up a network of foreign partners, in Europe, within the Atlantic Alliance or in areas of strategic interest; and lastly (6) furthering the emergence of a national cyber defence community, relying on a group of partners and on the reserve's networks (Ministry of Armed Forces 2014).

Overall, the intentions displayed by Jean-Yves Le Drian are congruent with the approach embraced so far by French authorities. On the cyber offensive-defensive field, the main decisions are about improving the defensive stance and reorganizing the cyberdefence through the Director of the Defence Information and Communication Systems (DGSIC); strengthening the responsive stance by improving the operational cyberdefence capacities of the Planning and Operations Centre (CPCO) created in 2011, and spreading them through all the components of the Ministry; developing a new range of cybersecurity tools, both hardware and software, improving cyberdefence of the armed force; fostering research activities and creation of a center of excellence in Brittany; deepening the partnerships with our main allies and playing an active role within international arenas (UE, NATO) to improve our collective security; and finally developing the exchange between the cyberdefence community and the national services and foster the cyberdefence spirit between the army, the ANSSI, the DGA and the operational reserve (Ministry of Defence 2014).

Then, as far the technical side is concerned, there is a will to strengthen of the technical expertise (knowledge sharing, crisis management training) of the Brittany excellence center drawing upon the Information Assurance Division of the DGA (DGA-MI), by building on the

local branch of the Analysis Centre for Cyber Defensive Operations (CALID)[24]. In the end, the ultimate goal is to diffuse this know-how and knowledge across the services. Another element which is essential for French authorities is developing legal expertise in the cyberdefence field to give armed forces a solid legal framework (Ministry of Defence 2014).[25]

Lastly, a section of the Cyberdefence Pact includes a crucial actor, the private sector. Indeed, a twofold action is provided in that regard. One the one hand, the government calls for supporting small and medium enterprises (SMEs) through the job creation program, set in motion by the Defence Procurement Agency (DGA), so-called RAPID, which aims at combining job creation and innovation. On the other hand, it insists on the need for the ANSSI to keep on assisting the largest defense industries in the events of cyber-attacks (Ministry of Defence 2014).

While the Cyberdefence Pact is not referred to as a strategy document as such, it does help us to grasp the strategic thought of the French government.

- *French National Digital Security Strategy - 2015*

Released against the backdrop of a series of cyberattacks (defacement of administration's websites, disruption of the French television channel TV5 Monde[26]), this document has its main focus on the digitalization of society and the underlying effect of this phenomenon. (ANSSI 2015:7). The ANSSI puts forward five aims the French state has to reach in order to protect its cyberspace (ANSSI 2015:9).

The primary aim, and most relevant for our study, is " to ensure France's freedom of expression and action as well as the security of its critical infrastructures in case of a major cyberattack" (ANSSI 2015:9). As said above, France and its fundamental interests have been attacked and critical infrastructures, intended as "operators of vital importance or strategic businesses", are the first to be threatened (ANSSI 2015:14). Therefore, the ANSSI is committed to get "the scientific, technical and industrial capabilities required to protect sovereign information, ensure cybersecurity and develop a trustworthy digital economy" (ANSSI 2015:14). This notably implies the creation of an expert panel for digital trust placed under the supervision of the

[24] Cf. appendix 10 to see the location of the center.
[25] It is interesting to bear in mind that the first attempt to codify rules applying to cyber conflicts and cyber warfare occurred in 2013 with the publication of the first Tallinn Manual on the topic.
[26] Occurred on 9th April 2015, the attack shutdown the infrastructures of TV5 monde, which had to stop its broadcasting for a few hours. The attack was claimed by the Islamic state (Alonso, Luc Mathieu, and Guiton 2015).

ANSSI and the SGDSN. Furthermore, another action aiming at the pursuit of this first aim is the "active monitoring of the security of technologies and uses for the State, businesses and citizens", by adapting the legal framework to new technologies and warning to inform French authorities (ministries, businesses, and other territorial administrations) of potential risks or security breaches (ANSSI 2015:15). Furthermore, achieving such goal means pushing forward State Information Systems Security Policy, which was set in place around 2010, and which aim is to keep ensuring France's autonomy by providing new security mobile terminals or homemade software for instance (ANSSI 2015:17). Additionally, the ANSSI wants to prepare France and the multilateral organizations where it sits to face major cybersecurity crises (ANSSI 2015:17). This entails to extend the framework applied to operators of vital importance (OIV) to other operators - both public and private - participating in these sensitive information systems; to also extend cybersecurity crises management exercises over the national territory; to support the development of the cyber operational reserve; and support the work of the European agency ENISA (European Union Agency for Network and Information Security) (ANSSI 2015:17). On the whole, the ANSSI wants to elaborate an autonomous way of thinking that fits French values (ANSSI 2015:14–17).

The second aim of France for its national digital security strategy is to "protect the digital lives of citizens and businesses and combat cybercriminality" (ANSSI 2015:20–23). In that regard, while the ANSSI is " the identified State contact in case of serious cybersecurity incidents that affect the administrations and operators of vital importance, there is far less clarity regarding the public offer for assistance to victims of cybermalevolence for the other stakeholders" (ANSSI 2015:20). Moreover, the opinions that are spread on the internet go against "France's fundamental interests and are an attack on defence and national security" (ANSSI 2015:20). Thus, the aim in that matter for France is twofold. On the one hand, the French cyberspace must reflect its values while protecting the digital lives of its citizens. On the other hand, French authorities will tackle even more the issue cybercrime and provide proper assistance to victims of cybermalevolent[27] acts (ANSSI 2015:21).

To answer these challenges, the ANSSI provides an array of initiatives. First, the French state aims at "advocating and defending our [French] values on electronic communication networks and in international proceedings" by preserving a free and open cyberspace and informing citizens of the risks of manipulation and propaganda techniques they could encounter on the

[27] To Baumard, it is "identified as a broad target for a passive and dynamic defense, which includes both passive monitoring and active retaliation when 'France national interests are at stake'" (Baumard 2017:61).

internet (ANSSI 2015:21) and improving the operational mechanisms of legal international mutual aid and universalizing the principles of the Budapest Convention on Cybercrime (ANSSI 2015:23). Furthermore, should they be victims of cybermalevolent acts, they will be able to turn to a national system to get assistance as of 2016 (ANSSI 2015:21). The measures targeting the protection of digital lives, privacy and personal data of the French people go in the same direction. In this regard, there are two main actions, the implementation of the European regulation on electronic identification (eIDAS - Electronic Identifiation and Trust Services) and the reassertion of the right to privacy for individual and collective control of personal data (ANSSI 2015:22). Eventually, we come back to technical solutions and the promotion of the development of French solutions for both public and private sectors (ANSSI 2015:22).

The third aim of French authorities is to "ensure the education and training required for digital security" (ANSSI 2015:9). The basis of this goal lies on raising the awareness of all French citizens notably by creating an educational website (CyberEdu) managed by the ANSSI (ANSSI 2015:26). Over the next years, the French state will progressively integrate "cybersecurity awareness into all higher and continuing education programs" and "cybersecurity training into all higher education that includes some information technology" (SecNumedu) (ANSSI 2015:27; ANSSI 2018b). Also, this process entails a pro-active stance which involve "anticipating the initial and continuing education needs" of all actors, "in collaboration with all the stakeholders concerned in the administration and the private sector" (ANSSI 2015:26–27)

The fourth aim is to strive towards a digital friendly environment in which both public and private sectors trust the technologies (ANSSI 2015:9). Again, there is the idea that the technology used to protect French infrastructures be French and accessible to every actor. In more concrete terms, it means developing technologies, allowing for their transfer intra- and inter-service, but also diffuse the French know-how worldwide. It is interesting to note that France wants to "preserve its financial and industrial capacity to develop solutions with the highest levels of security" in order to protect "its sovereignty and notably the protection of its information concerning the national defence secret" (ANSSI 2015:30–34).

Last but not least, the fifth aim refers to the cooperation between states in different international organizations (UE, OSCE, UNO) and the pledge for an ever closer cooperation to achieve a European digital strategic autonomy (ANSSI 2015). An allusion to the multilateral cooperation

is done by mentioning the decision taken in 2013 by the states to acknowledge "cyberspace was governed by existing international law" (ANSSI 2015:38). Indeed, the observations from the past were confirmed and the trend is that more and more countries are equipped with offensive capabilities, which is a continuous threat for states. As a consequence, what France wants to achieve within the EU but also inside its own territory, is playing "an active role in the promotion of a safe, stable and open cyberspace" (ANSSI 2015:38). The direct effect will be to increase the place dedicated to the debate on new technologies and the securization of the cyberspace within the European fora (increase of the bilateral and multilateral exchanges) (ANSSI 2015:39–40).

With this strategy document, we notice a shift in the discourse. While the focus was put on a securitization of infrastructures, due to fears of a cyber interstate conflict in the previous white papers, the debate progressively moves towards the securitization of every infrastructure in the country and beyond, through multilateral organizations. The main reason may be the fact that the document was issued by the ANSSI, which mandate is not only to protect OIV but also lead the French private and public sector towards a self-awareness of the role they play in the protection of the French cyberspace. Another probable reason may be that French authorities have noticed that cyberwars were not on the doorsteps of France yet, and that they should rather focus on everyday life practices in the future rather than on potential comprehensive warfare scenarios.

- *Defence Minister Jean-Yves Le Drian speech - 12 december 2016*

This speech is not a strategic document per se, but marks a critical juncture in the French cyberstrategy. Indeed, former Defence Minister Jean-Yves Le Drian delivered a speech at the DGA-MI, center of excellence in Rennes (see Appendix 8), in which he declared the establishment of a cyber commandment called COMCYBER/CYBERCOM in order to "maintain France's sovereignty and stay master of its destiny" (free translation). This new component is a part of the Chief of the Defence Staff (CEMA) and is placed under the supervision of a commander responsible for all the military operations. Furthermore, the COMCYBER will work hand in hand with the head of ANSSI[28] for all the matters revolving around the protection of the vital infrastructures (such as the OIVs), the DGA delegate (SGA)[29] for all technical engineering and technological equipment procurement. His work will be

[28] Itself under the authority of the Prime Minister.
[29] Itself under the authority of the Defense Minister.

divided in 4 sections: networks protection; defense center integrating the Analysis Centre for Cyber Defensive Operations (CALID); attack and intelligence center equipped with attack teams; and a center dedicated to the (cyber) operational reserve (RCD)(Le Drian Jean-Yves 2016).

In addition to this announcement, Le Drian argues France needs a doctrine for its cyberfield and thus comes back on the missions that the army should carry in the field of cyberdefense. Indeed, he divides them into three categories: intelligence and investigation; protection and defense; and response and neutralization. In order to achieve these means, he wants to increase the global cyber workforce to 3200 in the different French services, which includes the number of participants to mission "cyber", the so-called cybercombatants, and to 4400 the people from the two reserves, namely the cyber military civil reserve and the operational reserve people (a complete graph summarizing all the figures given will be provided in the detailed analysis) (Le Drian Jean-Yves 2016).

Another interesting point is made about France's stance on what we could call "cyberdeterrence". To Le Drian, French tacticians only conceive deterrence as deriving from the nuclear power as no other power or weapon, cyber weapons included, is capable of deterring or could ever produce the effect of a nuclear bomb. Cyber weapons therefore fall into the category of conventional weapons. Overall, this set of actions is in Le Drian's words a way "to assert French interests in this new space of confrontation" (*translation ours*) (Le Drian Jean-Yves 2016).

- *Defence and National Security Strategic Review – 2017*

Far from being a game-changer document for French national cyberstrategy, the Defence and National Strategic Review does present a few features which are interesting to us. It was released by the Defence Communications and Information Delegation (DICOD), which is the same department that released the white papers we presented above. We therefore stay within the same framework. On the top of that, this release also occurred a couple months after President Emmanuel Macron came to office, who was the one commissioning the Minister for the Armed Forces to realize this review.

Overall, it is an assessment of the situation in the wake of the release of the Military Planning Act (LPM [30]) 2019-2025. Thus, a first point to be made is that the ever-increasing interdependency and interconnectedness have led to increased risks and vulnerabilities for countries, as the network plays the role of a multiplier effect turning small attacks into major systemic crisis (Ministry of Armed Forces 2017:20).

Additionally, this dissemination of attacks is facilitated by other factors such as the low cost it requires to launch them, but also by the lack of coordination and cohesion. Indeed, managing these attacks for states is always complicated as they sometimes expand "beyond the scope of defence" and may involve international cooperation (Ministry of Armed Forces 2017:33–34). Moreover, states bear an indirect responsibility, as their techniques and methods of cyber-attacks are mimicked by attackers who replicate these methods within states (Ministry of Armed Forces 2017:33).

Further in the document, the authors reassert the digital space as a domain of confrontation and put the emphasis on the growing role of private actors as "challengers to state sovereignty" that reshape "the balance of power between state, non-state, and private-sector actors" (Ministry of Armed Forces 2017:46). In this case, famous actors, giant of the internet, such as Facebook or Google are mentioned. However, what is particularly interesting is to see that the expansion of such private actors is linked to the assertion of power and sovereignty. The supremacy of the United States is even acknowledged "across all aspects of cyberspace (including hardware, technological and economic, legal, political, and military dimensions)" (Ministry of Armed Forces 2017:46). By reading such lines, one can wonder if France is not getting envious of such giants, and if his desire to develop his French tech's private sector is not purely economic but rather based on the will to increase its control on national sovereignty. Indeed, the authors even mentions the need "to protect our [France] sovereignty in the digital world" (Ministry of Armed Forces 2017:53)

Another part of the review deals with the reassertion of interests, especially redefining and while broadening their definition. In that regard, we should specify that the interests and priorities are not carved in stone, and that it is the duty of the President to set them through time (Ministry of Armed Forces 2017:53–54). For once, there is a direct, although vague, attempt to define France's interests, namely as "all factors that contribute to its security, prosperity, and

[30] We did not include the earlier Military Planning Act, namely 2014-2019, because they are the preparatory works preceding the white papers.

influence" (Ministry of Armed Forces 2017:52). They add that interests have been primarily addressed in terms of vital interests, themselves never really defined, and that the integrity of the territory and the protection of the population are central to the vital interests (Ministry of Armed Forces 2017:52). On top of that, "vital interests cannot be restricted to the national scope, because France does not conceive its defence strategy in isolation, even in the nuclear field" (Ministry of Armed Forces 2017:52).

Thus, interests should be constantly adapted to the context. A good example of this is the way domestic interests are intertwined with European or global ones as the world is more and more internet connected (Ministry of Armed Forces 2017:53). In this way, from now on we should not only conceive national interests as a sole category but as encompassing both traditional interests (territory and population lives) and shared interests, which themselves would be divided in different categories, such as European interests and global interests (Ministry of Armed Forces 2017).

Nonetheless, it must be said that the preservation of the national interests remains based the nuclear deterrence, both airborne and maritime (Ministry of Armed Forces 2017:6), and that France's ultimate goal is to reach a stage of strategic autonomy by 2030 (Ministry of Armed Forces 2017:51).

- *Military Programming Law (LPM) 2019-2025 – 2018*

This LPM was presented at the beginning of February 2018 and was divided into two documents, the main draft bill and its appendix, but also into four pillars.

While the first pillar aims at improving the conditions of soldiers, both material and immaterial, the second pillar targets the modernization of weapons and equipment. However, what interests us here are the legal and institutional changes that come alongside them as they reshape the French cyberstrategy. The legal status of cyberdefense is defined by the Code of Defense, especially the articles L2321-1 and following. And with the LPM, it is completed giving a reinforced role for the ANSSI in matter of competencies (Ministère de la Défense 2018a:11). Indeed, in order to pursue the development of "cyber" resilience, the ANSSI is authorized by the state to ask electronic communications operators to examine evidence of computer attacks; to compel the aforesaid operators to warn their subscribers or users of potential breaches; to investigate and ask the operators for access to their data when OIV or public administration

networks are threatened; and to access to technical data only gathered by the detection systems of the operators; to set up detection mechanisms directly at the host website or on the electronic communications operator's networks when a potential threat against OIV or public administration networks is known; again, this only concerns technical data[31]. In addition to these new powers, according to the art 20 of the LPM, the government is empowered to change the aforementioned modalities, but this is not all. Indeed, the following article 21 entails a very powerful clause, which state that actions occurring within the digital framework do not engage the criminal accountability of the military personnel. Such a disposition can make us wonder if this does not pave the way for cyberwar. Also, article 22 states that the DGA is entitled to approve the compliance of new military transmitter for intelligence purposes and also to test them and make them approved by the Commission for the Control of Intelligence Techniques (CNCTR)(Ministère de la Défense 2018a:15).

The third pillar tackles the assertion of the French strategic autonomy (Ministère de la Défense 2018a:48–53). Even though France still relies a lot on nuclear deterrence to ensure its vital interests, the information systems on which vital infrastructures rely are not completely shielded from cyberattacks (Ministère de la Défense 2018a:12). But having a strategic autonomy also means mastering the attack. In order to act in the new confrontation spaces, spatial or cyber components are needed (Ministère de la Défense 2018b:52). Thus, the development of the cyber as an integral component is on the way. For instance, in case of crisis, France will be able to deploy Military staff including cyber combatants as part of the Chief of Defence Staff (CEMA) but also as an integral component (Ministère de la Défense 2018a:16). Actually, the CEMA has undertaken a redefinition of the expectations linked to jobs to increase their appeal and jobs requiring computer skills are among them (Ministère de la Défense 2018a:28–29). That being said, the CEMA wants to add 1500 more cybercombatants to its cyberworkforce between 2019 and 2025 to reach 4000 people by 2025 (see graph and table in Appendix 12), especially within the CALID and the specialized units gathered on the Rennes' center (Ministère de la Défense 2018a:31).

Furthermore, because cyberdefense is seen as a transversal tool covering all other strategic function, it is de facto a cornerstone for the preservation of French national sovereignty (Ministère de la Défense 2018b:52). Therefore, protecting weapons and information systems is instrumental from their creation to their use. In this regard, France will adopt a so-called

[31] Data collected within this framework can be kept up to 5 years (Ministère de la Défense 2018:31)

permanent cyber stance (PPC) revolved around networks monitoring both offensive and defensive computer warfare (Ministère de la Défense 2018b:51–52).

The fourth pillar of this LPM is innovation and investment. Its aim is to provide more means, improve the tools and to include every ministry. Nonetheless, a very important of this pillar is to participate to new technological breakthroughs that can directly impact the operational field, cyber included. (Ministère de la Défense 2018a:54). To that end, 1.600 billion euros will be dedicated to cyberspace defense and development during the period covered by the LPM and globally France's aim for the future is to raise its defense spending/military expenditures to up to 2% of its GDP. As with the previous LPM, expenses will be reviewed and updated at the halfway mark that is 2021 (Ministère de la Défense 2018b:59).

On the whole, not only does this LPM improve the military material, it will also have a positive impact on the French economy as it will create new jobs (Ministère de la Défense 2018a:56). For the cyberfield, we must keep in mind the reinforced role of ANSSI and the increase in French cyberworkforce.

- *Strategic review of cyber defence – 2018*

The last document shares a lot with the LPM presented above (Ministère de la Défense 2018a:52). The LPM was still undergoing some amendments after the 2018 strategic review was published, which is why some of the actions are to be found in the two documents, which provides them with even more weight and legitimacy.

The 2018 review is split into three parts. In the first part, the emphasis is put on the cyber threats, which are presented as having far-reaching consequences, both in terms of scale and scope (SGDSN 2018:4–5). In the second part, there are two subsections. The first subsection reasserts the role of the state as the actor in charge of cyberdefence. In this regard, a special focus is put on the organization of French cyberdefence, which contrary to Anglo-Saxon countries has split the offensive and the defensive parts of its capabilities (SGDSN 2018:5). This has two direct consequences. First, the five strategic functions as defined in the 2008 White Paper, namely knowledge and anticipation, deterrence, protection, prevention and intervention are transformed into six categories "prevention, anticipation, protection, detection, attribution and reaction" (SGDSN 2018:5). Second, the cyberdefence mission is reorganized into four operational chains: the protection (in the hands of the SGDSN and the ANSSI), the military

(under the supervision of the President of the Republic), the intelligence (acting on government's orders) and the judicial (including actions of the police, gendarmerie (police outside the cities) and justice services) (SGDSN 2018:5–6). Coupled to this reorganization, two new mechanisms are created: the Cyber Defence Management Committee and the Cyber Defence Steering Committee. The former will monitor the implementation of policies related to the cyberfield while the latter will do the preparatory work (SGDSN 2018:6). Furthermore, in order to improve the reach of the government, the 2018 strategic review advises the creation of a Cyber Crisis Coordination Centre (C4), gathering all stakeholders to better contain and manage small to medium scales crises (SGDSN 2018:6).

The second subsection is dedicated to the improvement of the nation's cyberdefence, especially the strengthening of the protection of the systems (SGDSN 2018:5–9). This protection not only includes the state systems and the critical infrastructures, but also the electronic communications operators and web hosts infrastructures. To this end, the government calls for more regulations and protections because of the overwhelming importance of both electronic communications and electricity supply sectors in our daily life. It even suggests starting transposing the European directive (EU) 2016/1148 or so-called Networks and Information Systems (NIS) directive[32], adopted by the European Parliament on 6 July 2016 and entered into force in August 2016 (EUR-LEX 2016). This directive aims at setting common standards among member states in terms of security of network and information systems (The European Commission 2018). In addition to these legal measures comes a series of changes in terms of competencies, especially for the ANSSI. Indeed, with this 2018 strategic review the ANSSI is endowed with a twofold prerogative. On the one hand, the ANSSI will have the possibility to "implement detection systems in their networks to detect cyberattacks targeting their subscribers", which are detection markers (SGDSN 2018:7). On the other hand, should it detect a potential threat on the network, the ANSSI is entitled "to set up a local detection device on a web host's server or on the equipment of an electronic communications operator under the control of an attacker" (SGDSN 2018:7). It has to be said that this plan will be overseen by the "the French regulatory authority for electronic and postal communications", the so called ARCEP (SGDSN 2018:7). Lastly, the 2018 strategic review entails the creation of regional cybersecurity hubs, where an ANSSI representative will be appointed in order to diffuse ANSSI good practices and know-how, but also to better account for the difficulties within French regions (SGDSN 2018:7–8).

[32] "Member States have to transpose the Directive into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018" (The European Commission 2018).

On another note, a part of the 2018 review is dedicated to France and its action on the international stage. As it was always the case in the previous strategic documents, French authorities still support the idea of maintaining good relationships with their allies and partners and the review calls for the establishment of a doctrine of action. This doctrine should include both national and international legal standards so that it constitutes a tool for France and the international community. Additionally, this doctrine will follow the French "interpretation of the existing internal law to cyberspace" (SGDSN 2018:8). To achieve such standards and actions, France has committed to abide by three principles, namely prevention (intended as preventive actions because of the difficulty of attribution), cooperation (as good relationships and common practices are instrumental to succeed) and stability (including a kind of reciprocity right in case of an attack) (SGDSN 2018:8–9). Nonetheless, France is aware that actions must also come from the private sector. Thus, it set priority actions for these actors, including "greater control of offensive action by the private sector in cyberspace"; "export control for attack tools"; and "corporate responsibility in designing and maintaining digital products" (SGDSN 2018:9). Eventually, the review encourages France to suggest the creation of a European think tank dedicated to cyber defence issues (SGDSN 2018:9).

In the third part, we come back to the state and its role as "guarantor of cybersecurity" (SGDSN 2018:10). A first crucial element for us is the use and the definition of the [French] digital sovereignty as something that:

> *can be described as the ability of France to retain in the digital space the autonomous ability of appreciation, decision and action, as well as to preserve the most traditional elements of its sovereignty in the face of the new threats that exploit the increasing digitalisation of society* (SGDSN 2018:10).

Thus, the digital sovereignty appears as a means to preserve the traditional sovereignty. Moreover, some technologies are designated as essential to maintain French digital sovereignty, twhich is the case for "encryption of communications, detection of cyberattacks and professional mobile radios" but also for "mastering artificial intelligence" and cloud-computing (SGDSN 2018:10). In this regard, the French state also supports the establishment of a comprehensive policy on the use of the cloud but also on the promotion of ANSSI certified cloud solution providers (SGDSN 2018:10). As we said above, the State is the guarantor of cybersecurity in society, but the government should also act as such and help in setting up a "cross-sectoral approach" that is to "guarantee a minimum level of cybersecurity for the most critical entities, in order to protect France's fundamental interests in face of the cyber threat"

(SGDSN 2018:11). To achieve this, France should include all sectoral actors and help them to implement this cross-sectoral approach.

Another point in the third part consists in improving "the certification framework in order to improve product security", both at the domestic and European levels (SGDSN 2018:11–12). There are increasingly more connected objects around us and a basic security requirement is needed. The cyber package presented in September 2017 goes in this direction, as it was aiming to harmonize the security certification across the Union. Moreover, the review emphasizes the need to build up the industries related to cybersecurity. One of the actions here is the creation of start-ups, which would be helped to grow and strive in order to develop them into "champions of cyber-security" (SGDSN 2018:12). However, increasing the number of companies also increases the risks they carry. This is why the review also proposes to develop a cyber rating offer, as some companies would be handling more sensitive data than others, and should therefore comply with certain extra rules (SGDSN 2018:13). By the same token, even if insurances for cyber risks already exist, the review suggests the creation a European database of the cyber incidents as well as of the costs they entail, in order to better account for this new phenomenon (SGDSN 2018:13).

Eventually, the last topic tackled by this review is closely linked to citizens. The 2018 strategic review strives to develop a more pedagogical approach in the process of transmitting knowledge. This initiative entails raising the awareness of the young generation as well as their teachers through the implementation of trainings inside their curricula or even create a smartphone application to check the knowledges of the people and teach them good practices, should they need it (SGDSN 2018:13–14). Furthermore, a last point is dedicated to the skills management. Basically, it refers to the management of the human resources, who are skilled in digital security or who intend to begin a training in this field. Thus, the state is advised to carry on with the *CyberEdu* initiative, which is an online platform that unites all the people from the sector and the future cyber professionals and develop higher education courses for people not following computer sciences study. Also, another proposal made in this review is for the ANSSI to create accrediting digital training, for the state to ensure that people having acquired cyber skills can easily optimize their use during their career, and finally, create structures to pool cyber capabilities in general (through regional coordination structures for instance) (SGDSN 2018:14).

From this review, we can infer that the French cyberstrategy is moving from a purely centralized organization towards a more inclusive and decentralized system. Furthermore, the role of the ANSSI is reinforced giving it the power to ensure which products is adequate and which is not, through the certification of security solutions. Overall, the French state spur these actors not only to use the available security services but also to:

> *place a priority on protecting our information systems; adopt an active stance of attack deterrence and coordinated response; fully exercise our digital sovereignty; provide an effective penal response to cybercrime; promote a shared culture of information security; help bring about a digital Europe that is safe and reliable; act internationally in favour of a collective and controlled governance of cyberspace* (SGDSN 2018:3).

Without going into details, we suggest our first observations on what the dominant cyberdoctrine should be per text, based on the decisions we listed in the framework (appendix 13).

Table 6 *Observations from the first step*

	Document	Leaning towards the cyberdoctrine
1.	2008 – White Paper	Power-sovereign (III)
2.	2011 – Information System Defence and Security	Societal (I)
3.	2013 – White Paper	Technocrat (II)
4.	2014 - Cyberdefence Pact	Power-sovereign (III)
5.	2015 - National Digital Security Strategy	Power-sovereign (III)/ Societal (I)
6.	2016 - Le Drian's speech	Power-sovereign (III)
7.	2017 - Defence and National Security Strategic Review	Power-sovereign (III)
8.	2018 - Strategic Review of Cyber Defence	Societal (I)/ Power-sovereign (III)

Note: Elaborated by our care.

On the long-run, the dominant French cyberdoctrine and strategy seem to point to the third type, namely Power-sovereign. As a reminder, countries fitting to the type Societal (I), Technocrat (II), and Power sovereign (III) should respectively lean towards a cyberdiscourse of type (I) every day security pratices, (II) technification and (III) hypersecuritization. Through the lexicometry analysis, we will see if in our case, France does adopt an hypersecuritization cyberdiscourse.

4.1.1.2. *Second step (Lexicometry)*

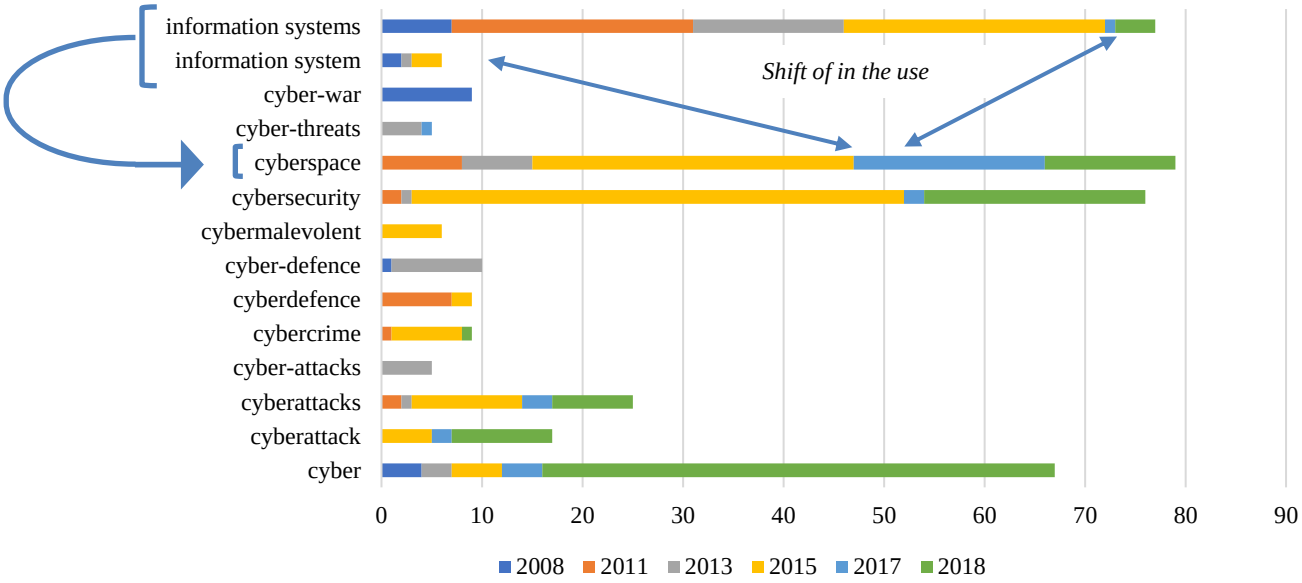
We have seen the complete picture of France's cyberstrategy from a chronological and rather descriptive way. We will now use the lexicometry software TXM and our codebook

to quantify the proportion of each cyberdiscourse. The first descriptive step helped us find new words that could be useful to analyze (see appendix 14 for the updated list). Within this list, some symbols have been used "(s)" when both singular and plural forms were put together, "(-)" when both written forms (for instance cyber-attack and cyberattack without hyphen) were merged, and "/" to indicate the first word remains the same for the combination (for instance "public sector", public administration" ect). Moreover, numerous words from the first codebook have been deleted or replaced because they were either inappropriate (e.g.: global issue), or no longer used (e.g: user-end).

Before moving on to the lexicometry analysis, it should be noted that the terminology surrounding cyberspace is new and is still changing at the time we are writing this research. In addition to that, the USA have the supremacy on the cyberspace terminology for three reasons. First, English has been the lingua franca in the international relations for a century and for the sake of comprehension, people tend to adopt and borrow concepts from the English language. Second, their supremacy is not only linked to their language, but also to the new technologies that stem from their industry and they are, de facto the first users of new technologies. Third, to remain the global actor in cyberspace, the USA can count on its flagship regional organization, the NATO, to diffuse its vision and concepts, impacting consequently both policies making and cyberdiscourse. Still, in the different documents we selected from the French cyberstrategy (we kept 6 out 8 texts - list available in the appendix 13), some words have been supplanted by others while some have gained importance throughout the decade.

In this regard, it is very interesting to look at the evolution of the words linked to the cyber dimension. Indeed, while some words like "information system" seem on the verge of decrease in their use, others have not succeeded in taking roots (cybermalevolent) or converge towards a common form without hyphen (cyberattack(s), cyberdefence, cybersecurity). In any case, the prefix cyber- will continue to provide new concepts to describe the reality we are facing. If we look at the Figure 10 below, we can have an overview of this evolution and see how some concepts reflect France's preoccupations (notably cyberspace, cybersecurity and cyberattacks).

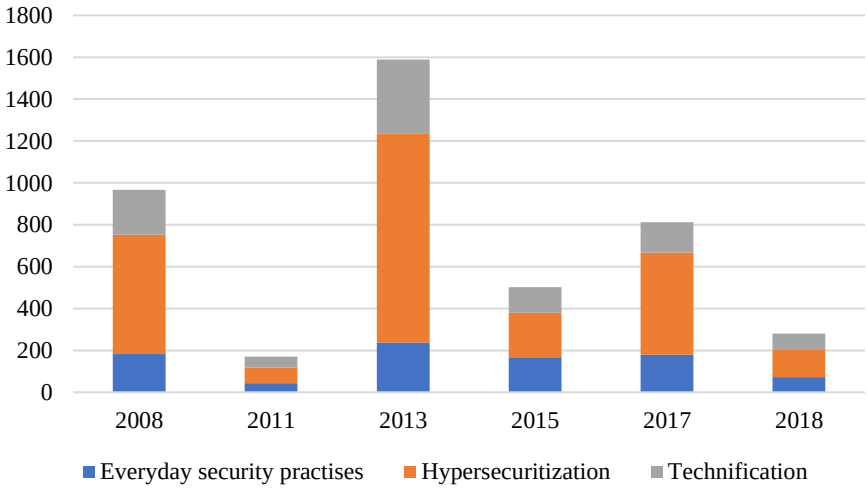
Figure 10 *Use of the cyberwords through time (in words) - France*



Note: made from the extraction of data through the software TXM, please refer to appendix 16 to consult the data used.

From the words we collected for cyberdiscourse types, we established a graph of the evolution of the most used cyberdiscourse per year, throughout the decade 2008-2018.

Figure 11 *Cyberdiscourse use between 2008-2018 (by type and words) - France*



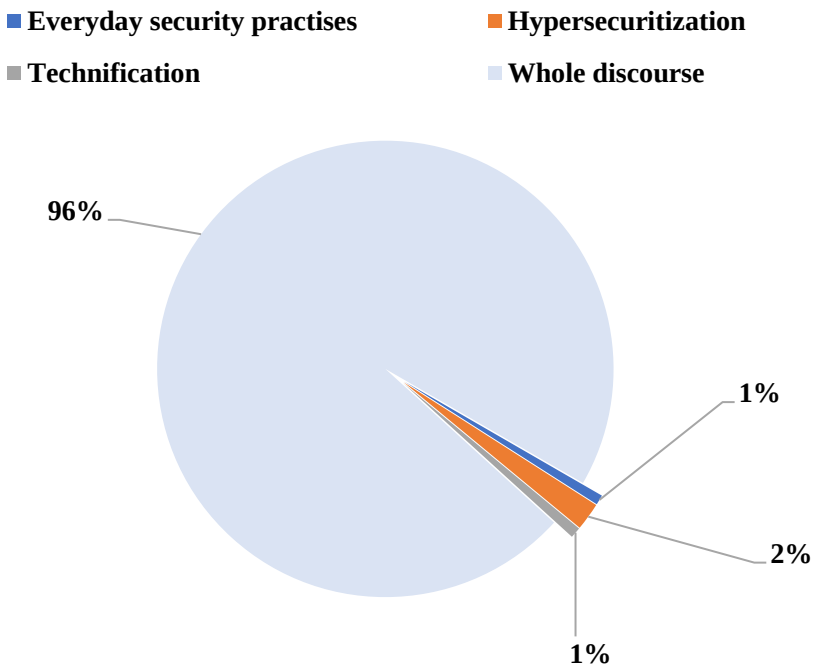
Note: made from the extraction of data through the software TXM, please refer to appendix 17 to consult the data used.

This graph suggests that not only is France's cyberdiscourse leaning towards hypersecuritization, it has also been the same type for the past decade. If we compare with what was suggested above, we see that for the years 2011, 2015, 2017 and 2018, our observations were correct. Yet, for the documents of 2011 and 2013, there is a discrepancy between what we

induced from the content we analyzed, and the cyberdiscourse that was really used. Even if the disparity is small for some years, the appendix 17 shows us the amount of words used, and confirms this finding.

Moreover, in the introduction, we mentioned we wanted to explore this phenomenon that is cyberstrategy but also to try to distinguish a pattern of decisions. Even if we only have two cases for the study, we will try to head in this direction. Thus, we decided to make an average use for the decade in order to see what the place of the cyberdiscourse within the discourse of France on defense and security were. That being said, on the next graph we can see that hypersecuritization remains the most used cyberdiscourse, which is logical as it was the dominant cyberdiscourse over the decade. As such, this does not bring a lot more to the analysis, but maybe the case of Italy will be different and allow for a comparison.

Figure 12 *Cyberdiscourse type average between 2008-2018*



Note: made from the selected words for each cyberdiscourse and applying an average (in respect to whole discourse), please refer to appendix 17 to consult the data used.

Again, the cyberdiscourse of hypersecuritization type remains the most used in respect to the two others. Eventually, we tried through TXM to bring some sense to the data related to the national interest. Displaying tables with the iterations of the word interest(s) would show us its use through time but would not be relevant alone. Therefore, we chose to look up combinations of words that would be of interest.

Using TXM, we elaborated a series of concordance tables, that is, using a query in the software, we looked for combinations of selected words in context, and keeping a determined number of words on the left and on the right of the selected group of words. After a few different queries, we obtained some interesting results. The first query was the word "interest(s) with the following words (+ France/France's/fundamental/protects). This allowed us to obtain a correlation between the interests and cyberspace (see appendix 18). Indeed, the idea that comes up from that query is that cyberattacks damage French fundamental interests; opinions disseminated on the networks are an attack on defense and national security; and France will defend its fundamental interests against major cyber-threat. The second interesting query about interests is the association between "protects" and "interests". Indeed, it show us that even if ICTs have gained high salience our lives, the state still thinks the nuclear deterrence is the sole tool enabling them to protect its interests (see appendix 19). Eventually, as we said above, before using "cyberspace", France used to talk about "information system(s)". It appeared that combining "protect" and "information system(s)" was useful, as it turned out that "protect the state information systems" was used from 2008 to 2015 to indicate the securitization of what we now encompass as cyberspace (appendix 20). Arrows have been added on the Figure 10 to indicate the moment where the shift of use happened between the two. We assume that this shift shows us France does not limit its approach to cyberspace to computer systems only, but rather adopts Baumard's idea of strategic sphere, a more comprehensive approach. This is congruent with the absence of the term "cyber-war" in recent documents and the development of a galaxy of words having "cyber" for prefix.

Thus, new threats coming from cyberspace allowed France to reassert the protection of its national interest, which mainly depends on nuclear deterrence.

4.1.1.3. *Third step (Analysis)*

We have seen the whole picture of France's cyberstrategy from a chronological and rather descriptive way, followed by a concise quantitative point of view. Drawing upon our methodological framework - especially upon Baumard but also upon Hansen and Nissenbaum's works - we will now describe the evolution of the French cyberstrategy and observe if we can already try to partly provide an answer to our hypothesis. We will define to what extent the actions taken by France throughout the decade reflect what we think is a dominant power-sovereign strategy. As a reminder, should it be the case, France would adopt decisions falling

under the national cyberdefence pattern, that is the creation or expansion of large specialized units or military corps; constant references to critical infrastructures; and development of offensive and defensive capabilities.

As Baumard pointed out, the 2008 White Paper (WP) marks a turning point as "the protection of information systems is clearly defined as an integral component of the French national defense and security policy" (Baumard 2017:56). Indeed, French authorities elaborated a new national security strategy in 2008, aiming at reasserting the role of the state as protector of the nation's interests, namely population, territory, sovereignty and critical infrastructures. What is understood as critical infrastructures was already defined in a regulation of 2 June 2006, but with the 2008 WP the internet is included, intended as cyberspace. The will to include it not only stemmed from the growing threat generated by cyberattacks, but also from the need to make the internet more resilient. To that end, the ANSSI was created with the mission of protecting the information systems. Furthermore, the development of an array of tools to protect critical information systems was devised as well as the setting up of a detection center. This was the beginning of the development of French offensive and defensive cybercapabilities.

With the 2011 Information System Defence and Strategy, the empowerment of the French state continued. Indeed, the role and the workforce of the ANSSI was reinforced. Two years later, the 2013 White Paper was released, and the capabilities were again enhanced: an operational cyber-defense platform as well as a cyber-defense unit within the operational reserve were created. Moreover, both defensive and offensive capacities were increased to better prevent and detect attacks in cyberspace. In conjunction with these general increases, the level of security of information systems and the encryption means for defending them were upgraded. On top of that, these capacities – detect, prevent and protect – were integrated as components of the national sovereignty. French authorities used the growing cyberattacks happening worldwide, especially the cyberattacks directed at the G20 hosted in Paris at the time, to put forward this integration, arguing states cyber-arming themselves were a direct threat to essential institutions, companies and sectors for the nations' life, and consequently a threat to its national interest.

In 2014, the Cyberdefence Pact was brought forth. The whole cyberdefence was reorganized through the Director of the Defence Information and Communication Systems (DGSIC) and the operational cyberdefence capacities of the Planning and Operations Centre (CPCO) created in 2011. This aimed at strengthening the responsive stance of French forces but also at developing the exchange between the cyberdefence community and the national services,

fostering a cyberdefence spirit between the army, the ANSSI, the DGA and the operational reserve. Moreover, to achieve this reorganization, a new range of cybersecurity tools, both hardware and software, was designed to improve cyberdefence of the armed forces. However, the most important decision taken with this document, was creation of a center of (cyber) excellence in the Brittany region.

In 2015, the French National Digital Security Strategy was released by the French government to provide a balance between security and the digital[33]. Actually, if this strategic document is more oriented toward the civil society, we argue that France has over time understood the growing importance of non-state actors, especially individuals and companies, and purposely designed it this way. Indeed, each person is increasingly more connected and represents the possibility to be the weak link that could endanger the whole system. Therefore, to better reinforce its stranglehold on its cyberspace, France should secure each and every one level of entry point beforehand. Thus, many initiatives were implemented on the defensive side. Among these measures was the creation of an expert panel for digital trust at the national level, and placed under the supervision of the ANSSI and the SGDSN, but also the support for the development of French cybersecurity solutions and the improvement its critical networks' security as well as its resilience. In addition, the French state introduced the active monitoring of threats and security breaches for French authorities including ministries, businesses, and other territorial administrations. Lastly, cybersecurity crisis management exercises were extended over the national territory, while the development of a standalone cyber operational reserve was suggested.

In this case, the French process falls right into the approach of hypersecuritization, as the act of securitization is guided by the underlying potential threat of cyberattacks, to bring down with it an array of "other referent objects and sectors", namely all the actors cited above, because it mobilizes the "specter of the future"(Hansen and Nissenbaum 2009:1164). Indeed, within the 2015 document we can read "[i]n the future, an attacker could take control of connected objects, remotely interrupt an industrial activity or destroy its target"(ANSSI 2015:14).

One year later, the 2016 Le Dian's speech gave a boost to French cyberdefence. Along with his call for a new doctrine of the cyberfield, he announced the establishment of a cyber commandment called COMCYBER/CYBERCOM, working hand in hand with the head of

[33] Again, it is interesting to notice that "digital" progressively replaced "ICTs".

ANSSI for all matters revolving around the protection of the vital infrastructures (such as the OIVs), and the DGA delegate (SGA) for all technical engineering and the acquirement of technological equipment. In parallel to this new commandment, the actions in the cyberdefense field of the armed forces were divided into three categories: intelligence and investigation; protection and defense; and riposte/response and neutralization. Again, we clearly distinguish the couple offensive/defensive capabilities, the former being led by the Army, notably through the CALID, and the latter by the ANSSI. To achieve these changes, an increase in the global cyber workforce within the different French services to 3200, and an increase in the number of people from the two reserves to 4400. Specifically, the cyber military civil reserve and the operational reserve people were announced (see appendix 14). This long-term increase perfectly fits to the behavior of a power-sovereign country and to the hypersecuritization discourse as there is a constant expansion of France's cybercombatants.

In 2017, the conduct of a Defence and National Security Strategic Review was ordered by President Macron. The document bestows yet again more powers to the ANSSI, which can compel electronic communications operators to do a series of action (access to infrastructures, warn subscribers of potential breaches, set up detection mechanisms on site). However, this new power can also be reinforced upon decisions of the government, which strengthens the power of the French state even further. Finally, the pursuit of a cyber resilience continues with the 2018 document, which once again changes the French cybersecurity organization (now revolving round four operational chains) and marks the creation of two entities: the Cyberdefence Management Committee responsible for the implementation of decisions regarding the development and the general organization of the field taken by the High Council of National Defence (CSDN), and the Cyberdefence Steering Committee dedicated to the improvement of the knowledge of cyberthreats; the elaboration of an industrial, regulatory and normative policy on digital/cyber sovereignty. These institutions reflect the will we already mentioned of ensuring the protection of all actors. By the same token, the creation of a coordination center for the cyber crises (C4) as well as the network of cybersecurity correspondents aim at dealing with minor crises management, which are increasing and will continue to increase in the future. Yet, the French state does not forget its priorities such as strengthening the State's information systems protection (OIV and the core activities) is also on the agenda, by defining basic safety requirements. Finally, the definition of a doctrine of action in the face of a cyber-attack and ensuring secure communications belong to the strengthening of the attack-defense couple.

From an analytical point of view, we saw that the French national cyberstrategy followed a gradual evolution. The first phase that we can call wakening phase (2008-2013), was marked by the cyberattacks in Estonia. The probability of an upcoming cyberwar set the alarm and allowed France to adopt a hypersecuritization discourse, using the cyberthreat as the main reason. All the background work as well as the establishment of legal foundations were carried out. This phase was accompanied by the creation of the state's tool to protect its information systems, the ANSSI, with the 2009 decree setting down in writing the national agency and its abilities. During this first phase, the challenge was to build the foundations of the unknown. France turned inward to better reassert its sovereignty, redefining its national security, its national interest and its underlying components.

Then, the second phase was the expansion (2013-2015). It consisted of two aims, ensuring the current institutions were strong enough to face the future and broadening the scope of their mission. Slowly, the scenario of cyberwar was faded away to leave room for the growing threats of massive coordinated cyberattacks and daily cybercrime. In other words, without forgetting the worse-case scenario, France refocused its effort on better prevention and resilience in the face of daily cybercrime. Nevertheless, French authorities continued to use the specter of cyber threat to further develop their military capacities (more people) as well as capabilities (both software and hardware) and their legal framework, and to build the range of their sovereignty. Yet, as the challenge to protect the country was high and, France had to develop new ways to keep up the pace with cyberthreats, and the operational reserve was one of them. In parallel, a lot has been undertaken in this matter, such as the creation of the cyber center of excellence, with the aim of creating a French cyberculture, and partnerships with schools to ensure the future of the field.

Finally, there is the phase in which we are still, which is the consolidation (2015-?). The securitization of cyberspace has allowed the state to protect its sovereignty by protecting every referent object related to it. At the beginning, France was essentially focusing its attention on state and critical infrastructures, but time has proved these were not the main targets of cyberattacks. Recently, the shift towards more inclusion was engaged is now taking its roots in society. Indeed, there is a clear distinction of the roles of each institution. On the one hand, the ANSSI takes care of the prevention, raising the awareness of all actors of society and monitors the critical infrastructures. On the other hand, if France is under attack, the CALID takes over to contain and then solve the situation. Overall, the institutionalization of cyberdefence as a field has been effective, but the very structure was still too centralized from the beginning

onwards. Therefore, French authorities started a decentralization of its infrastructure, towards the regions and by setting a coordinator in each of them. At the same time, the numerous online platforms of the ANSSI have enabled it to diffuse its conception, good practices and keep the monopoly on information.

The French cyberstrategy has known various changes over the past decade. Still, based on the actions we listed in the appendix 13, not only does France seem to follow the path of the type power-sovereign but also to translate it through a dominant hypersecuritization discourse. The framework we have built seems to be coherent. Nevertheless, the two are not mutually exclusive. France may display a behavior of type power-sovereign but can also adopt decisions falling into the categories of the two other types. What we detect here is a trend, and the same applies to the discourses. Indeed, while the hypersecuritization is pervasive in all discourses, we inferred that if the power-sovereign does characterize France as a long-term trend, the state also took decisions oriented towards the two other types, namely societal and technical. It is important to remember that the cyberstrategy/cyberdoctrine is the combination of the three types.

4.1.2. Italian Case

4.1.2.1. *First step (Descriptive)*

As we have pointed out in the introduction, the attacks on Estonia marked a turning point as their impact left the states of the international community fearing the same scenario happening in their country, and most of them realized they were not ready. On its website, Italy's Intelligence System for the Security of the Republic (SISR) also looked back on these attacks to explain how itss new intelligence system was shaped eleven years ago (SISR 2018a). In our study, we decided to start from 2008 to February 2018. Yet, we have to start a bit before in the Italian case as the main institutional change happened one year before. Afterwards, we will go through the main documents identified as belonging the Italian cybersecurity path (SISR 2018b:4).

- *Law no. 124/2007*

Before 2007, the Italian system had not been reformed so deeply since the law no. 801 of 1977 (SISR 2018a). This law[34] brought huge institutional changes in terms of separation of functions and powers (SISR 2007). We will start with the functions. The former institutions related to intelligence services were dissolved and merged into a system called System for the Security of the Republic (SISR)[35]. The SISR groups six different actors: the President of the Council of the Ministers (after PCM), the Interministerial Committee for the Security of the Republic (CISR), the Delegate authority, and the three components of Italian secret services, namely the Security Intelligence Department (DIS), the External Intelligence and Security Agency (AISE) and the Internal Intelligence and Security Agency (AISI). We may now address the functions. First of all, as stated in section 1 of the law, the political responsibility is no longer shared with the Ministers of Defense and of the Interior but exclusively assumed by the President of the Council of Ministers (SISR 2018a). Additionally, he may delegate powers to the Delegate Authority. Together, they rule over the intelligence sector through the DIS and in return the appointed Director of DIS reports to them (SISR 2007:4–5). The PCM can count on the CISR to assist him. The CISR's main mission is to advise, propose and deliberate on the guidelines and general aims of information policy for security, as well as help in drawing up these legislative measures (art. 5 in the SISR 2007:7). Additionally, the CISR also decides on the financial resources granted to three secret service components mentioned above. As for the

[34] The law also deals with legal provisions that deeply change the framework surrounding state secrets, but it does not bring anything for our topic, we will therefore not enter into this part into details.
[35] For an overview of the complete SISR, please see appendix 21.

AISE and the AISI, their fields of action are indicated in their name. Indeed, the former deals with matters on the domestic level while the latter deals on the international level. Nonetheless, what may be the most relevant for comes at the section 1 (art.3), as stated:

> *[T]he President of the Council of Ministers shall co-ordinate security intelligence policies, issue directives and, after prior consultation with the Interministerial Committee for the Security of the Republic, issue every measure necessary for the organization and operation of the Intelligence system for the security of the Republic* (SISR 2007:5).

Thus, not only do they coordinate security intelligence policies together, but they are the only ones in charge of protecting the information systems. One last detail is provided by the article 38 and introduces an annual *Relazione al Parlamento,* which is a document presented to the Parliament and going back on the changes occurring the year before, in terms information security policy (SISR 2007).

- *Legislative decree no. 101 – January 9th, 2008*

The following year, the Ministry of the Interior defined the critical infrastructures of Italy in the decree no. 101 (Gazzetta Ufficiale 2008). According to the article 1.1, the infrastructures considered as critical information infrastructures of national interest are the IT services and systems dedicated to the support of the following institutional functions:

> *a) ministries, agencies and bodies, operating in the areas of international relations, security, justice, defense, finance, security and justice communication, transport, energy, environment, health; b) the Bank of Italy and independent authorities; c) companies owned by the State, regions or municipalities operating in areas of no less than 500,000 inhabitants, in the sectors of transport, energy, health and water; d) any other institution, administration, entity, public legal person or private persons whose activity is, for reasons of public order and security, recognized as being of national interest by the Minister for the Interior, including on a proposal from the prefects - provincial authorities of public security* (Gazzetta Ufficiale 2008:9).

In conjunction with this listing, an institution dealing with the prevention and repression of computer-related crime aiming the national critical infrastructures was created, the so-called Computer Centre for the Protection of Critical Infrastructure (CNAIPIC) under the article 3 of the same law (Gazzetta Ufficiale 2008:10). Insofar, the institution does not elaborate any strategic document or takes decisions in the matter of critical infrastructures, which is why we do not study this institution in this thesis.

- *Decreto del PCM – May 2010*

Promulgated on 5th May 2010, this PCM's decree (DPCM afterwards) established two bodies: the Political Strategic Committee (COPS) as political authority for crisis management,

and the Interministerial Situation and Planning Unit (NISP) as central coordinating authority for the Italian Government (Gazzetta Ufficiale 2010). On the one hand, the COPS gathers many actors, namely the Ministers of Foreign Affairs, of the Interior, of Defence, of the Economy and of Finance (art. 4 in the Gazzetta Ufficiale, 2010). It aims at assessing the elements of the situation, defining the measures to be submitted for the approval of the Council of Ministers, and may authorize the adoption of law enforcement measures (art. 4 in the Gazzetta Ufficiale, 2010). On the other hand, the NISP has a support function for the COPS. Chaired by the Secretary of State, it promotes and coordinates the conduct of interministerial exercises that involve the simulation of crisis situations or subjects under discussion (art. 6 in the Gazzetta Ufficiale 2010). Among the participants to the NISP, we find "representatives from the Ministries of Defense, Foreign Affairs and the Interior as well as from other agencies and administrative bodies including the AISI and the Department of Fire, Rescue and Public Civil Defence" (CCDCOE 2015:11). Furthermore, the NISP contributes to the harmonizing of common procedures and capabilities among these actors (Gazzetta Ufficiale 2010). Finally, should a crisis occur, NISP has a coordinator role and works closely with the COPS and the PCM to formulate "a national position collaborative efforts vis-à-vis international actors" (CCDCOE 2015:11). Yet, when preparing its response, NISP relies on approval and support from the Ministry of the Interior and its Interministerial Technical Commission for Civil Defence (CITDC) (CCDCOE 2015:11).

- *Laws no. 133/ 2012 and 134/2012 – amendments of the law n.124/2007 - 2013*

During the month of August 2012, a series of amendments of the 124/2007 law were passed. In the first amendment (133/2012), the competencies of the PCM were modified with a new paragraph added on section 1.1 of the Law 124/2007. An article was added and specified the range of the PCM power. Indeed, it is stated that:

> *after consultation with the CISR, he communicates to the DIS and security information services directives in order to reinforce the information activities for the protection of material and immaterial critical infrastructures, with a particular emphasis on cybernetic protection and national cyber security* (Parlamento 2012:1).

Thus, with this amendment the PCM should consult the CISR before going further in the decision-making process. Also, the DIS was modified in this law and was entitled to "carry out the coordination of information research activities aimed at strengthening cybernetic protection and cyber national cyber security" (Parlamento 2012:2). Additionally, the art. 38 we mentioned above about the annual *Relazione al Parlamento* was modified to also deal with "cybernetic protection and information security" . In the second amendment (134/2012), Italy endows itself

with a new institution the Agency for Digital Italy (AgID) (art.19), which actually replace the former *DigitPA* (Parlamento 2012:96–97). All the functions of the AgID are detailed in the article 22, but if we were to sum up its mission, it would be "guarantee[ing] the achievement of the Italian digital agenda objectives and contribute to the diffusion of information and communication technologies, with the aim of fostering innovation and economic growth" (AgID 2018). The AgID also "supports digital innovation and promotes the dissemination of digital skills, also in collaboration with international, national and local institutions and bodies" (AgID 2018).

- *Decreto del Presidente del Consiglio dei Ministri - 2013*

The Decree of the PCM of January 24th constitutes the first major document for the Italian cyberstrategy. The reason of its drafting is stated in the preamble, namely "because of the features of the cyber threat being a risk to national security, it is necessary to define a national strategic framework"[36] (Parlamento 2013). It is divided in three main orientations: (1) policy guidance and strategic coordination; (2) support and (3) crisis management. The decree defines:

> *the institutional architecture for the protection of national security regarding material and immaterial critical infrastructures, with particular regard to cybernetic protection and national information security, indicating to this end the tasks assigned to each component and the mechanisms and procedures to be followed for the reduction of vulnerability, risk prevention, timely response to attacks and the immediate restoration of the functionality of systems in the event of a crisis.* (Parlamento 2013)[37]

It is interesting to notice that we find the same key components to be protected as in the French case, that is critical infrastructures. In the article 2 of the decree, we have four definitions of interest to us: cyberspace, cybernetic security, cybernetic threat and cybernetic event, which seems to correspond to a cyber(netic) attack. Let us have a look at the first definition.

Thus, Italy defines its cybernetic space as "the entirety of the interconnected computer infrastructures, including hardware, software, data and users, as well as the logical relations, however established, between them". We notice that this definition is broad and even include the software part which is quite peculiar. Then, we have the definition of cybernetic security, which is defined as:

> *condition for which the cybernetic space is protected thanks to the adoption of suitable physical, logical and procedural security measures with respect to events, of a voluntary or accidental nature, consisting in the unlawful acquisition and transfer of data, in their unlawful modification or destruction, or in the damage, destruction or blockage of the*

[36] Translated from "in ragione delle caratteristiche della minaccia cibernetica quale rischio per la sicurezza nazionale, sia necessario definire un quadro strategico nazionale." (Parlamento 2013).
[37] Free translation.

regular functioning of networks and information systems or their constituent elements (Parlamento 2013)

At a first glance, it is surprising that Italian authorities still stick to the full cybernetic form instead of cyber, maybe the lexicometry analysis will show an evolution in that regard. On the content itself, the term condition implies that several requirements must be met in order to be secured, but overall this definition is also broad, the constituent elements of which can allow to stretch the range of what can be securitized, which is useful for a state. The next definition is the cybernetic threat which remains classic and the one of cybernetic events. This definition is also standard, though the name is a bit unusual and though we would already expect the term cyberattack instead or cybernetic event (Parlamento 2013).

We then move on to the functions of the actors within the two future frameworks. First, the PCM has the final say on the adoption or update of the National Strategic Framework or the National Plan for Cyberspace Protection and ICT Security (art.3). However, it is the CISR that leads the changes and suggest them to the PCM for approval. Then, the CISR is to be assisted by a new body provided by the article 5 of the DPCM. Finally, this DPCM brings another important body attached to the Office of the Military Counsellor, namely the Cyber Security Unit (NSC). Under the article 8, the NSC is created and under article 9 it is stated that it will act as a link between the various components of the institutional architecture that intervene in various capacities in the field of cyber security, and act in compliance with the powers attributed by law to each of them (Parlamento 2013). At the end of the decree, we find article 11 on private operators. According to this article, "private operators providing public communications networks or publicly available electronic communications services, or operating critical infrastructures of national or European importance" should communicate with the NSC, adopt best practices, share information with other entities link the protection of the cybernetic security, and help in reestablishing the systems in times of crisis (Parlamento 2013).

Following this DPCM, two major documents were released: the National Plan for Cyberspace Protection and ICT Security, and the National Strategic Framework for Cyberspace Security.

- *National Strategic Framework for Cyberspace Security – 2013*

It turns outs that the two documents are linked. The first one, the framework, provides an assessment of the situation and gives definitions of each term related to cyberspace. Interestingly, the English version shows us that Italy has adopted the form cyber while it stays

cibernetica in Italian. The framework reminds us that "[t]he digital arena is not a space outside ofthe law" which echoes to the NATO statement the same year (PCM 2013:5; UN General Assembly 2013). Overall, the first part of the document is very descriptive. It recalls all the characteristics of cyberspace and many definitions that we will not compare as they do not bring much to the analysis. Nonetheless, the second part brings more information on the Italian stance on cyber-related issues. For instance, we should point out that when talking about cyberthreats, Italy is more worried about cybercrime than cyberwarfare. Indeed, Italian authorities explain that "the theft of the original scientific, technological and companies' know-how is a direct damage to their existing comparative advantage, undermining their competitiveness in the global markets" (PCM 2013:13). For them, cybercrime is therefore "a threat of primary importance"(PCM 2013:13). Furthermore, at two different moments, Italy mentions cybercrimes threaten "innovation [which is] at the cornerstone of its growth and competitiveness" (PCM 2013:5). In the light of these statements, should we infer that it is more important for the Italian national interest to protect its innovation rather than its critical infrastructures? A deeper analysis will help us solve this first question. Before moving the next point, it is interesting to note that Italian authorities conceive "deterrence capabilities in cyberspace […] as a disincentive to potential adversaries and criminals" (PCM 2013:25). Indeed, such a stance goes against what we have seen in the French case.

Eventually, we have acquired some information on the role of State in cyberspace (PCM 2013:14). Italian authorities assert the primacy of the state in this domain not as a given but based on two reasons. First, states "have the ultimate responsibility for the protection of ICT infrastructures on their own territory, even if they are owned and operated mostly by the private sector" (PCM 2013:14). Second, they "have the human and financial resources as well as the capability to organize and manage, overtime, complex organizations" (PCM 2013:14–15). Faced with this position, what interests us is to look at the six strategic guidelines dictated in this framework (PCM 2013:9). To have a better explanation, we will directly move on to the national plan where these measures are fully explained.

- *The National Plan for Cyberspace Protection and ICT Security – 2013*

First of all, it is instrumental to specify that Italy aims at involving actively both of private and public stakeholders, intended as operators providing "public networks of communications or electronic communication services to the public, operating national and European critical infrastructures depending on ITC systems' "(SISR 2013:26). In return, they are expected to

communicate every breach of their systems to the Cybersecurity Unit, adopt best practices, share information with the state agencies, and globally collaborate the crisis management should one crisis occur (SISR 2013:26) Among the public actors we find again those mentioned above, namely the Agency for Digital Italy, the PCM, the Ministry of Foreign Affairs, the Ministry of Interior, the Ministry of Defence, Ministry of Economy and Finance and the Ministry of Economic Development (MiSE) (SISR 2013:27–28).

That being said, we may come back to the six strategic guidelines Italy wants to implement during the period 2014 to 2025. The guidelines are the following:

> *(1) enhancement of the technical, operational and analytic capabilities of all concerned stakeholders and institutions through a joint effort and a coordinated approach; (2) strengthening of our capabilities to protect national critical infrastructures and strategic assets and stakeholders; (3) facilitation of all public-private partnerships; (4) promotion and dissemination of the Culture of Cybersecurity; (5) reinforcement of our capability to effectively contrast online criminal activities and illegal contents; and (6) strengthening of international cooperation* (SISR 2013:6).

These six strategic guidelines are divided in eleven operational guidelines, namely:

> *(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; (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; and (11) implementation of a national system of Information Risk Management* (SISR 2013:7).

Overall, the Italian framework is an ambitious undertaking. First, the country wants to develop a whole set of institutions to protect its cyberspace, developing both offensive and defensive. The former would be developed through the creation of the Joint Headquarters Cyber Operations (COCI), a command and a control structure, whereas the latter would be developed through the creation of a national and regional computer emergency response teams (CERT) as well as a Computer Incident Response Capability (CIRC). Furthermore, a whole section is dedicated to the actions at both national and international. With this framework, Italy has undertaken several projects. At a national level, it plans to enhance the cooperation of the public and the private sector; develop trainings and involve academia in the shaping of the national cyberstrategy; enhance the communication between all stakeholders. At the international level, Italy draws a lot on what has already been done abroad and within the IOs. Even if Italy was a late-comer in the field, this is a real advantage. Indeed, it is always easier to mimic others to better set up a system (SISR 2013:9–30).

As far as the Italian cyberdiscourse is concerned, the Italian authorities have a dual approach. On the one hand, Italy seems to adopt a societal cyberdoctrine, including the public and private actors in the process, drawing on its neighbors and the international organization to develop its cyberinfrastructures. On the other hand, it relies a lot on the adoption of technical norms and legislation, often implementing what is done at the European level. Many elements are borrowed from the NATO, like the semantics for instance. Contrary to France, Italy has never left the integrated military structure and has benefitted from its know-how ever since the Alliance was created. A last point is to be raised on the national interest, namely that we might expect some standardization measures and the development of a classification of the ICT networks supporting national critical functions, but no real mention of the national interest is made.

After the publication of these two documents, the CERT for the public administration as well as the national one was set up in 2014, and was followed by the signature of a collaboration agreement between the National Interuniversity Consortium for Informatics (CINI) in October 2014 (SISR 2018b:4). This agreement is an instrumental step as it marks the beginning of a long-term collaboration which continues up to this day.

- *Directive on the inter-ministerial coordination – 2015*

On 1st August 2015, the PCM Matteo Renzi passed the so-called directive on the inter-ministerial coordination, which aim was to consolidate the system in order to ensure the resilience of the national IT infrastructure in the face of events such as accidents or hostile actions that may compromise the functioning of the systems, and the physical assets controlled by them (SISR 2015). Therefore, the PCM wanted the alignment of the Italian strategic assets with its international counterparts to interact with its main international partners as equals. To achieve this objective, he pointed at four domains in which Italy should pursue efforts: public administration, public-private partnerships (PPP), national research and international cooperation. In practical terms, he suggested several actions to follow, that is: an increased and more effective coordination with the public administration by strengthening their capacity to react to cybernetic events from a technical point of view and setting minimum safety standards (provided by the AgID); for the PPP actions, he advises to develop relations with the private sector, creating an effective and thorough partnership with all non-public operators, who are entrusted with the control of information and computer infrastructures, on which rest essential

functions for the country system. For the research, he puts the emphasis on more research, and especially, on the development of instruments of defense and reaction to be as advanced as possible from a technological point of view of research bodies. Finally, for the international cooperation, he stresses the need for Italy to meet the necessary "common level of preparation and interoperability" in order to conduct properly its bilateral and multilateral relations.

- *Decree-Law no. 174 - 30 October 2015*

The next document relevant to our analysis is the decree-law passed in October 2015, which aims at changing provisions on Intelligence matters, especially the competences of the CISR. Amending art. 5 of the law no. 124 of 3 August 2007, it states that the CISR "may be convened by the PCM, with the functions of advice, proposal and deliberation, in case of crisis situations involving aspects of national security, according to procedures established by specific regulations pursuant to Article 43 of Law no. 124 of 3 August 2007" (art. 7-bis in the Gazzetta Ufficiale 2015).

- *Law No. 208 - Stability Law for 2016 - 28 December 2015*

With the 2015 stability law, Italy boosts its defense sector by granting €300 million for the modernization of defense and security sector equipment and instruments, and for investments to adapt counter-terrorism capabilities. Yet, what is especially interesting for our case is the €150 million budget allocated to strengthen its cyber security (MEF 2016).

- *Development until the Gentiloni DPCM – 31 March 2017*

Following the stability law, Italian cybersecurity development went on as, in June 2016, the process of transition for the infrastructures devised in the 2013 frameworks was launched (SISR 2017a). A month later, the European Parliament adopted the NIS directive, providing legal measures to improve the level of cybersecurity in the EU, that should be implemented by May 2018 (SISR 2018b:4). However, the next step for Italian cybersecurity came in March 2017. Indeed, with the Decree of the PCM Paolo Gentiloni, the new National Plan for Cybernetic Protection and Information Security was adopted. Up to this adoption, the biannual plan for 2014-2015, triggered by the 2013 strategic documents, was a good start, yet a lot remained to be done. Italy became aware that his vison of national security was too focused on the public sector as far as sensitive information is concerned, neglecting the relevance of private actors operating in strategic sectors. Thus, the need for a systemic implementation became crucial and

implied setting the basic safety requirements for the Italian critical and strategic systems (SISR 2017b:9). Furthermore, the Italian authorities realized the need to leverage the competences and responsibilities of the different actors (public, private, research) that constitute the backbone of the national cyber fabric to achieve a successful implementation. In addition to that, the DPCM Gentiloni was the opportunity to modernize and prepare the Italian cyber architecture for the future NIS implementation.

- *National Plan for Cybernetic Protection and Information Security – 2017*

This new plan was devised around six strategic orientations:

> *(1) strengthening the defense capabilities of the national critical infrastructures and the actors of strategic importance to protect the country as well as the system; (2) improvement, of the technological, operational and analytical capabilities of the institutional actors concerned following an integrated approach; (3) encouraging cooperation between national institutions and companies; (4) promoting and disseminating a culture of cyber security; (5) strengthening international cooperation on cyber security; (6) strengthening capacities to fight illegal online activities and content* (SISR 2017b:6)

To achieve such orientations, the plan has devised eleven operational orientations:

> *(1) reinforcement of the intelligence, the police, as well as the civil and military defense capabilities; (2) reinforcement of the organization and the arrangements for coordination and interaction at national level between public and private bodies; (3) promotion and dissemination of a culture of information security as well as education and training; (4) international cooperation and exercises; (5) operationalization of national incident prevention, response and remediation structures; (6) legislative measures and compliance with international obligations; (7) compliance with security standards and protocols; (8) support industrial and technological development; (9) strategic and operational communication; (10) resources (11) implementation of a national cyber risk management system* (SISR 2017b:6)

In practical terms, we can divide the action of the national plan in three parts: the core changes and competencies, the civil society and the private sector, and the power capabilities.

First, we will analyse the core changes that aim at enhancing the overall integrated response capabilities to cybernetic events, intended as cyberattacks. The DPCM fortifies the role of the CISR which will contribute to raising the country information security awareness by issuing guidelines (SISR 2017b). To this end, the CISR can count on the support of the interministerial coordination of the CISR administrations, namely the technical CISR, and the DIS (SISR

2017b:7)[38]. Moreover, formerly attached to the Office of the Military Counsellor, the Cyber Security Unit, headed by a deputy General Manager, will from now on be under the supervision of the DIS to ensure a coordinated response to cybernetic events. The latter is of significant concern for national security, and in connection with all the structures of the competent Ministries on the subject (SISR 2017b:10). Then, the relationship between the two CERTs (National and Public Administration) will be strengthened in order to ensure the necessary operational alignment of the same rules and responsibilities for the Italian public administration (through the Digital Agenda and AgID) and the private sector (through the Ministry of Economic Development) (SISR 2017b:10). Additionally, the DPCM entails the creation of a National Evaluation and Certification Centre (CVCN) inside at the Ministry of Economic Development (MiSE) to verify the reliability of the infrastructures. Eventually, the range of entities designated as operating in sectors of interest to national security will be expanded, including essential service operators and digital service providers. The latter will have an obligation to notify major cyber incidents, resulting otherwise in penalties in case of omissions (SISR 2017b:11).

To realize such initiatives, it is also necessary to involve the academic world and the research sector, as well as a widespread collaboration with two components of the national cyber fabric, which are civil society and the private sector.

A first step in this regard will be to create start-up financing or even encourage participation in venture capital. Then, the Italian state will create two new bodies to support the research. The first is the National Centre for Research and Development in Cybersecurity, which field of study will be vast, tackling malware analysis, security governance, critical infrastructure protection as well as threat analysis systems. The second body is the National Cryptography Centre which will be involved in the design of ciphers, the creation of a national algorithm and blockchain, and in safety assessments (SISR 2017b:11–12).

Nevertheless, building a national defense infrastructure is not enough. Indeed, Italy also needs to develop a capacity to counter cyberattacks. Following this idea, the Italian Defense administration decided to protect its networks, both on its national territory and on the operational theatre, by developing cybernetic capabilities. This capacity building entails the establishment of a Joint Headquarters Cyber Operations (CIOC), responsible for the protection of the systems and networks of the ministries, as well as for the execution of operations in the

[38] To better picture this new cyber organization please refer to appendix 22.

field cybernetic and the creation of a national virtual polygon. The latter is a cybergroup meant to improve cyberdefence skills at the Telecommunications School of the Armed Forces of Chiavari, located in Genova (SISR 2017b:12)

Finally, to have a better coordination between all of these entities and to integrate the CIOC, the definition of a common protocol is entailed in the DPCM. The Italian Intelligence and the Defence Staff have developed a strategic framework to allow the better positioning of the constituent CIOC with regard to operations in the digital domain (SISR 2017b:12).

Overall, the DPCM Gentiloni reshuffles the way cyberdefence and its prevention have been so far conceived by the Italian authority. If we look at the words used to formulate its orientations, we notice a change of semantics which stems from the harmonization with the terminology used by international organizations such as the NATO, the UN and the EU (SISR 2017b:7). As far as the organization is concerned, bodies are reshaped (NSC), better coordinated (CERTs), created (CVCN, National Committee for Research in Cybersecurity and National Encryption Centre), and the chain of command for the management of crises is contracted to improve its efficiency.

There is no point in reproducing the same table we did for the French case (table 6), as the Italian case has only two official frameworks from the government and through the SISR only. Nevertheless, based on the results we gathered in the framework for Italy (appendix 23) we cannot yet predict a dominant cyberdoctrine or cyberstrategy. Indeed, Italy seems to display a mix between the societal and technical visions of cyberdoctrine and uses a technical cyberdiscourse to implement societal decision. The lexicometry analysis may help us to confirm our first guesses.

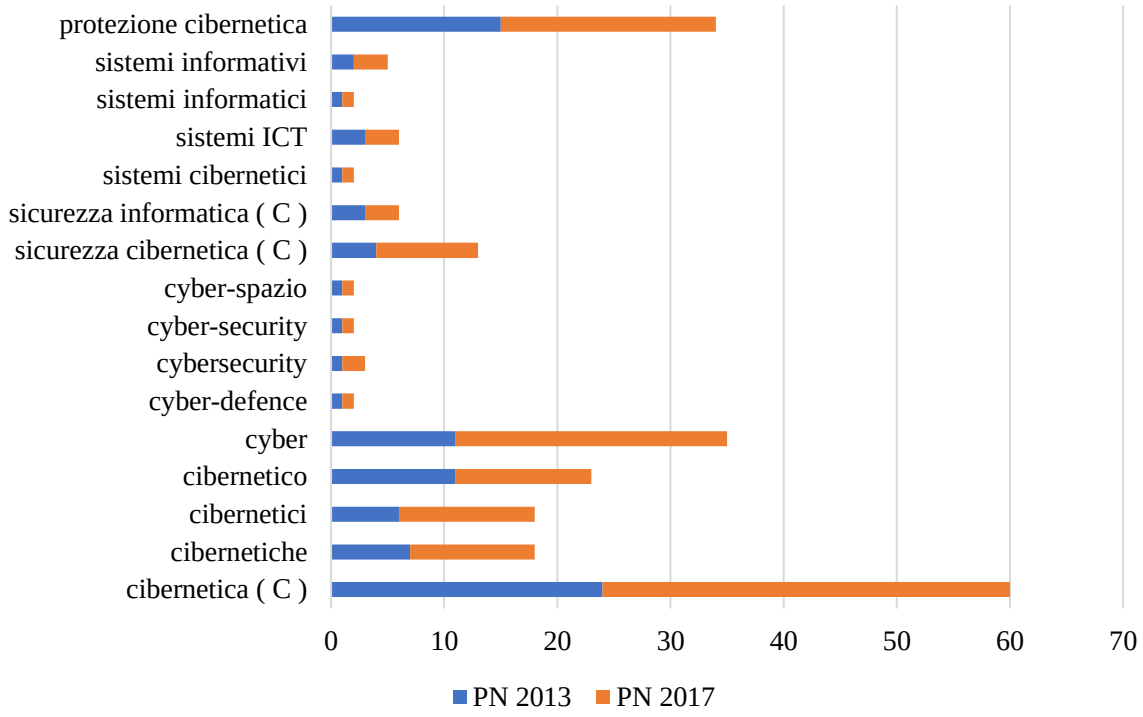
4.1.2.2. *Second step (Lexicometry)*

We now move on to the second step for Italy, that is the lexicometry analysis. The remarks enumerated in the section 4.1.1.2 also apply to the Italian case (symbol and software used)[39]. Nonetheless, we should mention some specificity for the Italy. First, we have to take into account the number of texts available and how the Italian national cyberstrategy was devised. In our case, we only have three documents at our disposal, two of which having the

[39] There are only two variations (i/e) for the plural forms and (C) for the merging of words in capital letters with words not in capital forms.

same content to some extent. Therefore, we will only take two documents for this analysis, namely the two National Plans for Cybernetic Protection and Information Security of December 2013 and March 2017[40]. Then, we will have to use the original document in Italian, as the second one was not translated. Thus, we provide a new codebook, translating the previous one in Italian (appendix 16).

Figure 13 *Use of the cyberwords through time (in words) - Italy*

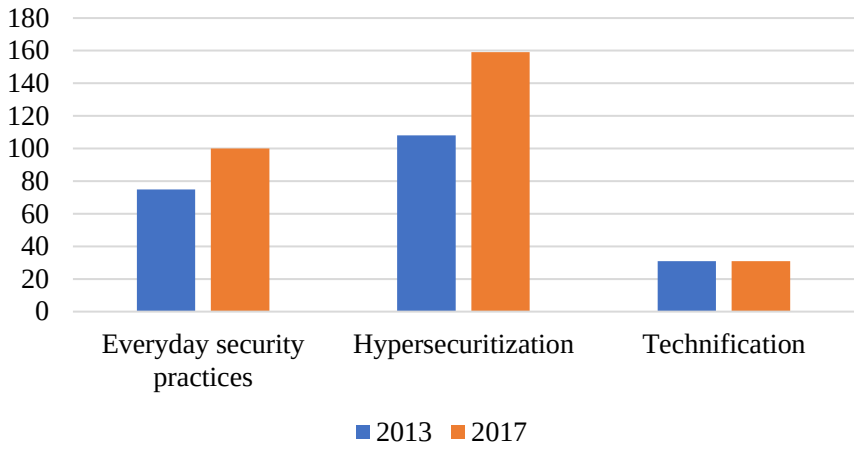


Note: made from the extraction of data through the software TXM, please refer to appendix 27 to consult the data used.

We performed the same analysis of the set of cyber-related words used in the corpus. Even if we only have two documents, we can still detect a slight increase in all the words, and an almost twofold increase for "cibernetica" and "cyber". We also included the words made with the Italian prefix *ciber* to see if Italian authorities had been using anglicized forms. The results cannot really confirm whether it is the case. On one hand, the form "cibernetica", both alone and in combination with other words, is still used in 2017. On the other, we can point to the growing use of "cyber".

[40] (original version: *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica 2013 & 2017*)

Figure 14 *Cyberdiscourse use between 2013-2017 (by type and words) - Italy*

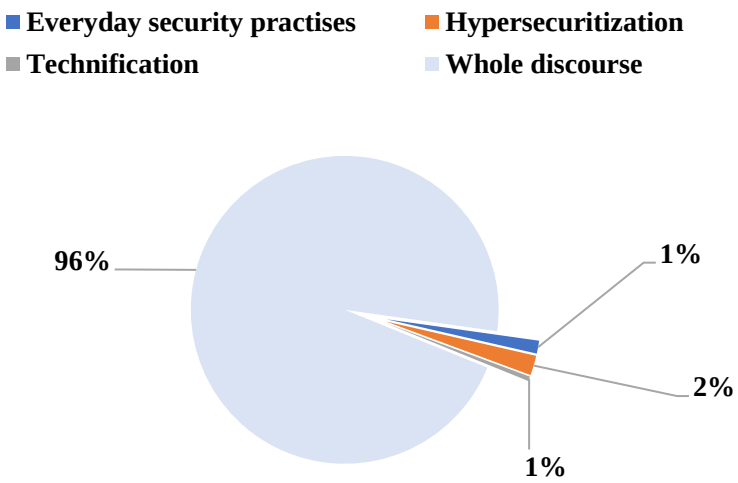


Note: made from the extraction of data through the software TXM, please refer to appendix 26 to consult the data used.

During the period 2013-2017, our results contradict the assumptions we had, at least for the technification part. Part of this result, without any doubt, stems from the few documents selected for the lexicometry analysis. Nonetheless, we can assume that Italy is adopting a hypersecuritization cyberdiscourse but adopting a different type of cyberstrategy. However, a deeper analysis would be necessary with more documents to confirm it.

As for the French case, we established the average use of each cyberdiscourse and their space within the whole cyberdiscourse, but the result does not bring much to the complete analysis. We obtained the same results as for France with a dominant hypersecuritization cyberdiscourse.

Figure 15 *Cyberdiscourse type average between 2013-17*



Note: made from the selected words for each cyberdiscourse and applying an average (in respect to whole discourse), please refer to appendix 26 to consult the data used.

Overall, for the Italian case, the lexicometry is not very useful, if not to detect change in the words used. This only confirms the harmonization of the terminology used with the one of IOs, such as the EU or the NATO, and discussed in the 2017 National Plan for Cybernetic Protection and Information Security. Unfortunately, the lack of comprehensive strategic documents, like the French white paper, is the reason of these poor results. Yet, we do not argue that Italy does not possess white paper on defense at all, which would be a false statement. We merely suggest that the place dedicated to cybersecurity and cyberdefence has been quite absent so far, if not weak. We will come back on the issue in the next part and suggest alternatives to better analyze the Italian case.

4.1.2.3. *Third step (Analysis)*

The two first steps have demonstrated how Italy, despite being a late-comer in the cyberfield, succeed in catching up its European partners. Like for the French case, we will try to provide an adequate splitting of the different phases Italy has undergone to reach its current status.

As we have seen, the cornerstone of the Italian cyberstrategy is the law no. 124 of 2007. The reform of the Italian architecture was also decided after the changes occurring on the international stage. Thus, we can also say that the first phase Italy has gone through was the awakening. From the beginning onwards, the President of the Council of Ministers was the central piece of the Italian cyber-architecture. Indeed, the year 2007 marked the formation of a whole new ecosystem for Italy, the SISR. Soon enough, the Italian authorities decided to frame what they understood to be critical infrastructures, and to create an institution placed under the Ministry of the Interior, the CNAIPIC. However, the legislative decree of 9th January 2008 was not part of the cyberstrategy. Then, came the decree of May 2010 and the two new bodies (COPS and NISP) to better deal with crisis management. Again, this did not change a lot in the Italian cyber-landscape. Indeed, we must wait for the laws 133 and 134 in 2012, amending the 2007 law, to observe a change in the Italian structure. These two laws brought about two main changes: a growing role for the CISR, which had to be consulted before the decision-making process got through the DIS, and the creation of the Agency for Digital Italy (AgID) to achieve the Italian digital agenda, foster growth and innovation, and "support digital innovation and promote the dissemination of digital skills, also in collaboration with international, national and local institutions and bodies" (AgID 2018).

In 2013, Italy entered a second phase that we could call realignment. This realignment began with the decree of the PCM of 24th January 2013. As mentionned, this initiative was launched "because of the features of the cyber threat being a risk to national security, it is necessary to define a national strategic framework" (Parlamento 2013). The crucial point here is to see that Italy based its framework on the active involvement of both private and public stakeholders, which differs from France, which remained focused on the state. In the analysis, we saw that the framework reshuffled the places within the Italian cyber-architecture. As part of its biannual program (2014-2015), the Cyber Security Unit (NSC) was put under the DIS, whereas the management of the cyberdefence was improved, through the creation of a command and control structure (CI) and two CERTs computers (one national and one for the public administration), as well as a Computer Incident Response Capability (CIRC).

This alignment went on with the 2015 directive on the inter-ministerial coordination that strengthens the role of the CISR, which becomes crucial in times of crisis. Furthermore, the 2016 stability law provides a budget for the national cyberdefence.

Finally, the National Plan for Cybernetic Protection and Information Security came in 2017. Its content aims at fortifying the role of the CISR, which now has the role of raising the country information security awareness by issuing guidelines. In this mission, it is assisted by the CISR-T and the DIS. In addition, the two CERTs are strengthened, a National Evaluation and Certification Centre is set up to verify the reliability of the infrastructures, while the range of essential operators is also expanded, including essential service operators and digital service providers. The 2017 framework is also the opportunity for Italy to reassert its willingness to include the stakeholders within society. It calls for more collaboration between the civil society and the private sector, but also encourages academicians to carry on research on cyber-related topics. Finally, the offensive-defensive capabilities were reinforced with the establishment of the Joint Headquarters Cyber Operations (CIOC) in charge of protecting ministries' networks and systems. To improve the cyber-skills of its combatants, a cybercell was also put in place within the Telecommunications School of the Armed Forces of Chiavari, located in Genova.

By going into details into the Italian case, we have seen that the construction of the Italian strategy had been different. The lexicometry did not enable us to confirm our assumption.s However, we still believe the Italian cyberdoctrine is mainly based on a mix of societal and technical type, eventhough its discourse seems to lean towards hypersecuritization. It is hard to tell if Italy has entered a third phase of consolidation in 2017, because much of what is done

remains hidden in a way. Indeed, we do not have any information on the annual budget or the workforce of the different institutions we mentioned. Is it part of the Italian strategy not to display all its assets or does it a reflect a cyberfield still burgeoning? It would require a deeper analysis to shed light on these phenomena, to which we are unable to bring answers at this point.

4.2. Comparison

After having gone through a decade of documents, we were able to delineate the main differences and similarities for the two countries. We will divide this section in two parts: one going back on the qualitative analysis, and the other on the quantitative analysis. For the qualitative part, we will first go through general features, then move on to their operational institutions, and finally talk about the education and training in both countries. For the quantitative part, we will compare the difference between our assumptions and the proper results. To better picture the results, it is useful to keep in mind the two organigrams of France (appendix 11) and Italy (appendix 22) as well as a table which summarizes all the information below (appendix 28).

Firstly, as far as political responsibility is concerned, the results are relatively similar for both France and Italy. While in the French case, the Prime Minister bears the political responsibility, in the Italian case, it is the President of the Councils of Ministers (PCM), as we have seen with the 2007 law. Furthermore, the definition of the cyberstrategy in Italy is elaborated by the PCM, who has to consult with the Interministerial Committee for the Security of the Republic (CISR), whereas in France, the President of the Republic, being the head of the state, has a word with the Ministers and his Prime Minister, who then apply the decision. In both cases, it is a rather top-down approach. As we have observed all along the French case, the national interest is determined by the population, the territory, the critical infrastructures and sovereignty. In the Italian case, there is no such discourse, except on intellectual property. With regards to national infrastructures, both countries have adopted legislative dispositions stating what is intended as such in the past decade or earlier (Regulation of 2 June 2006 and white paper (2008) for France and Legislative decree no. 101(2008) for Italy). Also, a very interesting point concerns the deterrence. Italian authorities do not rule out cyberdeterrence, they even conceive it as “a disincentive to potential adversaries and criminals” (PCM 2013:25). On the contrary, for France, notably to former Foreign Minister Le Drian, there is no such thing as cyberdeterrence, as only nuclear power matter in terms of deterrence (Le Drian Jean-Yves 2016). Eventually, what is the role of the state in the cyberdefence field? In Italy, the question was an observation rather than a choice. Indeed, the state is one of the main actors in cyberspace because the infrastructures mentioned are located on its territory, and because it is one of the only actors having the sufficient resources to organize and manage cyberdefence (SISR 2013:14). For France, the state is the sole responsible actor of cyberdefence and that is it (SGDSN 2018).

Secondly, our comparison tackles the institutions. On both sides, there are institutions to monitor and defend the state but also to counter attacks if needed. For operational centers in the public sector, we have the Agency for Digital Italy as well as the CERT for the public administration on the Italian side, and which also deals with the private sector. Whereas in France, it is the ANSSI especially and the National CERT. For the defensive part, Italy can count on its national CERT, while France relies on the ANSSI as well as its operational reserve. As far as the offensive operational centers are concerned, France's counterattack capabilities lie in the hand of the Analysis Centre for Cyber Defensive Operations (CALID), which is under the responsibility of the Ministry of Defense and DGA, and the cyber commandment (COMCYBER). In Italy, this task goes to the Joint Headquarters Cyber Operations (CIOC), placed under the responsibility of the Minister of Defense. Eventually, both countries are also endowed with an institution protecting its critical infrastructures. In Italy, this matter is dealt with by the Computer Centre for the Protection of Critical Infrastructure (CNAIPIC), and under the responsibility of the Minister of the Interior and the National CERT while in France, it is again managed by the ANSSI.

Thirdly, both academic and military trainings have been set up in the two countries. Looking at the public part, we mainly encounter academic and computer sciences studies that include a more detailed emphasis on security matters. In the case of France, many universities have included governmental recommendations to include a core knowledge that should be shared by all students and future professionals. This initiative is called *SecNumedu*. Furthermore, as far as the military training is concerned, Italy has established tabletops at the Telecommunications School of the Armed Forces of Chiavari, in Genova. We can assume this kind of knowledge was acquired by means of its active participation to the NATO. In France, we saw in the analysis that the CALID in Brittany acts as a center of excellence within the formation organized with the Information Assurance Division of the DGA. Finally, France also set up an online platform called CyberEdu to diffuse good practices and common knowledge on cybersecurity to the public.

Now, returning to the qualitative, we obtain mixed results. For the French case, based on the decisions taken by the French authorities during the past decade, we assumed France adopted a cyberdoctrine of type III - that is Power-sovereign - and therefore should follow an hypersecuritization cyberdiscourse. It turned out that the quantitative results came to support our assumption. Indeed, figure 11 showed us that France has had a dominant hypersecuritization cyberdiscourse which confirms our hypothesis (H2). For the Italian case, the results of the

qualitative analysis left us thinking we were facing a combination of the societal and technical visions of the cyberdoctrine. As our main documents were decrees and laws, we also assumed Italian authorities would use a technical cyberdiscourse to implement societal decision. However, the lexicometry analysis showed us that the Italian cyberdiscourse from 2013 to 2017 was also leaning towards a hypersecuritization cyberdiscourse. Yet, in this case, the analysis *in se* cannot be compared to what we obtained with the French analysis, as we had lesser documents over a shorter period of time. The main reason for this, is that Italy has not released as many documents as France did, and the few documents available are mainly listing decisions and orientations, which makes it difficult to spot a trend in the discourse. Nonetheless, the hypothesis (H2) is not validated for the case of Italy, as far as the quantitative analysis is concerned. For the qualitative one, we still argue Italy employs a technical cyberdiscourse to implement societal decision.

As far as our first hypothesis (H1) is concerned, namely that the securitization of French and Italian cyberspaces aims at asserting their national interest, we saw that it was confirmed for France and partly confirmed for Italy. The national interest is intended here as an all-encompassing set of things a state is ready to defend, both material and immaterial, even by means of violence if needed. For both countries, we observed that national interest has been wielded in the face of threats endangering the population, the territory, the sovereignty, the critical infrastructures or even intellectual property. Indeed, for France we noted that, early on, in the 2008 White Paper, French authorities were stating that "the internet will need to be considered as critical infrastructure and considerable effort will be made to improve its resilience" (Mallet, France, and France 2008:174). As the French national interest is made up of its population, its territory, its sovereignty and its critical infrastructure, we can effectively confirm this hypothesis. While for the Italian case, the argument put forward is that cybercrime is "a threat of primary importance" (PCM 2013:13) which threaten "innovation [which is] at the cornerstone of its[Italian] growth and competitiveness" (PCM 2013:5). In both study cases, it is necessary to slightly stretch the meaning, but we do discern the connection between the implementation of such far-reaching policies and the use of threats to the national cyberspace that encourage their achievement.

Conclusion

Our research aimed to study to what extent cyberspace constitutes a way to reaffirm a country's national interests through the implementation of a cyberstrategy. Drawing upon two theoretical frameworks (Hansen and Nissenbaum 2009; Baumard 2017), we have built our own theoretical framework, not only to determine the kind of cyberdoctrine adopted by states, but also to unveil the type of cyberdiscourse that accompanied it.

Our methodological framework was based on the mixed-methodological approach that combines both qualitative and quantitative tools. Moreover, we followed a sequential exploratory design. This process entailed that the first phase of our work would be dedicated to the qualitative data collection and analysis of strategic documents, while the second phase consisted in using a quantitative tool, namely the lexicometry software TXM, to detect the direction to which the cyberdiscourse was leaning. The second phase builds on the results found in the first, hence the name exploratory (Creswell and Creswell 2009:211). As our work was based on the study cases of two countries, France and Italy, the final stage also involved a comparative analysis.

At the end of our analysis we found different results:

(1) France and Italy did securitize their cyberspaces to assert their national interest, but for different reasons.
(2) The French discourse on cyberspace does lean towards hypersecuritization and has adopted a power-sovereign type cyberdoctrine
(3) The Italian discourse on cyberspace does not lean towards technification and does not belong solely to the technical type.

For the first hypothesis, as we have concluded in the comparison section, both countries have been using their national interest to start the implementation of a cyberstrategy, but to different ends. We explained that the starting point was the wave of attacks on Estonia, and that the idea of being paralyzed as the Estonian systems were in 2007 pushed France and Italy to devise a comprehensive cyberstrategy. Furthermore, our results for the second and the third hypotheses were divergent. While the second hypothesis was confirmed by the two steps-analysis, qualitative and quantitative, the third hypothesis ended up distorted. There are multiple reasons, that we will explain by exposing the limits of our work.

First, there are limitations to our methodology. One of the main criticisms concerns our mixed-methodological approach. Indeed, conducting both qualitative and quantitative analyses requires considerable time. In that matter, the preparation of the texts for the lexicometry software was time-consuming and invisible to the eye of the reader. This proves to be even more frustrating when the analysis does not bear its fruits, as was the case with Italy. Moreover, the case study can also entail case-selection bias, and therefore, abstracted results from these methods cannot provide us with generalizations, especially as we have only selected two cases. Another criticism that could be raised against our methodology could be the split we made in the qualitative part. Indeed, it may appear too descriptive at a first glance. Nevertheless, we think this cut was more appropriate insofar as it accounted for the evolution of each country's cyberstrategy by reaching for their bedrocks.

Secondly, our theoretical basis could also be criticized. Indeed, even if Baumard and Nissenbaum gave us the key components to build our framework, one could argue that the selection we have made is partly biased. However, this criticism also proves to be the most bold and innovative part of our work, as we set up a dual analysis.

Thirdly, the empirical part may be the weak point of our thesis, at least for the Italian qualitative case. As it turned out, the results for the Italian case were not what we had expected for the quantitative part. The reasons of this misrepresentation between the quantitative part and qualitative part may be related to several factors. One could be the low number of documents and their short length. Another factor could be a wrong selection of words in Italian. We are not native speakers; thus, it may be that we lack the perception of a native person.

Nevertheless, we argue that our work still contributes to the flourishing field of cybersecurity studies and allows to update data on a phenomenon which is still not widely addressed.

For this reason, we want to highlight several elements that were complicating our research. First, the availability. Unlike the French case, it was harder to find relevant and comprehensive documents for the Italian case. The French White papers are clear and straight forward while the Italian documents were vague and far from the details of the French ones.

This may be linked to the various reasons. First, the Italian cybersecurity field started properly in 2013 while in France the first White Paper was released in 2008. This delay may be a factor. Second, as we have already mentioned it, maybe it is part of the Italian strategy to not show its

capabilities to the world. Indeed, we had all the budgets and workforce amount for the French case, while we only got one figure for the Italian case, and we are unaware to which branch of the Italian cybersecurity it would be allocated. Third, it may also partly be due to the fact that we decided to only use documents issued by the main representative of cybersecurity for the Italian government, namely the SISR.

Over a longer time span, we would have added further documents to the Italian analysis. For instance, it would have been interesting to link the annual *Relationze al Parlamento* to our analysis, especially to the lexical one, as these documents display interesting discourse elements. However, there are even more instrumental documents for the Italian strategy. However, the limits of our subject have kept us from such endeavor, as it could be the topic of an entire thesis. This bring us to the further avenues for the research.

The cyber-related studies are flourishing alongside the expansion of our use of ICT technologies. Every single item we add to the collection of this interconnected world could be the subject of a thesis on his own.

As we stated, because we wanted to stay within a governmental framework, we did not pick the Cyber Intelligence and Information Security (CIS) reports elaborated by the *Università Sapienza di Roma*. Nonetheless, these reports, and especially the last White paper, contain the future orientations of the Italian strategy. Even within an Italian perspective, it would be stimulating to study the impact of the private sector, whose importance was highlighted during the analysis, as well as the impact of the research sectors. For the latter, we think it would bear even more results because of two factors. First, the willingness of Italy to base its cyberstrategy on a private-public-partnership that was put forward from the beginning. Second, proof of the importance of the research within the Italian cyberstrategy is the agreement reached in February 2017 between the National Interuniversity Consortium for Informatics (CINI) and the National Research Council (CNR) and giving birth to the National Committee for Cybersecurity Research[41]. Last but not least, Roberto Baldoni, Head of the CIS department at the *Università Sapienza di Roma* and head of the CINI was appointed vice-president of the DIS. This is the ultimate evidence that shows how crucial the research in the Italian decision making in terms of cybersecurity has become (Valentini 2017).

[41] No official translation.

In conclusion, many contextual events must be faced by both countries. From a legal point of view, both countries have to implement the NIS directive and the General Data Protection Regulation (GDPR) (EU) 2016/679 (European Parliament 2016; The European Commission 2018). From a political perspective, the Italian elections gave Italy a new government which may have other priorities than securing the cyberspace, while in France, the new LPM was approved by the Senate, while the amount suggested already raises questions among the political sphere (Reuters 2018). Only the future knows where cybersecurity is headed.

Appendixes

Appendix 1 Table of Figures

Appendix 2 Table of Tables

Appendix 3 Analytical Framework of the French cybersecurity landscape

	THEME AND CRITERIA	Yes/No/Partial
Legal foundations	1. Is there a national cybersecurity strategy in place?	✓
	2. What year was the national cybersecurity strategy adopted?	**2011**
	3. Is there a critical infrastructure protection (CIP) strategy or plan in place?	×
	4. Is there legislation/policy that requires the establishment of a written information security plan?	×
	5. Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✓
	6. Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✓
	7. Is there legislation/policy that requires (at least) an annual cybersecurity audit?	×
	8. Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	×
	9. Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✓
	10. Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	×
	11. Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	×
	12. Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	Partial
Operational entities	1. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✓
	2. What year was the computer emergency response team (CERT) established?	**2008**
	3. Is there a national competent authority for network and information security (NIS)?	✓
	4. Is there an incident reporting platform for collecting cybersecurity incident data?	✓
	5. Are national cybersecurity exercises conducted?	✓
	6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	×
Public-Private Partnerships	1. Is there a defined public-private partnership (PPP) for cyber-security	×
	2. Is industry organised (i.e. business or industry cybersecurity councils)?	×
	3. Are new public-private partnerships in planning or underway (if so, which focus area)?	Partial
Sector-specific cybersecurity plans	1. Is there a joint public-private sector plan that addresses cybersecurity?	✓
	2. Have sector-specific security priorities been defined?	×
	3. Have any sector-specific cybersecurity risk assessments been conducted?	×
Education	1. Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✓

Note: table extracted from Alliance (2015)

Appendix 4 Analytical Framework of the Italian cybersecurity landscape

	THEME AND CRITERIA	Yes/No/Partial
Legal foundations	1. Is there a national cybersecurity strategy in place?	✓
	2. What year was the national cybersecurity strategy adopted?	**2014**
	3. Is there a critical infrastructure protection (CIP) strategy or plan in place?	✓
	4. Is there legislation/policy that requires the establishment of a written information security plan?	×
	5. Is there legislation/policy that requires an inventory of “systems" and the classification of data?	✓
	6. Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✓
	7. Is there legislation/policy that requires (at least) an annual cybersecurity audit?	×
	8. Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✓
	9. Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	×
	10. Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	×
	11. Does legislation/policy include an appropriate definition for “critical infrastructure protection" (CIP)?	✓
	12. Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✓
Operational entities	1. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✓
	2. What year was the computer emergency response team (CERT) established?	**2014**
	3. Is there a national competent authority for network and information security (NIS)?	✓
	4. Is there an incident reporting platform for collecting cybersecurity incident data?	✓
	5. Are national cybersecurity exercises conducted?	✓
	6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✓
Public-Private Partnerships	1. Is there a defined public-private partnership (PPP) for cyber-security	Partial
	2. Is industry organised (i.e. business or industry cybersecurity councils)?	Partial
	3. Are new public-private partnerships in planning or underway (if so, which focus area)?	Partial
Sector-specific cybersecurity plans	1. Is there a joint public-private sector plan that addresses cybersecurity?	×
	2. Have sector-specific security priorities been defined?	×
	3. Have any sector-specific cybersecurity risk assessments been conducted?	×
Education	1. Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✓

Note: table extracted from Alliance (2015)

Appendix 5 Future Analytical Framework designed by the ITU (2018)

Models / Tools	Geographic Focus		Target Strategy Applicability		Areas of improvement		Linkage/reference to other models		Designed for assessing improvements
	Global	Regional	New	Existing	Identify	Address	Global	Regional	Indicators
ITU National Cyber Security Toolkit (This project)	X	X	X	X	X	X	X	X	X
ITU - National Cybersecurity Strategy Guide (2011)	**X**		**X**						
Oxford Martin School - Cyber Capability Maturity Model (2014)				**X**	**X**				
CTO - Commonwealth Approach For Developing National Cyber Security Strategies (2014)		**X**							
Microsoft - Developing a National Strategy for Cybersecurity (2013)			**X**						
CCDCOE - National Cyber Security Framework Manual (2012)	**X**		**X**						
OECD - Cybersecurity Policy Making at a Turning Point (2012)			**X**						
OAS - Cyber Security Program (2004)		**X**	**X**						

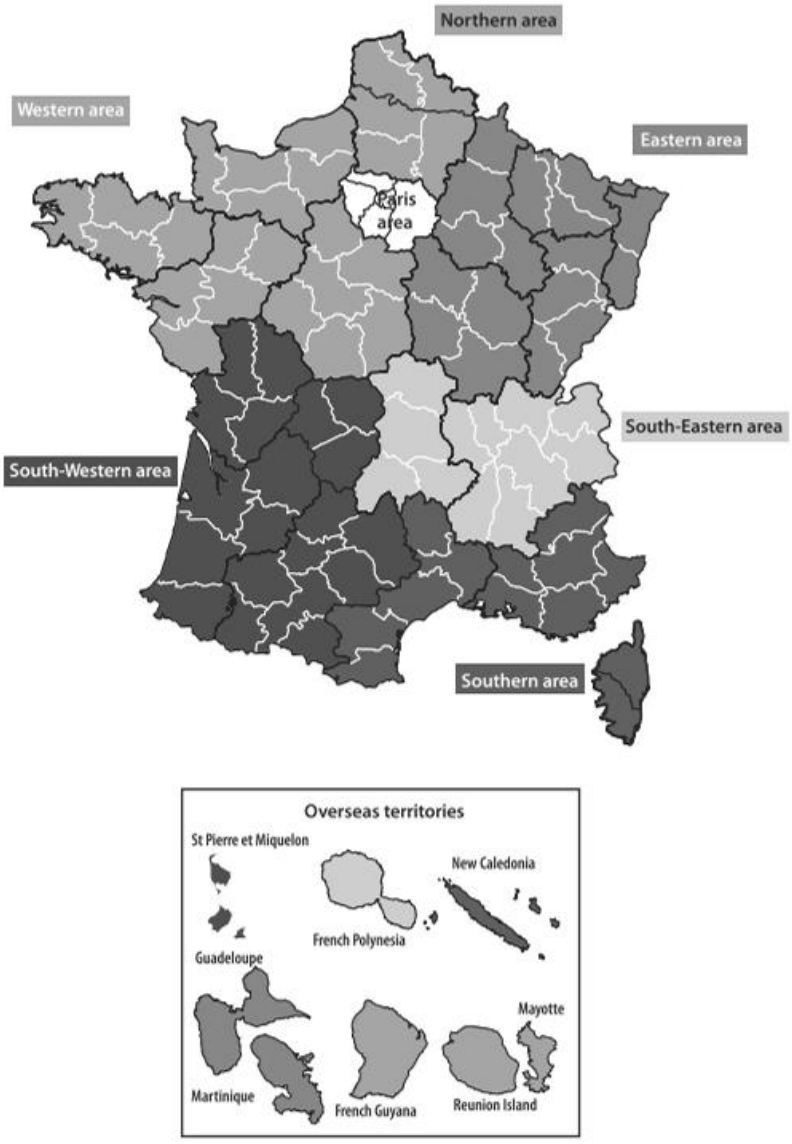
Note: table extracted from ITU (2018)

Appendix 6 An ideal type of securitization.

Key concept(s)	What do they refer to?
Intersubjectivity	▪ Threats are social facts whose status depends on an **intersubjective** commitment between an audience and a securitizing actor
Securitizing moves & context	▪ **Securitizing moves** and **context** are co-dependent
Knowledge & existential threat	▪ The drivers of securitizing moves are **knowledge** claims about an **existential threat** to a referent object
Power relations	▪ **Power relations** amongst stakeholders structure both the processes and outcomes of securitizing move
Social mechanisms	▪ Securitizing moves are engraved in **social mechanisms** (persuasion, propaganda, learning, socialization, practices, etc.)
Policy	▪ Securitization instantiates **policy** changes – for example, 'deontic powers' (rights, obligations, derogations exceptional or otherwise, etc.)
Responsibility	▪ Securitization ascribes responsibility

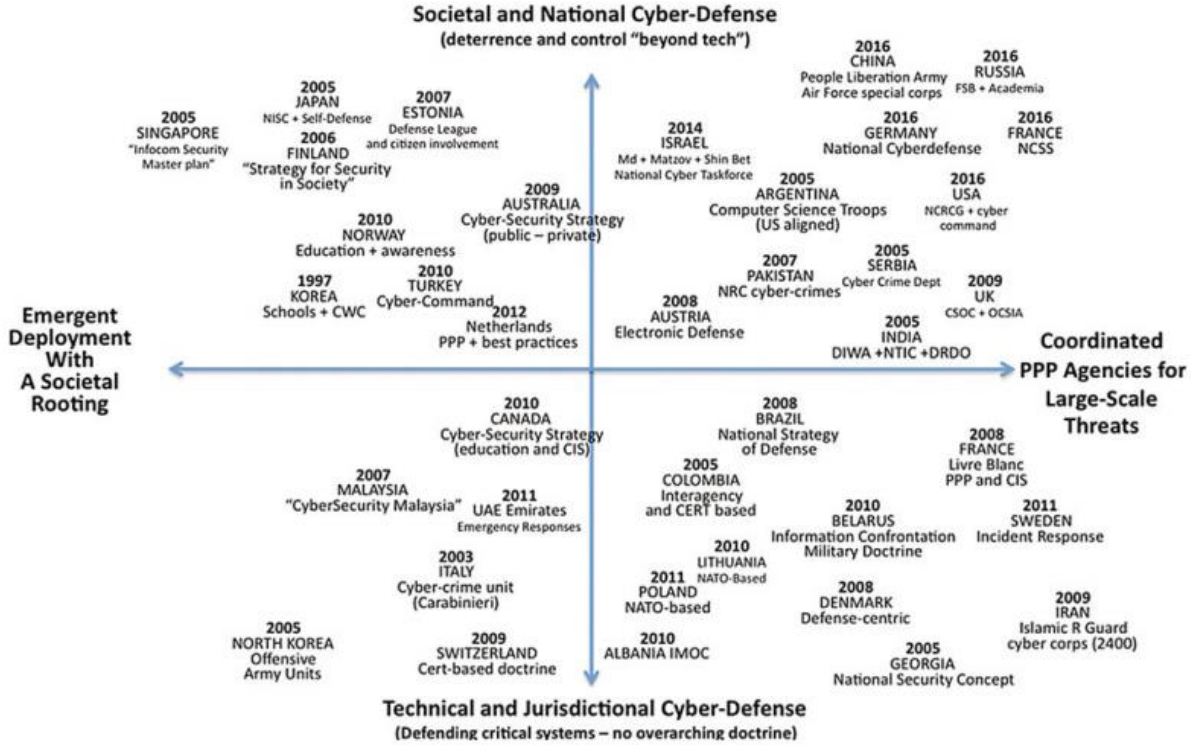
Note: table extracted from Balzacq (2015:105)

Appendix 7 Defense and security zones



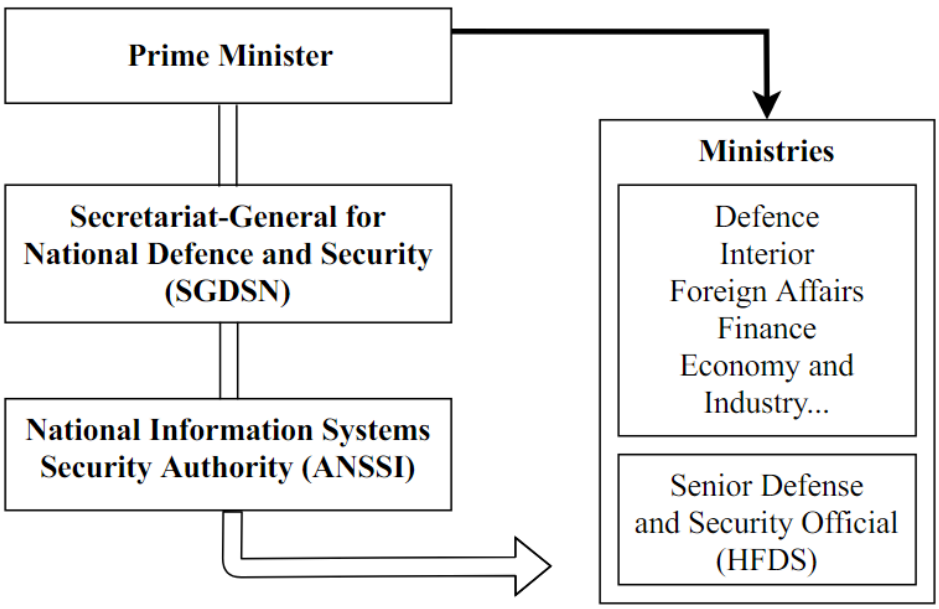
Note: figure adapted from Mallet, France, and France (2008:173)

Appendix 8 Baumard's analysis results on national cyber-crime doctrines (1994-2007)



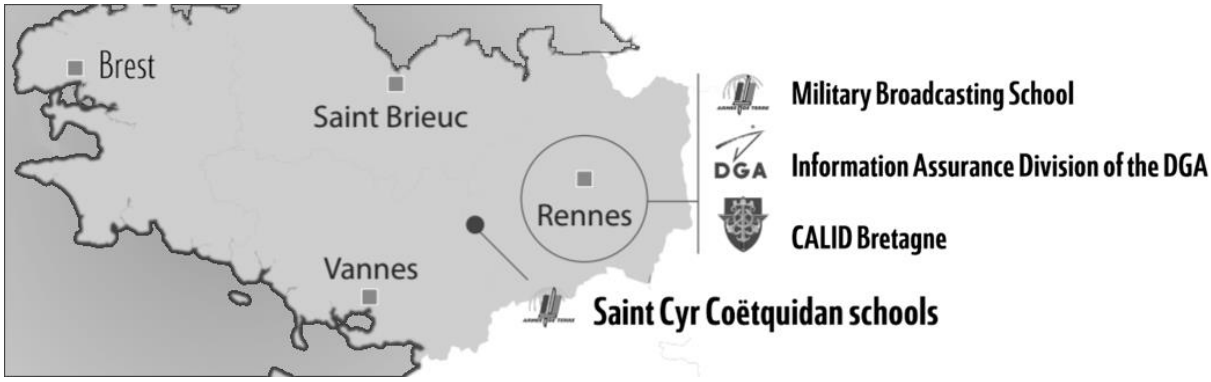
Note: figure extracted from Baumard (2017:69)

Appendix 9 ANSSI**'s** organization chart



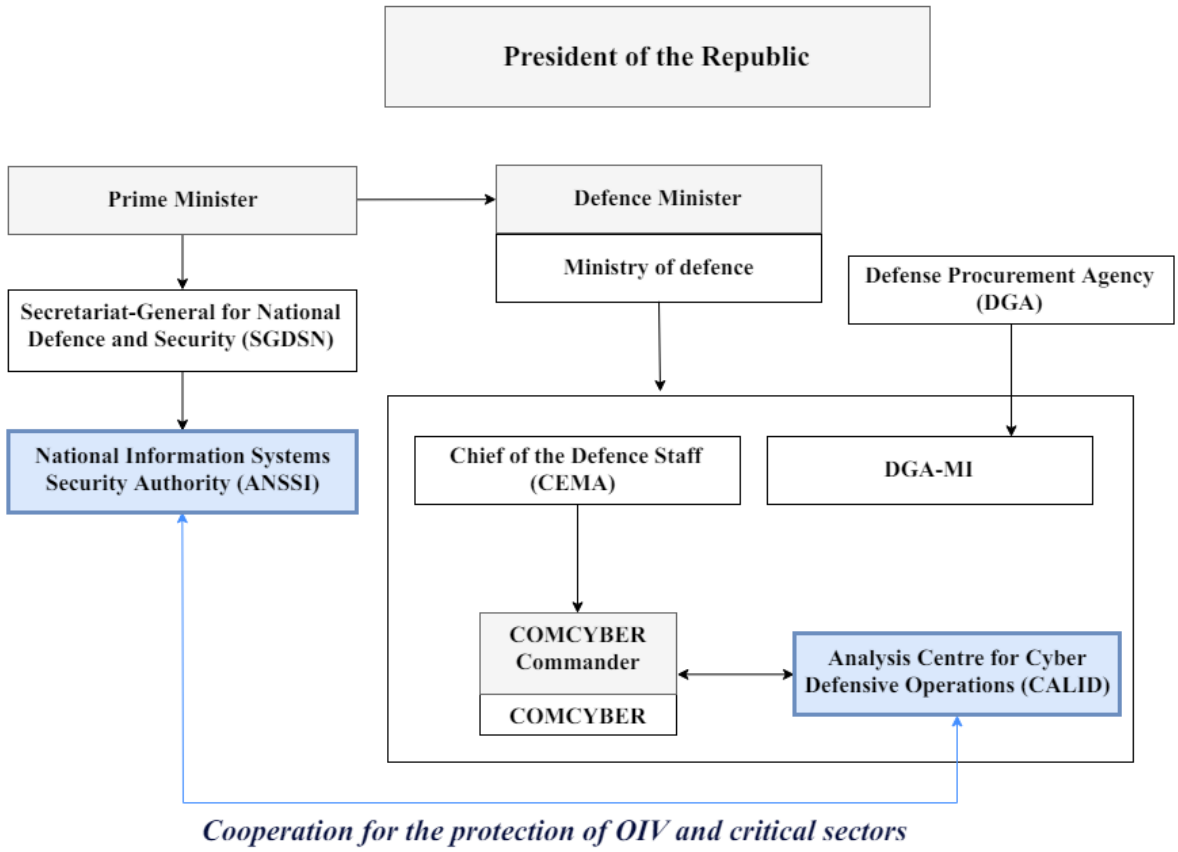
Note: figure adapted from the ANSSI website (2018)

Appendix 10 Map of Brittany displaying the cyberdefence center of excellence



Note: figure adapted from Ministry of Defense (2014:12)

Appendix 11 Organization of the French cyberdefence



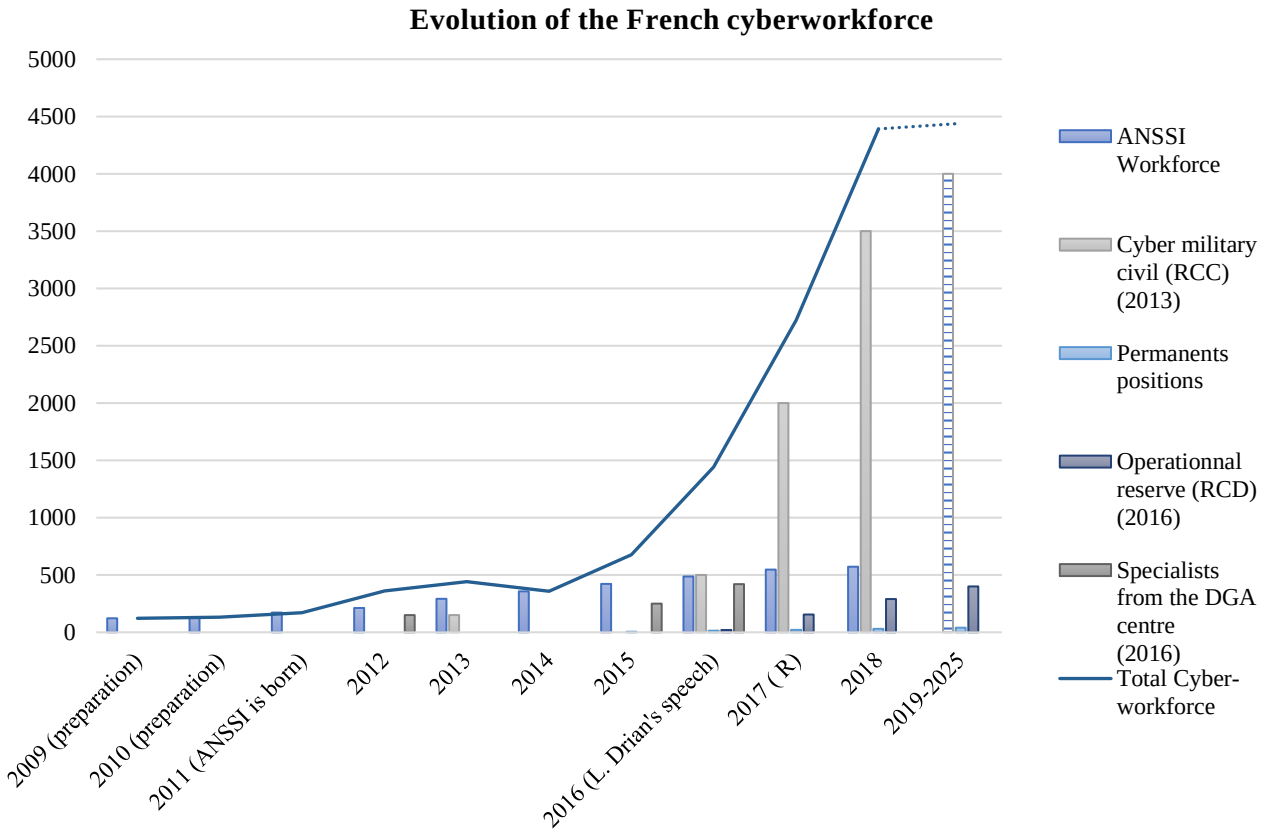
Note: figure elaborated by our care from the information in ANSSI (2018).

Appendix 12 Evolution of the French cyberworforce

Note: figure elaborated by our care from the information in ANSSI (2018).

Year	ANSSI Workforce	Reserve (together after 2016)			Specialists from the DGA centre (2016)	Total Cyber-workforce
		Cyber military civil (RCC) (2013)	Permanents positions	Operationnal reserve (RCD) (2016)		
2009 (preparation)	122					122
2010 (preparation)	132					132
2011 (ANSSI is born)	172					172
2012	212				150	362
2013	292	150			*no data a.*	442
2014	357	*no data a.*			*no data a.*	357
2015	422	*no data a.*	5		250	677
2016 (L. Drian's speech)	487	500	14	20	420	1441
2017	547	2000	21	155	520 (p)	2723
2018	572	3500	30	290		4392
2019-2025		4000	40	400	650 (p)	4440

no data a.	*No data available*
	Previsions



Note: figure elaborated by our care from the documents and white papers used in the French analysis.

Appendix 13 French cyberdoctrine framework

Societal (I)	Technocrat (II)	Power-sovereign (III)	National interest
Actions falling under the societal rooting such as • Sensitive to opinion movements; • influence of the public space actors (including. hacking civil groups) to a certain extent Europe; • Have an "information warfare" active component; • Weak or borrowed national vision • Inclusion of the society through awareness campaign or good practices diffusion • Education	Actions falling under the technical and jurisdictional cyberdefence • incident-Response philosophies; • technocratic and delayed perception (also offensive) • domination of the technical expertise (ie. Police); • vertical walls and jurisdictional response;	Actions falling under the national cyberdefence: • Creation or expansion of large specialized units or military corps; • Obsessed with critical infrastructures; • development of offensive and defensive capabilities;	Delimitation of the geopolitical, economic and information assets of a country viewed as critical sectors Threats to: - the sovereignty, - survival of the state, - cyberspace and its components,

List of the selected texts (texts selected for TXM are in bold):

1. **2008 – White Paper (WP)**
2. **2011 – Information System Defence and Security (ISDS)**
3. **2013 – White Paper (WP)**
4. 2014 - Cyberdefence Pact
5. **2015 - National Digital Security Strategy**
6. 2016 - Le Drian's speech
7. **2017 - Defence and National Security Strategic Review (DNSSR)**
8. **2018 - Strategic Review of Cyber Defence**[42]

[42] Restriction to List Chapter 3 -11 and 11 for WP 2008, as the rest of the paper is dedicated to Defense in a broad sense.

	Societal (I)	Technocrat (II)	Power-sovereign (III)	National interest
2008	**5 main strategic functions: knowledge and anticipation, deterrence, protection, prevention and intervention**			
2008 WP (1)		• Adoption of very high-security products to protect State secrets guaranteed "trusted products and services" • Enhance expertise in the cyberfield, with more personnel in the ministries and create a reservoir of competencies • Setting up of a nationwide network of experts in information system security observatories in the defence and security zones • Make any actions in compliance with the French legislation	• Effort to make the Internet more resilient • Creation of the ANSSI • Protection of the information systems • Definition of the French critical sectors (Regulation of 2 June 2006) and inclusion of the cyberspace within these • Formulation of a body of doctrine for offensive cyber-war capabilities • Development of an array of tools to protect critical information systems: o Early-warning systems to detect cyber-attacks o Setting up of a detection center o Security products and trust networks	• Definition of map of the defense and security zones covered, namely seven national zones and five overseas areas • Develop the surveillance of national spaces and those in which France has interests, including outer space. • Definition of the "Internet" as critical infrastructure • Definition of the French critical sectors (Regulation of 2 June 2006) and inclusion of the cyberspace inside these • Introduction of the concept of national security (Law of 20 July 2009) • Defense of the national interest through intervention and (nuclear) deterrence
2009	**France's return to the NATO Integrated Military Command Structures**			
2011 ISDS (2)	<u>For citizens:</u> • Strengthen its operational partnerships with its closest allies (p.11) and promote the sharing of essential data with them • Ensure that the field of information systems security remains attractive for young	• strengthen or enact legal rules in cyberspace • formulating cyberdefence policies within international organizations • implementation of EU law inside the national law	• ANSSI becomes the national authority in charge of information systems defence • protecting public cyberspace (interesting distinction between public and private) • creation of an "operation room" for the ANSSI	

	graduates to prevent the gradual erosion of our expertise (p.12) and to expand the pool of expertise available in the country (WP 08) <u>For the administration:</u> • Promote safe and confidential way of communication in both administrations and public spheres (p.12) <u>For the private sector:</u> • providing companies and individuals with good practices • Project of a cyberdefence research centre in collaboration with industrial partners • Promote industrial strengthening using State resource, in particular through strategic investment funds. • Setting up of a public-private-partnership to share state's expertise on threats analysis against new technologies protection from the private sector (p.17)	• promote international judicial cooperation on repression of offences committed on or through electronic communication networks • Monitoring updates and security breaches in the software • adoption of the General Security Framework (RGS) (2010) • (WP 08) Redefinition of the French strategy on security products and components • (WP 08) introduction of robust authentication systems based • (WP 08) use of cryptography techniques • (WP 08) secured governments networks (interdepartmental intranet, high availability and encrypted telephone network)	• (WP 08) Acquiring a cyberdefence capability • (WP 08) conceal the «information related to our sovereignty" • (WP 08) protecting the operators of critical infrastructures, electronic communication networks and securing the core systems of critical infrastructures' operators (p.13)	
2013	**States acknowledged that far from being a space without rules, cyberspace was governed by existing international law**			

2013 WP (3)	• Establishment of a general, inter-ministerial contract defining the civilian capacities required for missions relative to national security by the SGDSN • Development of policy of awareness-building directed at decentralized state administrations, regional authorities and their public establishments and at the principal users of the cyberspace	• Reinforce the obligations [legal] of operators of vitally important services and infrastructure to detect, notify and deal with any IT incident affecting their sensitive systems. • (ISDS 2011) Improve the consistency between the domestic and the Union legislation • Definition by the state of security standards for activities of vital importance for the normal functioning of the nation: o ensuring that operators adopt all necessary measures to detect and handle any such incident affecting their sensitive systems o specifying the rights and obligations of public and private actors, particularly in relation to audits, the mapping of their information systems, notification of incidents and the capacity of the ANSSI, and, where applicable, of other state agencies, to intervene in the event of a serious crisis.	• Upgrade very significantly the level of security of information systems and the means for defending them • Develop the capacity to detect attacks in cyberspace • Creation of a cyber-defense unit within the operational reserve which would constitute an enhanced cyber-defence capacity in the event of a major IT attack. • Identification of all the critical capabilities by the SGDSN • Incorporation of an operational cyber-defence platform within the armed forces	• Sovereignty and international legitimacy are two essential and complementary pillars of strategy for defence and national security • Protecting the national territory, fellow citizens and the continuity of the Nation's essential functions are core to French defence and national security strategy • Defense of the national interest through intervention and (nuclear) deterrence • Components of the national sovereignty: o capacity to detect and protect ourselves against cyber-attacks and to identify those responsible for them o capacity to produce security systems, on a fully autonomous basis, notably in the fields of cryptology and attack detection • States developing offensive IT capabilities are seen as a direct threat to essential institutions, companies and sectors for the Nations' life (consequently to threat to the national interest)

2014 Cyberdefence Pact (4)	• Support small and medium enterprises (SMEs) through the job creation program, RAPID, set in motion by the Defence Procurement Agency (DGA) • Support the ANSSI in assisting the largest defense industries if they undergo an attack	• Strengthen the technical expertise (knowledge sharing, crisis management training) of the Brittany excellence center drawing upon the Information Assurance Division of the DGA (DGA-MI) building on the local branch of the Analysis Centre for Cyber Defensive Operations (CALID) • Develop legal expertise in the cyberdefence field to give armed forces a solid legal framework	• Improve the defensive stance and reorganization of the cyberdefence through the Director of the Defence Information and Communication Systems (DGSIC) • Strengthen the responsive stance by improving the operational cyberdefence capacities of the Planning and Operations Centre (CPCO) created in 2011 and spreading them through all the components of the Ministry • Develop a new range of cybersecurity tools, both hardware and software, to improve cyberdefence of the armed force • Fostering research activities and creation of a center of excellence in Brittany • Develop the exchange between the cyberdefence community and the national services and foster the cyberdefence spirit between the army, the ANSSI, the DGA and the operational reserve • Deepen the partnerships with our main allies and play an active role within international arenas (UE, NATO) to improve our collective security	

2015 national digital security strategy (5)	• Raise the awareness of all French people
	  ○ Creation of an educational website (CyberEdu)
	• integrate "cybersecurity awareness into all higher and continuing education programmes" and "cybersecurity training into all higher education that includes some information technology" (SecNumedu)
	• Inform citizens of the risks of manipulation and propaganda techniques used by malicious players on the Internet. (e.g.: platform post Paris attacks) [duty of the state]
	• Provide local assistance to victims of cybermalevolent acts
	• Put in place indicators to measure cybercrime
	• Transferring acquired knowledge to the private sector to contribute to the handling of its cybersecurity
		• Adapt the legal framework to new technologies
		• Extend the framework applied to operators of vital importance (OIV) to other operators both public and private participating in these sensitive information systems
		• Pursue the State Information Systems Security Policy (2010)
		• Reinforcing the operational mechanisms of legal international mutual aid and universalizing the principles of the Budapest Convention on Cybercrime.
		• Implementation of the European regulation on electronic identification (eIDAS - Electronic Identification and Trust Services)
		• Reassertion of the right to privacy for individual and collective control of personal data
			• creation of an expert panel for digital trust placed under the supervision of the ANSSI and the SGDSN
			• Active monitoring of threats and security breaches for French authorities (ministries, businesses, and other territorial administrations)
			• Reinforce the security of its critical networks and its resilience
			• Extend cybersecurity crises management exercises over the national territory
			• Support the development of the cyber operational reserve
			• Support for the development of French cybersecurity solutions
			• Reinforcing French presence and influence in the international discussions on cybersecurity
			  ○ increase its investment in more informal international forums in which the technical and academic communities and the political decision-makers come together to discuss the future balances.
			  ○ Intensification of the participation in multilateral negotiations on cybersecurity (UNO, OSCE)
			  ○ Reinforcement of bilateral contacts, notably inter-ministerial diplomatic dialogue
				• Cyberattacks threaten French fundamental interests
				• Extension of the definition of critical infrastructures now intended as "operators of vital importance or strategic businesses"
				• New threats:
				  ○ Opinions spread on the Internet go against France's fundamental interests and are an attack on defence and national security
				  ○ Increasing number of countries declaring themselves equipped with offensive capabilities,
				  ○ The level of conflict between States is increasingly being expressed in cyberspace
				• For the protection of its sovereignty and notably the protection of its information concerning the national defence secret, France will preserve its financial and industrial capacity to develop solutions with the highest levels of security

2016
Le Drian's speech (6)
			• Establishment of a cyber commandment called COMCYBER/CYBERCOM working hand in hand with:
			  ○ the head of ANSSI for all the matters revolving around the protection of the vital infrastructures (such as the OIVs),
			  ○ the DGA delegate (SGA) for all technical engineering and technological equipment procurement.
			• Call for a new doctrine for the cyberfield
			• Division of the army's action in the cyberdefense field into three categories: intelligence and investigation; protection and defense; and riposte/response and neutralization
			• Increase the global cyber workforce in the different French services to 3200
			• Increase the people from the two reserves to 4400, namely the cyber military civil reserve and the operational reserve people
				• CYBERCOM in order to "maintain France's sovereignty and stay master of its destiny" working hand in hand with:
				• Reassertion of the nuclear deterrence
				• Actions taken for the cyberfield allows to assert French interests in this new space of confrontation [cyberspace]

2017 DNSSR (7)		• A new provision states that actions occurring within the digital framework do not engage the criminal accountability of the military personal.	• Development of a cyber resilience through the reinforcement of the ANSSI which is granted the right: ○ to ask electronic communications operators to examine evidence of computer attacks; ○ to compel the aforesaid operators to warn their subscribers or users of potential breaches; ○ to investigate and ask the operators for access to their data when OIV or public administration networks are threatened; ○ access to technical data only gathered by the detection systems of the operators; ○ to set up detection mechanisms directly at the host website or on the electronic communications operator's networks when a potential threat against OIV or public administration networks is known; again, this only concerns technical data • Government can modify the conditions in which the ANSSI intervene for the monitoring missions quoted above	• Definition of French's interests as all factors that contribute to its security, prosperity, and influence • Integrity of the territory and the protection of the population are central to the vital interests but: ○ Interests are not carved in stone ○ One duty of the President is to set them through time • Preservation of the national interests remains based the nuclear deterrence, both airborne and maritime • National interests encompass both traditional interests (territory and population lives) and shared interests, which themselves would be divided in different categories such as European interests and global interests/global commons • France's goal is to reach a stage of strategic autonomy by 2030 • Reassertion of the digital space as a domain of confrontation and emphasis put on the growing role of private actors as "challengers to state sovereignty" that reshape the balance of power between state, non-state, and private-sector actors

2018 Strategic Review of Cyber Defence (8)	<u>French cyber action at the international level:</u> • Supervision of the activity of private actors in cyberspace: o Launch of a French initiative in the framework of the G20 in to regulate private sector activities that have an impact on the on international cyberspace security o Promote the prohibition of Hackback by actors of the private sector in cyberspace o Establish a principle of responsibility at the international level the security of systemic private actors for the design and maintenance of their products and services digital • Strengthening the fight against cybercrime o Conduct a reflection on the relevance of investigating cybercrime more systematically, including in the absence of a	• Improving the certification framework to improve product safety o Introduction of basic cybersecurity certification based on the "CE" marking required for the marketing of certain goods or services within the European area.	• Consolidate the French cybersecurity organization: o Set up four operational chains: protection, military action, intelligence and legal investigation (instead of the three established in Le Drian's speech) o Setting up of a Cyberdefence Management Committee responsible for the implementation of decisions regarding the development and the general organization of the field taken by the High Council of National Defence (CSDN) o Establish a Cyberdefence Steering Committee dedicated to the improvement of the knowledge of cyberthreats; the elaboration of an industrial, regulatory and normative policy on digital/cyber sovereignty; o Design an official global response doctrine to face cybercrisis. o Establish a coordination center for the cyber crises (C4) dedicated to minor crises management • Strengthening the securing of State's information systems protection o Submit for approval the most important and sensible computer projects to the state as soon as their star-up phase has begun	• Digital sovereignty is conceived as an essential component of national sovereignty • Encryption of communications, detection of cyberattacks and professional mobile radios are key technologies necessary to our [French] digital sovereignty

	complaint, when the information gathered suggests the likely existence of criminal offences o Hinder action against the most popular criminal platforms in order to reduce the sense of impunity that drives a number of cybercriminals o Development of an active collaboration network between magistrates and investigators both at European and international levels • Promote responsible standards of behaviour in cyberspace: o Strengthen export control mechanisms in the cyber domain for the most dangerous elements o Creation, at French or European level, of an international think tank dedicated to geostrategic and legal cyber defence issues within which France's ideas could echo		o Gradual junction of all ministries to the inter-ministerial network of the State (RIE) access platform (protection of State information systems) o Impose the overall coverage of the computer services used by state through a safety oversight mechanism, including the cases in which services are outsourced, and allow ANSSI to impose specific rules (implementation of detection mechanisms) to this end • Strengthening the securing of the OIV o Strengthening the requirement security level that apply to OIV and electronic communication and electric energy supply sectors • Strengthening the securing of core activities o Common set of minimum safety rules to protect actors supplying core services o Search for harmony within the EU on the rules of cybersecurity applied to core services providers • Increased involvement of electronic communications operators and hosting providers o Allow the ANSSI to rely on detection systems implemented by the operators of electronic communications to detect attacks	

	<u>Cybereconomy</u>: • Establish a global trust framework to guide the market for products qualified as SecNumCloud • Encourage major French manufacturers to complete their offer products and services for the civilian sector, in order to that they become international champions of the cybersecurity capable of competing with the giants of the American, Russian, Chinese or Israeli cyber security. • Support for SMEs' external growth strategies dedicated to cyberdefense by the mobilization of investment funds interested in the cyberdefense to foster creation of French medium-sized companies in this sector. • Support for the setting up of accelerators, start-ups studios and more generally structures to support start-ups dedicated to cyberdefense, by concentrating efforts on innovative companies		○ Allow the ANSSI, when aware of a particularly serious threat, to set up on a communications operator's network or information system of a hosting provider, a local and temporary detection device • Improvement of the cyber-protection of local authorities ○ Support the creation by local authorities of a network of cybersecurity correspondents ○ Improve the integration of needs and constraints specific to local authorities in the ANSSI reference frameworks and in its catalogues of products and services qualified • Definition of a doctrine of action in the face of a cyber-attack ○ Adoption of an attack classification scheme of computer systems. ○ Definition of response options to cyber incidents. • Structuring an industrial digital policy based on mastering key technologies: ○ Setting up an inter-ministerial team in charge of analyzing key technologies and developing trust solutions in conjunction with industrialists (technological watch and proposal of	

	which strategy can enable them to reach a footprint worldwide. <u>Cyber risks management</u>: • Support for taking into account the private sector dealing with cyber issues o Support the emergence of national or European actors of cyber rating. o Study the support for the development of a relevant cyber insurance mechanism by helping to better assess risks. o Support the implementation of a cyber risk valuation within accounting standards and its inclusion in accounting and financial documents. • Strengthening our trusted national industrial base in cyber defence o Carry out and maintain an industrial mapping o Support the emergence of at least one national reference industrial player in the field of threat analysis		choices dedicated to the emergence of key technologies, etc.). o Maintaining a national industry at the forefront in the field of communications encryption. o Development of a new generation of radios for the benefit of the security forces, and rescue units o Support research and development in the field of artificial intelligence applied to cyber defense • Secure communications: o Identify a critical component controlled by France and integrated in terminal equipment to be able to make secure mobile telephony o Develop encryption and software partitioning techniques o Study new professional radio related services based on civil (5^{th} G) technologies to bring resilience	

	and the development of markers capable of competing with major American, Russian and Israeli companies in the field. <u>Education and human stakes</u>**:** • Integration of cybersecurity rules in the learning transmitted by the School from the elementary school to the final year class of high school o Digital education including mastery of cybersecurity requirements in elementary, middle and all high school curricula. o MOOCS [43] on the transmission of cybersecurity rules dedicated to teachers in initial and in-service training designed by the Ministry of National Education with the strong support of the ANSSI.			

[43] Massive Open Online Courses

	• Dissemination of the culture of the digital security across the whole society o Creation by the ANSSI of a fun application, available on smartphone, allowing the French to test their level of knowledge in the field of safety culture and offering them many challenges o Study the contribution of nudges for the development of citizens' autonomy in cybersecurity. o Inclusion of a cybersecurity dimension in the support program for the digital transformation of businesses in the Ministry of Economy and Finance and Secretariat of state in charge of digital affairs. • Further development of competency management in the State cyber defence services. <u>Cloud:</u> • Invent a valuation strategy for cloud computing: o Establish a comprehensive state policy of cloud use			

	○ Encourage the development of encryption solutions for the cloud ○ Support strategic autonomy in this area.			

Note: table elaborated by our care from the documents and white papers used in the French analysis.

Appendix 14 Codebook updated (France)

Everyday security practices	Technification	Hypersecuritization
community	access	aggression (s)
business(es)	expert(s)	armed force(s)
company (ies)	expertise	attack(s)
competence(s)	framework(s)	authority
connectivity	implementation	awareness
critical sectors	knowledge	capability(ies)
cybersecurity sector	legal	command
data	measures	critical infrastructure(s)
dialogue	measures	cyber-attack(s)
digital sector	mechanism(s)	cyber-defence (-)
economic sector	network(s)	cyber-security (-)
education	policy(ies)	defence
energy sector	prevention	destruction
freedom	rule(s)	digital infrastructure
goods	standard(s)	doctrine
individual(s)	technical	essential infrastructure
industrial/industry (es)		government
sector		information system(s)
interdependence		land infrastructure
population (see in context)		military force(s)
private actors/operators/		nation
sector(s)/ stakeholders		protection
public action/		resilience
administration/ authorities/		state
sector/ security/sector		terrorist(s)
society		vital infrastructure
stakeholder(s)		war
training		warfare
vulnerability (ies)		

Note: table elaborated based on the Klingova (2013) codebook and by our care from the documents and white papers used in the French analysis.

Appendix 15 Tables of selected words (a)-(b)-(c) – French case

a) Selected words for the cyberdiscourse type everyday security practices

word	2008	2011	2013	2015	2017	2018	Total
community	2	0	19	10	9	3	43
business(es)	64	3	1	2	44	7	121
company (ies)	3	9	18	3	10	6	49
competence(s)	0	0	2	4	1	0	7
connectivity	0	0	0	0	3	0	3
critical sectors	1	1	0	0	0	0	2
cybersecurity sector	0	0	0	2	0	0	2
data	5	6	4	39	20	7	81
dialogue	2	0	19	3	6	3	33
digital sector	0	0	0	1	0	0	1
economic sector	0	0	0	1	0	0	1
education	0	1	12	24	6	4	47
energy sector	0	0	0	0	1	0	1
freedom	9	1	18	2	22	0	52
goods	9	0	9	0	2	1	21
individual(s)	8	7	10	8	1	1	35
industrial/industry (es) sector	0	0	1	2	0	0	3
interdependence	0	0	4	0	1	0	5
population (see in context)	28	1	23	1	12	0	65
private actors	1	1	2	0	4	0	8
private operators	2	0	3	1	0	0	6
private sector(s)	2	0	2	7	1	6	18
private stakeholders	0	0	0	1	1	2	4
public action	0	0	4	3	0	0	7
public administration	0	0	2	0	0	1	3
public authorities	1	3	6	1	0	1	12
public sector	0	0	0	0	1	0	1
public security	4	0	1	0	0	0	5
sector	4	1	14	21	8	11	59
society	11	3	12	2	3	7	38
stakeholder(s)	1	1	4	17	7	9	39
training	23	3	43	12	8	4	93
vulnerability (ies)	3	2	4	0	9	0	18
Total occurrences	183	43	237	167	180	73	883

b) Selected words for the cyberdiscourse type technification

word	2008	2011	2013	2015	2017	2018	Total
access	5	3	9	5	14	0	36
expert(s)	7	1	4	6	0	3	21
expertise	3	5	21	1	17	0	47
framework(s)	29	1	57	13	18	10	128
implementation	6	2	24	5	5	4	46
knowledge	14	0	28	5	5	4	56
legal	8	1	8	6	5	1	29
measures	17	3	9	15	5	8	57
measures	17	3	9	15	5	8	57
mechanism(s)	7	2	3	2	3	6	23
network(s)	26	20	19	22	11	8	106
policy(ies)	31	3	82	9	18	3	146
prevention	23	0	33	3	13	3	75
rule(s)	6	3	19	1	7	6	42
standard(s)	4	0	7	0	5	6	22
technical	11	5	22	15	15	4	72
Total occurrences	214	52	354	123	146	74	963

c) Selected words for the cyberdiscourse type hypersecuritiztion

word	2008	2011	2013	2015	2017	2018	Total
aggression (s)	7	0	18	1	8	0	34
armed force(s)	48	0	99	1	44	2	194
attack(s)	34	6	45	8	28	13	134
authority	7	1	16	4	2	5	35
awareness	2	3	7	11	4	2	29
capability(ies)	165	5	143	10	116	7	446
command	33	2	55	1	16	0	107
critical infrastructure(s)	5	9	0	4	1	1	20
cyber-attack(s)	0	2	9	16	5	18	50
cyber-defence (-)	1	7	9	2	0	0	19
cyber-security (-)	0	2	3	49	2	22	78
defence	69	5	266	18	123	21	502
destruction	1	0	16	0	2	0	19
digital infrastructure	0	0	3	0	0	0	3
doctrine	6	0	2	1	4	5	18
essential infrastructure	0	0	8	0	0	0	8
government	40	2	15	4	2	3	66
information system(s)	9	24	16	29	1	4	83
land infrastructure	0	0	1	0	1	0	2
military force(s)	5	0	4	0	5	0	14
nation	11	0	44	5	12	2	74
protection	68	6	73	11	36	7	201
resilience	12	0	11	2	12	3	40
state	29	0	83	30	22	17	181
terrorist(s)	8	2	24	4	23	0	61
vital infrastructure	0	0	3	0	0	0	3
war	4	0	21	1	12	0	38
warfare	5	0	3	0	6	1	15
Total occurrences	569	76	997	212	487	133	2474

Note: tables elaborated by our care from the documents and white papers used in the French analysis and the software TXM.

Appendix 16 Table of the evolution of cyberwords throughout the decade – French case

word	2008	2011	2013	2015	2017	2018	total
cyber	4	0	3	5	4	51	67
cyberattack	0	0	0	5	2	10	17
cyberattacks	0	2	1	11	3	8	25
cyber-attacks	0	0	5	0	0	0	5
cybercrime	0	1	0	7	0	1	9
cyberdefence	0	7	0	2	0	0	9
cyber-defence	1	0	9	0	0	0	10
cybermalevolent	0	0	0	6	0	0	6
cybersecurity	0	2	1	49	2	22	76
cyberspace	0	8	7	32	19	13	79
cyber-threats	0	0	4	0	1	0	5
cyber-war	9	0	0	0	0	0	9
information system	2	0	1	3	0	0	6
information systems	7	24	15	26	1	4	77

Appendix 17 Table of the evolution of cyberdiscourses throughout the decade

Type of cyberdiscourse	2008	2011	2013	2015	2017	2018	Total words		Average words between 2008-2018
Everyday security practices	191	43	247	171	181	73	906		151
Hypersecuritization	574	85	997	216	488	134	2494		415,6666667
Technification	214	52	354	123	146	74	963		160,5
						Total	4363		
Whole discourse	26173	2861	50376	9968	27299	5194	121871		20311,83333

Appendix 18 Concordance table for "fundament/interest(s)"

Queries in TXM:
("interests" []* [word="fundamental"]) | ([word="fundamental"] []* "interests") within 21
("interests" []* [word="france"]) | ([word="france"] []* "interests") within 21

Document	Left	Main idea	Right
2015	[France} is **the target of cyberattacks** that damage its	**fundamental interests**	. today, when an attacker targets the state, operators of
2015	objective france will ensure the defence of its	**fundamental interests**	in **cyberspace**. it will reinforce the digital security of its critical
2015	opinions that are **disseminated [in the cyberspace]** are therefore against france's	**fundamental interests**	and are **an attack on defence and national security** which is sanctioned
2017	a **major cyber threat** would undoubtedly affect our	**interests**; secondly, **france**	intends to fulfill its responsibilities globally, not limiting them to its
2018	critical entities, in order to protect france's	**fundamental interests**	in face of the **cyber threat.** nevertheless, cross-sectoral approaches do

Appendix 19 Concordance table for “protects + interest(s)”

Query in TXM: ("interests" []* [word="protects"]) | ([word="protects"] []* "interests") within 21

Document	Left	Main idea	Right
2013	capability for deterrence and intervention. nuclear deterrence	protects france from any state-led aggression against its vital **interests**	, of whatever origin and in whatever form. it rules out
2017	[nuclear deterrence] the cornerstone of our defence strategy. it	protects us from any aggression against our vital **interests**	emanating from a state, wherever it may come from and whatever

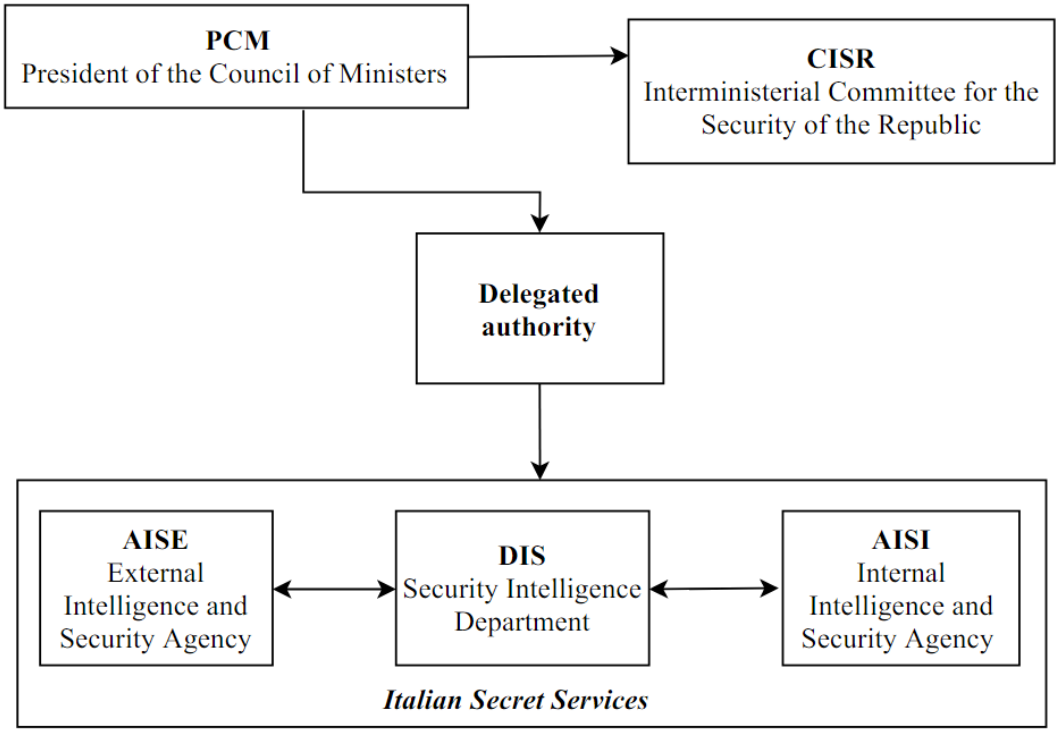
Appendix 20 Concordance table for “protect + system(s)”

Query in TXM: ([word="information"] [word="systems"] []* [word="protect"]) | ([word="protect"] []* [word="information"] [word="systems"]) within 11

Document	Left	Main idea	Right
2008	in the short term acquire reactive capability to	**protect the nation’s information systems**	. early-warning systems will be developed to detect cyber attacks by setting
2011	will enable the enactment of new rules to	**protect information systems**	and alert government authorities in case of incidents. • The enforcement
2013	implementation of a robust and resilient posture to	**protect state information systems**	, operators of essential infrastructure and strategic industries, paired with an
2015	as of 2009 to address cyberattacks and to	**protect the state information systems**	and critical infrastructures. an industrial policy in favour of the national

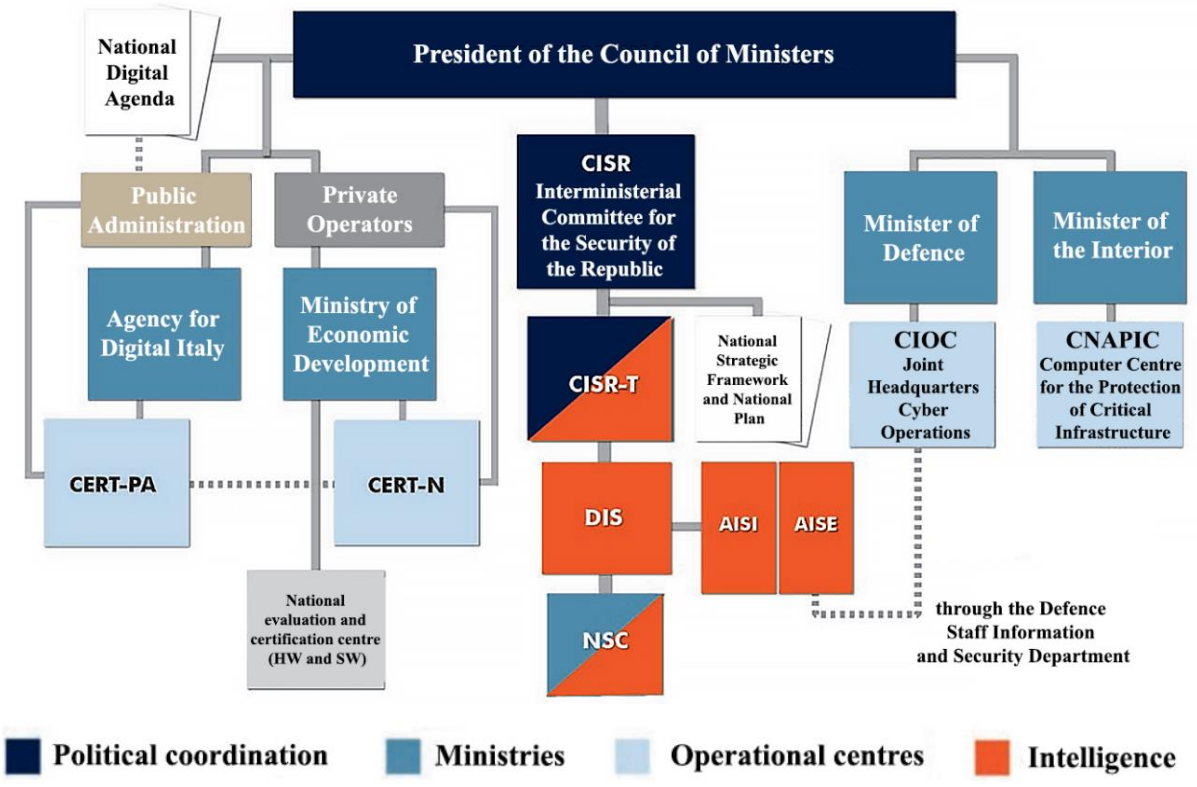
Note: tables elaborated by our care from the documents and white papers used in the French analysis and the software TXM.

Appendix 21 System for the Security of the Italian Republic **(**SISR)



Note: figure adapted from the information in SISR (2007)

Appendix 22 Organization of the cyber Italian architecture



Note: figure adapted and translated from SISR (2018:10)

Appendix 23 Italian cyberdoctrine framework

Societal (I)	Technocrat (II)	Power-sovereign (III)	National interest
Actions falling under the societal rooting such as • Sensitive to opinion movements; • influence of the public space actors (including. hacking civil groups) to a certain extent Europe; • Have an "information warfare" active component; • Weak or borrowed national vision • Inclusion of the society through awareness campaign or good practices diffusion • Education	Actions falling under the technical and jurisdictional cyberdefence • incident-Response philosophies; • technocratic and delayed perception (also offensive) • domination of the technical expertise (ie. Police); • vertical walls and jurisdictional response;	Actions falling under the national cyberdefence: • Creation or expansion of large specialized units or military corps; • Obsessed with critical infrastructures; • development of offensive and defensive capabilities;	Delimitation of the geopolitical, economic and information assets of a country viewed as critical sectors Threats to: - the sovereignty, - survival of the state, - cyberspace and its components,

List of the selected texts (texts selected for TXM are in bold):

1. Law no. 124/2007 (L 2007)
2. Legislative decree no. 101 – January 9th, 2008 (LD 2008)
3. Legislative decree no. 61 - April 11th, 2011 (LD 2011
4. National Strategic Framework for Cyberspace Security – 2013 (NSFCS 2013)
5. **National Plan for Cyberspace Protection and ICT Security – 2013 (NPCPS 2013)**
6. Directive on the inter-ministerial coordination 2015 (Directive 2015)
7. Decree-Law no. 174 - 30 October 2015 (DL 2015)
8. Law No. 208 - Stability Law for 2016 - 28 December 2015 (SL 2015)
9. Development until the Gentiloni DPCM – 31 March 2017 (DPCM Gentiloni 2017)
10. **National Plan for Cybernetic Protection and Information Security – 2017 (NPCPIS 2017)**

Doc	Societal (I)	Technocrat (II)	Power-sovereign (III)	National interest
L 2007			• Creation of the SISR and all the other institutions • Responsibility of the information systems on the PCM solely • Creation of a school giving training within the DIS	•
LD 2008				• Definition of the critical infrastructures with this decree
LD 2011		• Implementation of EU law inside the domestic one	○	•
2013	States acknowledged that far from being a space without rules, cyberspace was governed by existing international law			
NSFCS 2013	Same as for the National Plan for Cyberspace Protection and ICT Security – 2013			
NPCPS 2013	<u>National</u>: • Enhancement of the organization, coordination and dialogue between national private and public stakeholders (owning and operating critical national infrastructures) ○ Through integration of all actors ○ Through the creation of tools, initiatives and standards common for the above infrastructures ○ Through the interoperability and semantic coherence between public Administrations	• Promotion of ad hoc legislation and compliance with international obligations ○ Revision and consolidation of the legislation in the field of ICT security ○ Definition of a normative framework that is suitable to support activities concerning cybersecurity and, in particular, cyber operations ○ Attribution of responsibilities and sanctions in case of violations ○ proposals for the implementation of the Directive of the European Parliament and Commission concerning measures to ensure a high common level of	• Strengthening of intelligence, police, civil protection and military defense capabilities ○ Daily assessment of the threats and vulnerabilities and share the results with the responsible of critical infrastructures ○ Monitoring new ICT technologies to highlight early-on any possible vulnerability ○ Implement early warning procedures ○ Development of capabilities to contrast cyber threats (both in terms of attribution and response) • Development of key operational capabilities, in line with the Defense Directives in the cyber domain ○ Implement the full operational capability of all structures devoted	• Formulate a methodology for the identification of ICT networks and computer systems that support critical functions • Set out minimum requirements for cyber defense, both in terms of instruments and procedures, for the protection of critical infrastructures • (part of the standardization) Adopt standards of reference for the authentication of, and authorization to the access to the networks of interest

	, the private sector, the EU, and NATO • Promotion and dissemination of the culture of cybersecurity (for citizens, students, firms and public administrations' personnel) • Education and training o Educate and train the personnel, raising awareness on cyber-threat o make training and educational activities of the Ministry of Defence available to the personnel of other Administrations, of public and private sector firms, staff of the EU and NATO as well as nationals of partner countries o Involve the academia and the different Advanced School as well as the centers of excellence in the process • Strategic communication o develop a situational awareness of the content of	network and information security across the Union • Compliance with standard security requirements and protocols o Standardization (in accordance with the norms ratified with NATO and the EU) o Documents of references (best practices of the field) o Review of the management and operational documents and manuals o Keep up-to-date with security certifications and evaluation and participation in the institutions that define them o Verification of cyber defense measures applied to critical infrastructures o Ensure the compliance through audits and accreditations • Ensure organizational interoperability and semantic coherence among all public Administrations, the private sector, the EU, and NATO, so as to allow for a common definition and understanding both of cyber events and of the protection and reaction procedures for dealing with cyber crisis • National coordination of the works done by the Council of the EU	to the protection of the cyberspace, establishing the assets identified by the chain of command, and providing for their preparedness, training, leadership, protection, support and deployment o Develop Command and Control structures that are able to plan and conduct military operations in cyberspace in an effective, prompt and distributed way (Joint Headquarters Cyber Operations - "COCI") o Implementation of national CERT, CERT-PA and ministerial CERTs and foster the creation of Regional CERTs o Development of a national integrated Computer Incident Response Capability (CIRC) o Development of digital forensics analysis capabilities (improve the capture and collection of data) • Development of concepts and doctrine related to cyber operations and activities, also through the identification of international best practices o through the identification of international best practices o Improve at the national level, as well as at the NATO and EU level, the understanding of how dissuasion and deterrence may contain a potential escalation of a crisis in cyberspace • Implementation of a governmental laboratory of comparative analysis that	

	information and alerts, in order to ensure an effective communication o Establish a protocol for public communication aimed at giving a correct and transparent overview of voluntary and accidental cyber events as well as of the response and system recovery actions that are put in place • Creation of Regional CERTs with the task of supporting local public administrations and implementing national rules and models of organization <u>International</u>: • Strengthening of bilateral and multilateral cooperation through joint activities (NATO, EU, OECD and other nations) o ensure international cooperation and exercises at the pan-European level (Cyber Europe), with the United States (Cyber Atlantic), and with NATO (Cyber Coalition) o participate in multilateral organizations	regarding the proposal of the Directive in matter of cyber security • Support the full participation of the Italian judicial system in the European e-Justice Working Group so as to be able to develop the information-sharing platforms and provide the associated services, as they will be made available • Support the technical-functional and procedural evolution of capabilities that are similar to and in harmony with the NATO Computer Incident Response Capability - Technical Centre (NCIRCTC) Technical Centre (CIRC-TC) • Implementation of a national system of Information Risk Management o Identify at the strategic level a shared and unambiguous information risk management methodology, adopting a model for national ICT critical infrastructures in accordance with UNI EN ISO 27001:2011 o Involve research centers and Universities so as to be able to adopt up-to-date risk management tools and procedures • Measurement of the costs associated with cyber events (especially involving national critical infrastructures)	conducts comparative analysis of ICT systems that are interest to administrations and national critical infrastructures	

	(EU, NATO, UN, OECD etc.) to gain a better understanding of the topic • EU projects o Promote and disseminate, also to the benefit of the private sector, information regarding initiatives and ways to be eligible for and participate in EU programs o Optimize the access to EU funds o participate in projects financed by the EU, in particular in the so-called Advanced Cyber Defense Center (ACDC) • Participation of private sector actors in bilateral and multilateral events concerning cyber security, also taking place at the international level <u>Both</u>: • Support to industrial and technological development o Promote ICT innovation both at domestic and international level o Ensure a secure cyber supply chain	• Define norms and financial instruments to optimize and share expenditures related to cyber defense		
Directive 2015	• Public administration o more effective coordination with the public		• Consolidation of the system	

	administration by strengthening their capacity to react to cybernetic events from a technical point of view and setting minimum safety standards (provided by the AgID); • PPP o develop relations with the private sector, o create an effective and thorough partnership with all non-public operators, who are entrusted with the control of information and computer infrastructures, on which essential functions for the country system; • Research o development of instruments of defense and reaction as advanced as possible from a technological point of view by the research bodies; • international cooperation o meeting the necessary "common level of		• Ensure the resilience of the national IT infrastructure in the face of events such as accidents or hostile actions that may compromise the functioning of the systems and the physical assets controlled by them	

	preparation and interoperability" in order to conduct properly its bilateral and multilateral relations			
DL 2015			• Strengthening of the CISR o Functions of advice, proposal and deliberation, in case of crisis situations involving aspects of national security, according to procedures established by specific regulations pursuant to Article 43 of Law no. 124 of 3 August 2007 for the PCM	
SL 2015			• €300 million for the modernization of defense and security sector equipment and instruments and for investments to adapt counter-terrorism capabilities • €150 million budget allocated to strengthen its cyber security	
DPCM Gentiloni 2017	Triggers the NPCPIS below			

NPCPIS 2017	• Encourage cooperation between national institutions and companies; • Promote and disseminating a culture of cyber security • Strengthen international cooperation on cyber security • Strengthen capacities to fight illegal online activities and content Reinforcement of the organization and the arrangements for the coordination and interaction at national level between public and private bodies • Strengthen the integration of all partakers (notably operators of essential services, operators of national critical information infrastructures and other relevant actors in strategic and ICT sectors) o through technical and institutional tables o through instruments of cooperation between the public sector and the private sector (info-sharing system) o through the participation of private operators in security	• Improvement of the technological, operational and analytical capabilities of the institutional actors concerned following an integrated approach • Establish procedures for the acquisition of goods and services related to the cybernetic field <u>Legislative measures and compliance with international obligations</u> • Revision and consolidation of the legislation on information security o Create a system gathering the specialist legal knowledge related to the field of cybersecurity already present among the structures of the different administrations and staff o Assess the alignment between the current internal legal framework and the development linked to innovation technology, taking into account international best practices o Finalizing the regulatory framework for National Critical Infrastructures in public and private computer systems with a view to defining the criteria for their identification, taking into account also those established for the sectors falling within the scope of the Directive (NIS Directive) o Simplifying and harmonizing the formalities and obligations for administrations and businesses in	<u>Strengthening the defense capabilities of the national critical infrastructures and the actors of strategic importance to protect the country as well as the system</u> • Reinforcement of the intelligence, the police, as well as the civil and military defense capabilities o Constant monitoring of the threat coming from the system and from the technologies o Share the information with the essential services and with the critical infrastructures systems o Collaborate with universities and research centres, including private ones, for the development of innovative methodologies and technologies for the detection and analysis of threats and vulnerabilities. o Development of collection, processing and dissemination capacities (cyber intelligence) and the management of knowledge derived from it through early warning systems o Developing capacities to counter the cyber threat o Development of basic operational capabilities to perform defense tasks in the cyber environment o Strengthen the structures in charge of the defence of cybernetic space o Develop Command and Control structures capable of planning and	

	events cybernetics, including international cybernetics, at bilateral and multilateral levels • Promotion and dissemination of a culture of information security as well as education and training o Concept and doctrine development o Promotion and dissemination of safety culture computer science (differentiated initiatives for citizens, students, businesses and public administration personnel) o Education, training and instruction <u>International cooperation and exercises</u> • Strengthening of bilateral and multilateral cooperation (Joint activities at Defense, Inter-Ministerial, NATO, EU and Multinational levels) • Coordinate national participation in the public and private components, Pan-European exercises	the cyberfield to increase the effectiveness of data breach and incident notification communications o Stimulating at European level the take-up of a re-structuring of the process of simplification and harmonization of obligations and obligations for administrations and businesses • Defining an appropriate legal framework to support cyber security activities • Develop a legal framework to tackle the issue of attribution of responsibility and the sanction resulting from these violations • Promote the discussion with EU institutions and the private sector with a view to drawing up proposals for the implementation of the Directive on cyber security (Directive (EU) 2016/1148 or so-called NIS directive) <u>Compliance with security standards and protocols</u> • Standardization and compliance o Update the national reference framework to standards and best practices According to NATO ratified standards, EU and international levels o Identify and updating minimum security requirements to be	conducting military operations in cybernetic space in an effective manner. o Develop auto-learning process • Organize, on a regular basis, national cyber security exercises (e.g. Cyber Italy), stimulating the participation of key service operators and/or national strategic sectors <u>Operationalization of national incident prevention, response and remediation structures</u> • Development of an integrated national incident prevention, response and remediation capability o Establishment of a single point of contact and one or more CSIRTs with adequate incident response capabilities (NIS Directive) o Making operational one or more national authorities (NIS Directive) o Implementation of the regulatory framework of reference for cyber security structures, in particular CSIRT/CERT, SOC, ULS and technical intervention pool o Adapt the role of the current national technical-operative structures of cybernetic security (CERT-N, CERT-PA, CERTDifesa, CNAIPIC, Intelligence Sector, etc.), also in the light of the new actors and of the new	

	(Cyber Europe), with the United States (Cyber Atlantic) and in the NATO (Cyber Coalition) framework • Projects of the European Union and international organizations o Promote and disseminate, also for the benefit of the private sector, information on initiatives and methods of participation in funds made available by the European Union o optimize access to funds of the European Union o participate in projects financed by the European Union o improve the quality of the information provided by the European Union. o Participate in NATO and other international organizations projects <u>Support industrial and technological development</u> • Production, Innovation and Technological Cooperation	implemented PA and critical infrastructure networks and systems o Adopt reference standards, best minimum practices and requirements for network and system security o Establish a system for accreditation and auditing of the bodies responsible for issuing digital certificates for authentication and other IT security certifications o Preparation and publication of reference such as manuals, lists of standard procedures and recommendations (best practices industry), taxonomy and uniform vocabulary to be used for the exchange of information o Review and update periodically the documentation (rules, procedures, etc.) relating to the management of the security of the systems and networks o Checking cyber defence measures applied to essential service providers and critical infrastructure through periodic tests of protection through technical and procedural verification by an independent verification system (e.g. external audit) o Expand security certifications and evaluations of commercial ICT products and systems	provisions of the NIS Directive, clearly defining the relations existing between them and identifying the relative model of cooperation o Develop a standardized model for the management of cyber events o Minimize the impact of cyber incidents that have led to the loss or theft of information (classified or not) or the destruction of IT support systems and resources o Develop an integrated proactive approach to limiting and reducing cyber security risks, including the adoption of an integrated database for the collection of accident reports and the countermeasures taken; an integrated alarm detection system, online incident/intrusion detection, strong authentication o Develop resilience • Development of CERTs in line with the requirements of the NIS directive towards the respective constituencies (CERT-N, to the system of enterprises, including SMEs), and for CERT-PA (to the development of higher levels of accreditation by public administrations) o assess their respective effectiveness	

	○ Foster the creation of a chain the provisioning of safe and resilient components from the point of view of cybernetic security supported by a fast and reliable validation, verification and certification process ○ Promote ICT innovation ○ Strengthen cooperation programs, multilateral and bilateral, for the benefit of national research and development functions in the European and international context • Strategic communication and working ○ Develop coordination on situation awareness of contents and information • Effectiveness of expenditure ○ Develop regulatory and financial instruments for the optimization and possible sharing of expenses, related to cyber defense	• Develop measurement tools for the costs relating to events of a nature cybernetics • Identify an unambiguous cyber methodology risk management shared at the strategic level, adopting models for operators of essential services, critical infrastructures and national strategic sectors • Adopt the risks evaluation plan as part of the national strategy and also as referred to in the NIS Directive	○ strengthen cooperation with CERTs at international and European level, including through participation in the network of CSIRTs, as referred to in the NIS Directive • Foster the establishment of a government verification laboratory that would submit to comparative analysis the ICT systems of interest to the administrations and the critical Infrastructures of national interest • Define priorities and costs associated with cyber-security and cyber-defence measures for critical infrastructure protection and for the development of basic operating procedures (material and non-materials resources as well as staff	

	measures between Departments, between the public and private sectors, and possibly between countries for international cooperation programs • Personnel o facilitate inter-ministerial sharing with a view to fostering integrated approaches for the recruitment of specialized staff, also taking into account international best practices • Involve research centers and universities to enable the adoption of updated management tools threat			

Note: table elaborated by our care from the documents used in the Italian analysis.

Appendix 24 Codebook updated (Italy)

addestramento/formazione	accesso	aggressione (s)
azienda(e)	attuazione	forza armata
azione	esperto/i	attacco/i
pubblica/amministrazione/autorità/	expertise	ente
settore/sicurezza/settore	legislativa	awareness/consapevolezza
colloquio	meccanismo/i	capacità
compagnia	misure	ordine/commando
competenza(e)	norma (e)	infrastrutture critiche
connettività	politica pubblica	ciberattacco(i)/evento cibernetico
cultura	preparazione	ciberdifesa (-) cibernetica
individuo(i)	prevenzione	sicurezza informatica (-)
informazioni	regola(e)	difesa
interdipendenza	rete(e)	distruzione
libertà	struttura(e)/ piano/	infrastruttura digitale
merce	tecnico	dottrina
operatori privati/operatori/		infrastruttura essenziale
settore/i interessato/i		governativo/governo
popolazione/popolo		sistema(i) d'informazione
settore della sicurezza informatica		infrastruttura terrestre
settore digitale		Forza(e) militare(i)
settore economico		paese
settore energetico		protezione
settore industriale/industriale (es)		resilienza
settori critici		stato
società		terrorista(i)
stakeholder		infrastrutture vitali
vulnerabilità		conflitto
		warfare
		guerra

Note: table elaborated based on the Klingova (2013) codebook and by our care from the documents used in the Italian analysis.

Appendix 25 Tables of selected words (a)-(b)-(c) – Italian case

a) Selected words for the cyberdiscourse type everyday security practices[44]

word	2013	2017	total
amministrazione (C)	11	17	28
attori	6	13	19
autorità	2	6	8
competenza (e)	0	5	5
cultura (C)	3	6	9
dialogo	2	2	4
formazione	7	4	11
impresa (C)	4	9	13
informazione (i)	16	13	29
interdipendenze	1	1	2
operatori privati	1	1	2
settore privato (C)	8	7	15
settore pubblico (C)	2	5	7
società	1	1	2
training	1	1	2
vulnerabilità	9	8	17
crimine informatico	1	1	2
Total occurrences	75	100	175

b) Selected words for the cyberdiscourse type technification[45]

word	2013	2017	total
attuazione	6	6	12
certificazione (i)	7	12	19
legislative/i	0	3	3
meccanismo/i	0	1	1
misura (e)	6	13	19
norma (e)	2	2	4
preparazione	2	1	3
prevenzione	1	2	3
regola(e)	1	4	5
piano nazionale (C)	18	19	37
tecnico/a (i/che)	9	5	14
Total occurrences	31	31	62

[44] No results for azienda, connettività, individuo, libertà, merce, popolazione/popolo, settore digitale, settore economico, settore energetico, settore industriale/industriale (es), autorità pubbliche, azione pubblica
[45] No results for esperto/i, expertise, politica pubblica

c) Selected words for the cyberdiscourse type hypersecuritization[46]

word	2013	2017	total
attacchi informatici	0	1	1
attacco (i)	2	3	5
attacco cibernetico	1	1	2
attacco cyber	1	1	2
capacità cibernetiche	0	1	1
capacità informative	1	1	2
capacità nazionale	0	1	1
capacità operative	2	2	4
capacità tecnologiche	0	1	1
difesa cibernetica	1	1	2
distruzione	1	1	2
dottrina	1	1	2
forze	0	1	1
governativo	2	2	4
infrastrutture critiche (c)	16	24	40
operazioni militari	1	1	2
paese (i)	8	12	20
protezione (c)	24	33	57
protezione cibernetica	15	19	34
resilienza	1	1	2
servizi essenziali	0	10	10
sicurezza cibernetica (c)	4	9	13
sicurezza ict	1	0	1
sicurezza informatica (c)	26	32	58
Total occurrences	108	159	267

Appendix 26 Table of the evolution of cyberdiscourses throughout the decade

Type of cyberdiscourse	2013	2017	Total words		Average words between 2008-2018
Everyday security practices	75	100	175		87,5
Hypersecuritization	108	159	267		133,5
Technification	31	31	62		31
Whole discourse	4867	7527	12394		6197

[46] No results for aggressione, awareness, guerra, infrastruttura digitale/ essenziale/ terrestre/ vitali,padronanza, settori critici, settori essenziali, terrorista(i), warfare

Appendix 27 Table of the evolution of cyberwords throughout the decade – Italian case

Word	PN 2013	PN 2017	Total
cibernetica (C)	24	36	60
cibernetiche	7	11	18
cibernetici	6	12	18
cibernetico	11	12	23
cyber	11	24	35
cyber-defence	1	1	2
cybersecurity	1	2	3
cyber-security	1	1	2
cyber-spazio	1	1	2
sicurezza cibernetica (C)	4	9	13
sicurezza informatica (C)	3	3	6
sistemi cibernetici	1	1	2
sistemi ICT	3	3	6
sistemi informatici	1	1	2
sistemi informativi	2	3	5
protezione cibernetica	15	19	34

Note: tables elaborated by our care from the documents used in the Italian analysis and the software TXM.

A**ppendix 28** Table of comparison

	France	**Italy**
Political responsability	Prime Minister	President of the Councils of Ministers
Definition the cyberstrategy	President through Prime Minister	PCM consultation with CISR
Role of the state	Primacy of the state by choice	Primacy of the state by observation
Main object of National interest	Critical infrastructures	Intellectual property
Driver of cyberstrategy	Focus on national interest infrastructure	Focus on cybercrime 2013
Definition of critical infrastructures	Regulation of 2 June 2006 and white paper (2008)	Legislative decree no. 101(2008)
Opinion on deterrence	Only through nuclear	Cyberdeterrence possible
Operational institutions		
Public sector	ANSSI and the national CERT and operational reserve	Agency for Digital Italy and CERT-PA
Private sector	ANSSI and the national CERT	CERT-PA
Defense	the ANSSI is under the reponsability of the SGDSN and Prime Minister as well as the operational reserve	National CERT
Attack	The CALID under the responsability of the Ministry of Defense and DGA and COMCYBER	The CIOC under the responsibility of the Minister of Defense
Critical infrastructures	ANSSI	CNAIPIC under the responsibility of the Minister of the Interior and National CERT
Education		
Public training	Yes, through universities	Yes, through universities (SecNumedu)
Military training	Yes, at the Telecommunications School of the Armed Forces of Chiavari (Genova)	Yes, at the CALID (Brittany) with Information Assurance Division of the DGA
Online platform	No	Yes (CyberEdu)

Note: table elaborated by our care.

Bibliography

Scientific Articles

AL ‐ RIZZO Hasan M. (2008). "The Undeclared Cyberspace War between Hezbollah and Israel". *Contemporary Arab Affairs*, 1(3), p.391–405.

ARQUILLA John and RONFELDT David (1993). "Cyberwar Is Coming!" *Comparative Strategy*, 12(2), p.141–165.

BALL Desmond (2011). "China's Cyber Warfare Capabilities". *Security Challenges*, 7(2), p. 81–103.

BALZACQ Thierry (2015). "The 'Essence' of Securitization: Theory, Ideal Type, and a Sociological Science of Security". *International Relations*, 29(1), p.103–113.

BLANK Stephen (2008). "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy*, 27(3), p.227–247.

BORRIELLO Arthur (2017). "There Is No Alternative: How Italian and Spanish Leaders Discourse Obscured the Political Nature of Austerity". *Discourse & Society*, 28(3), p.241–261.

CARDASH Sharon L., CILLUFFO Frank J., and RAIN Ottis (2013). "Estonia's Cyber Defence League: A Model for the United States?" *Studies in Conflict & Terrorism*, 36(9), p. 777–787.

CAVELTY DUNN Myriam (2012). "From Cyber-Bombs to Political-Fallout: Threat Representations with an Impact". *International Studies Review,* 15(1), p.105-122.

CHARAUDEAU Patrick (2009). Dis-Moi Quel Est Ton Corpus, Je Te Dirai Quelle Est Ta Problématique. *Corpus*, (8), p.37–66.

CHOUCRI Nazli, and David D. CLARK (2013). "Who Controls Cyberspace?" *Bulletin of the Atomic Scientists*, 69(5), p.21–31.

CRANDALL Matthew (2014). "Soft Security Threats and Small States: The Case of Estonia". *Defence Studies*, 14(1), p.30–55.

CRANDALL Matthew and Collin ALLAN (2015). "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms". *Contemporary Security Policy*, 36(2), p.346–368.

CAVELTY Myriam Dunn (2008). "Cyber-Terror—looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate". *Journal of Information Technology & Politics*, 4(1), p.19–36.

CZOSSECK Christian and Kenneth GEERS (2009). "Towards a Global Regime for Cyber Warfare. The Virtual Battlefield", *Perspectives on Cyber Warfare*, 3, p106.

FAHEY Elaine (2014). "The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security". *European Journal of Risk Regulation*, 5(1), p.46–60.

GORR David and Wolf J. SCHÜNEMANN (2013). "Creating a Secure Cyberspace: Securitization in Internet Governance Discourses and Dispositives in Germany and Russia". *International Review of Information Ethics*, 20(12), p.37–51.

HACHIGIAN Nina (2001). "China's Cyber-Strategy". *Foreign Affairs*, 80, p.118.

HAGGARD Stephan and JON R. Lindsay (2015). "North Korea and the Sony Hack: Exporting Instability through Cyberspace". *East-West Center*, 117.

HANSEN Lene and Helen NISSENBAUM (2009). "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly*, 53(4), p.1155–1175.

INKSTER Nigel (2010). "China in Cyberspace". *Survival*, 52(4), p. 55-66.

JENSEN Eric Talbot (2012). "Cyber Deterrence Symposium: International Law and the Internet: Adapting Legal Frameworks in Response to Online Warfare and Revolutions Fueled by Social Media". *Emory International Law Review*, 26, p.773–824.

JOUBERT Vincent, and Jean-Loup SAMAAN (2014). "Intergovernmentalism in Cyberspace. A Comparative Study of NATO and EU Initiatives". *Hérodote*, No 152-153(1), p.261–275.

KACOWICZ Arie M. (2004). "Case Study Methods in International Security Studies. Models, Numbers and Cases", *Methods for Studying International Relations*, p.107–125.

LEIMDORFER François and André SALEM (1995). « Usages de La Lexicométrie En Analyse de Discours ». *Cahier Des Sciences Humaines*, 31(1), p.131–143.

LIJPHART Arend (1971). "Comparative Politics and the Comparative Method". *American Political Science Review*, 65(3), p.682–693.

LOBATO LuíSa Cruz and Kai Michael KENKEL (2015). "Discourses of Cyberspace Securitization in Brazil and in the United States". *Revista Brasileira de Política Internacional*, 58(2), 23–43.

LUPOVICI Amir (2011). "Cyber Warfare and Deterrence: Trends and Challenges in Research". *Military and Strategic Affairs*,3(3), p.49–62.

LYNN William J. (2010). "Defending a New Domain: The Pentagon's Cyberstrategy". *Foreign Affairs*, 89(5), p.97–108.

MAYAFFRE Damon and Céline POUDAT (2013). "Quantitative Approaches to Political Discourse. Corpus Linguistics and Text Statistics". *Speaking of Europe. Approaches to Complexity in European Political Discourse*, p.65–83.

NISSENBAUM Helen (2005). "Where Computer Security Meets National Security". *Ethics and Information Technology*, 7(2), p.61–73.

PIPYROS Kosmas, MITROU Lilian and GRITZALIS Damian (2016). "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare". *Information and Computer Security*, 24(1), p.38–52.

RID Thomas (2012). “Cyber War Will Not Take Place”. *Journal of Strategic Studies*, 35(1), p. 5–32.

SALEM André (1987). « Pratique Des Segments Répétés. Essai de Statistique Textuelle ». *Lexicométrie et textes politiques*.

SAMAAN Jean-Loup (2010). “Cyber Command: the rift in us military cyber-strategy*”, Rusi Journal*, 155(6), p.16–21.

STRITZEL Holger (2007). “Towards a Theory of Securitization: Copenhagen and Beyond”. European Journal of International Relations 13(3): 357–383.

THOMAS Timothy (2014). “ Russia’s Information Warfare Strategy: Can the Nation Cope in Future Conflicts?”, *The Journal of Slavic Military Studies,* 27(1), p.101–130.

THOMAS Timothy (2009). “Nation-State Cyber Strategies: Examples from China and Russia”. *Cyberpower and National Security*, p.475–76.

TIAN Nan, Aude FLEURANT, Pieter D WEZEMAN, and Siemon T WEZEMAN (2017). “Trends in World Military Expenditure 2016”, *Stockholm Inernational Peace Research Institute (SIPRI)*, https://www.sipri.org/sites/default/files/Trends-world-military-expenditure-2016.pdf, accessed June 7, 2018.

TSAGOURIAS Nicholas (2012). “Cyber Attacks, Self-Defence and the Problem of Attribution”. *Journal of Conflict and Security Law,*17(2), p.229–244.

VAISHNAV Chintan, Nazli CHOUCRI and David CLARK (2013). “Cyber International Relations as an Integrated System”. *Environment Systems and Decisions*, 33(4), p.561–576.

VENDIL PALLIN Carolina and Fredrik WESTERLUND (2009). “Russia’s War in Georgia: Lessons and Consequences”. *Small Wars & Insurgencies*, 20(2), p.400–424.

VON SOLMS Rossouw and Johan VAN NIEKERK (2013). “From Information Security to Cyber Security”. *Computers & Security*, 38, p.97–102.

Monographs

AMPERE André-Marie (1834). *Essai Sur La Philosophie Des Sciences*. Paris : Bachelier, 352p.

AUSTIN John Langshaw (1975*). How to Do Things with Words*. USA: Harvard University Press, 176p.

BAUMARD Philippe (2017). *Cybersecurity in France*. Basel: Springer International Publishing AG, 106p.

BOURDIEU Pierre (1979). *La Distinction : Critique Sociale Du Jugement*. Paris: Les Editions de Minuit, 672p.

BRYMAN Alan (2006). *Mixed Methods.* London: SAGE Publications Limited, 1680p.

BUZAN Barry (2004). *The United States and the Great Powers: World Politics in the Twenty-First Century*. Cambridge: Polity, 240p.

BUZAN Barry, Ole WÆVER, and Jaap DE WILDE (1998). *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers, 300p.

CAVELTY Myriam Dunn (2014). *Cybersecurity in Switzerland.* Basel: Springer International Publishing AG, 75p.
CAVELTY Myriam Dunn (2015). Cyber-security in *Contemporary Security Studies, 4th Edition-Cyber-Security* by COLLINS Allan (2016). UK: Oxford University Press, 544p.

CHAPAUX Vincent, Julien PIERET, Pascal MBONGO, François HERVOUËT, and Carlo SANTULLI (2015). *Dictionnaire Encyclopédique de l'Etat*. Boulogne-Billancourt: Berger-Levrault, 1000p.

CHARAUDEAU Patrick (2005). *Les Médias et l'information : L'impossible Transparence Du Discours*. Louvain-La-Neuve : De Boeck Supérieur, 256p.

CHOUCRI Nazli (2012). *Cyberpolitics in International Relations*. United States of America: MIT Press, 312p.

COMAN Ramona, Amandine CRESPY, Frédéric LOUAULT, et al. (2016). *Méthodes de la science politique. 1st edition*, Louvain la Neuve : Deboeck Superieur, 224p.

CRESWELL John W. and J. David CRESWELL (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. London: Sage publications, 304p.

DOSSE, Stéphane, Olivier KEMPF, and Christian MALIS (2013). *Le Cyberespace : Nouveau Domaine de La Pensée Stratégique*. Paris : Economica, 192p.

GIBSON William (1984). *1948-1984 Neuromancer*. New York: Ace Science Fiction Books, 271p.

GVOSDEV Nikolas K. (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. United States of America: Georgetown University Press, 258p.
KEMPF Olivier (2012). *Introduction à la Cyberstratégie*. Paris : Economica, 235p.

LEBART Ludovic and André SALEM (1994). *Statistique Textuelle*. Paris, Dunod, 342p.

LIBICKI Martin C. (1995). *What Is Information Warfare?* Washington: Center for Advanced Concepts and Technology, 110p.

LIVERI Dimitria and SARRI Anna (2014). *An Evaluation Framework for National Cyber Security Strategies.* Heraklion: ENISA, 42p.

MARCHETTI Raffaele and Roberta MULAS (2017). *Cyber security - Hacker, terroristi, spie e le nuove minacce del web*. Roma: LUISS University Press, 190p.

MAURER Tim and Kenneth GEERS (2015). Cyber Proxies and the Crisis in Ukraine in *Cyber War in Perspective: Russian aggression against Ukraine* edited by Kenneth GEERS. Tallin: NATO CCD COE Publications.

MORGENTHAU Hans Joachim (1993). *Politics Among Nations: The Struggle for Power and Peace*. New York: McGraw-Hill, 448p.

NYE Joseph S. (2010*). Cyber Power*. United States of America: Harvard University Press, 31p.

SCHMITT Michael N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. UK: Cambridge University Press, 300p.

SCHMITT Michael N. (2017). *Tallinn Manual 2.0 International Law Applicable Cyber Operations 2nd Edition*. UK: Cambridge University Press. 638p.

SPRINZ Detlef F., and Yael WOLINSKY-NAHMIAS (2004). Models, Numbers, and Cases: Methods for Studying International Relations. United States of America: University of Michigan Press, 424p.

TEDDLIE Charles and Abbas TASHAKKORI (2003). *Handbook of Mixed Methods in Social & Behavioral Research*. United States of America: SAGE Publications Inc, 784p.

TELÒ Mario (2009). *International Relations: A European Perspective.* Farnham: Ashgate Publishing Limited, 234p.

TELÒ Mario (2013). *Relations Internationales : Une Perspective Européenne*. Bruxelles : Éditions de l'Université de Bruxelles.

TEORELL Jan, and Torsten SVENSSON (2007). *Att Fråga Och Att Svara: Samhäll svetenskaplig Metod*. Sweden:Liber, 296p.

VENTRE Daniel (2011). *Cyberwar and Information Warfare*. London: ISTE Ltd, 432p.

VENTRE Daniel (2015). *Chinese Cybersecurity and Cyberdefense. 1st edition. Information Systems, Web and Pervasive Computing*. London: ISTE Ltd, 320p.

VENTRE Daniel (2016). *Information Warfare. 2nd edition. FOCUS Information Systems, Web, and Pervasive Computing Series*. Wiley-ISTE, 352p.

WALTZ Kenneth Neal (1959). *Man, the State, and War: A Theoretical Analysis*. United States of America: Columbia University Press, 282p.

WIENER Norbert (1948). *Cybernetics: Control and Communication in the Animal and the Machine*. New York: Wiley, 212p.

ZEDNER Lucia (2009). *Security: Key Ideas in Criminology Series.* London and New York: Routledge, 206p.

Press Articles

APF (2010). « Le virus informatique Stuxnet continue de toucher l'Iran », *Le Monde.fr,* http://www.lemonde.fr/technologies/article/2010/09/27/le-virus-informatique-stuxnet-a-touche-l-iran-sans-degats-serieux_1416389_651865.html, accessed March 8, 2018.

ALONSO Pierre, Luc MATHIEU and Amaelle GUITON (2015). « TV5 Monde Débranchée Par Des Pirates – Libération », *Liberation*, http://www.liberation.fr/futurs/2015/04/09/tv5-monde-debranchee-par-des-pirates_1238071, accessed May 19, 2018.

DRAGOSEI, Fabrizio (2007). “Da Mosca Attacco Informatico All’Estonia”, *Corriere Della Sera*, https://www.corriere.it/Primo_Piano/Esteri/2007/05_Maggio/18/mosca.shtml, accessed February 19, 2018.

HOLLINGER Peggy (2011). “Cyber Attackers Target G20 Documents”. *Financial Times*. https://www.ft.com/content/83dc8ce4-48f4-11e0-af8c-00144feab49a, accessed June 1, 2018.

LEE Dave (2014). “Cyber “stand-off” in Ukraine Crisis”. *BBC News*, http://www.bbc.com/news/technology-26447200, accessed April 30, 2018.

PERLROTH Nicole (2012). “Cyberattack on Saudi Oil Firm Disquiets U.S”. *The New York Times*, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, accessed March 8, 2018.

SWAINE Jon (2008).“Georgia: Russia “Conducting Cyber War,””, *The Telegraph*, https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html, accessed April 30, 2018.

THE NEW YORK TIMES (2007). “A Cyberblockade in Estonia”. *The New York Times, June 2*. https://www.nytimes.com/2007/06/02/opinion/02sat3.html, accessed April 6, 2018.

VALENTINI, Alessia (2017). “Roberto Baldoni (CINI): “Sulla cybersecurity serve coordinamento e organizzazione.” *Cyber Security*. http://cybersecurity.startupitalia.eu/56220-20171221-roberto-baldoni-cini-sulla-cybersecurity-serve-coodrinamento-organizzazione, accessed June 1, 2018.

Working Papers

ADAMS Samantha, Marlou BROKX, Lorenzo DALLA CORTE, et al. (2015). “The Governance of Cybersecurity: A Comparative Quick Scan of Approaches in Canada, Estonia, Germany, the Netherlands and the UK”. *Tilburg University*, https://pure.uvt.nl/portal/files/8719741/TILT_Cybersecurity_Report_Final.pdf, accessed March 6, 2018.

BACKMAN Sarah (2016). “The Institutionalization of Cybersecurity Management at the EU-Level: 2013-2016”. *Swedish National Defence College*, http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-6236, accessed March 10, 2018.

DAVÌ Marco (2010). “Cyber Security: European Strategies and Prospects for Global Cooperation”. *European Security and Defence Forum (ESDF)*, http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/1110esdf_davi.pdf, accessed June 7, 2018.

GAMERO-GARRIDO Alexander (2014). “Cyber Conflicts in International Relations: Framework and Case Studies”. *Massachusetts Institute of Technology* https://ecir.mit.edu/sites/default/files/documents/%5BGamero-Garrido%5D%20Cyber%20Conflicts%20in%20International%20Relations-%20Framework%20and%20Case%20Studies.pdf

HEIDEN Serge (2010). "The TXM Platform: Building Open-Source Textual Analysis Software Compatible with the TEI Encoding Scheme", *24th Pacific Asia Conference on Language, Information and Computation*, https://halshs.archives-ouvertes.fr/halshs-00549764, accessed June 8, 2018.

HJALMARSSON Ola (2013). "The Securitization of Cyberspace. How the Web was Won", *Lund University*, http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=3357990&fileOId=3357996 accessed June 6, 2018.

KLINGOVA Katarina (2013). "Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia". *Central European University, Budapest, Hungary*. http://www.etd.ceu.hu/2013/klingova_katarina.pdf, accessed June 7, 2018.

LUKIN Kimberly (2012). "Weaknesses in the EU Countries Cyber Strategies", *University of Turku (Finland)*, http://worldcomp-proceedings.com/proc/p2012/SAM9741.pdf, accessed March 10, 2018.

MAYER Marco, Luigi MARTINO, Pablo MAZURIER, and Gergana TZVETKOVA (2014). "How Would You Define Cyberspace". First Draft Pisa, https://s3.amazonaws.com/academia.edu.documents/33741270/Cyberspace_Definition.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1528291942&Signature=hpXgCMEl9uqBJVyCukwiguTonBQ%3D&response-content-disposition=inline%3B%20filename%3DHow_would_you_define_Cyberspace.pdf Accessed June 6.2018.

Reports

BOCKEL Jean-Marie (2012). « La Cyberdéfense : Un Enjeu Mondial, Une Priorité Nationale » *Sénat français*, https://www.senat.fr/notice-rapport/2011/r11-681-notice.html, accessed February 2, 2018.

LASBORDES, Pierre (2006). « La Sécurité Des Systèmes d'information : Un Enjeu Majeur Pour La France : Rapport Au Premier Ministre ». *La Documentation Française*, http://www.ladocumentationfrancaise.fr/rapports-publics/064000048/index.shtml, accessed June 7, 2018.

ROMANI Roger (2007). « Cyberdéfense : Un Nouvel Enjeu de Sécurité Nationale ». Rapport d'information n° 449, *Commission des Affaires étrangères, de la Défense et des Forces armées du Sénat*, https://www.senat.fr/rap/r07-449/r07-449-syn.pdf accessed May 22, 2018.

Statements

LE DRIAN Jean-Yves (2016), Déclaration de M. Jean-Yves Le Drian, ministre de la défense, sur la cyberdéfense, in Bruz on the 13 December 2016, http://discours.vie-publique.fr/notices/163003632.html, accessed February 14, 2018.

MALLET Jean-Claude (2008). "President of the republic France, and Ministry of Defence France: French White Paper on Defence and National Security". http://archives.livreblancdefenseetsecurite.gouv.fr/2008/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html, accessed February 8, 2018.

Official Documents

COMMISSION DU LIVRE BLANC SUR LA DEFENSE ET LA SECURITE NATIONALE – FRANCE (2007). *Mission Letter of the President of the Republic*. http://archives.livreblancdefenseetsecurite.gouv.fr/2008/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/ressources_888/translated_documents_890/index.html, accessed April 28, 2018.

DIRECTORATE GENERAL FOR INTERNATIONAL RELATIONS AND STRATEGY OF FRANCE (DGRIS) (2013). *White Paper on Defence and National Security 2013*, https://www.defense.gouv.fr/content/download/206186/2286591/Livre-blanc-sur-la-Defense-et-la-Securite-nationale%202013.pdf, accessed February 11, 2018.

EUROPEAN COMMISSION (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *Joint communication to the European parliament, the council, the european economic and social committee and the committee of the regions*. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, accessed June 7, 2018.

EUROPEAN COMMISSION (2018). *The Directive on Security of Network and Information Systems (NIS Directive). Digital Single Market*. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, accessed May 29, 2018.

GAZZETTA UFFICIALE (2008). *Ministero Dell'interno - Decreto 9 Gennaio 2008*. http://www.gazzettaufficiale.it/eli/gu/2008/04/30/101/sg/pdf, accessed June 3, 2018.

GAZZETTA UFFICIALE (2010). *DPCM 5 Maggio 2010 Organizzazione Nazionale per La Gestione Di Crisi.* http://www.sarannoprefetti.it/SP/index.php?option=com_content&view=article&id=789:dpcm-5-maggio-2010-organizzazione-nazionale-per-la-gestione-di-crisi&catid=144&Itemid=102, accessed June 4, 2018.

GAZZETTA UFFICIALE (2011). *Decreto Legislativo 11 Aprile 2011, n. 61*. http://www.gazzettaufficiale.it/eli/gu/2011/05/04/102/sg/pdf, accessed June 3, 2018.

GAZZETTA UFFICIALE (2015). *Decreto-Legge 30 Ottobre 2015, n. 174.* http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2015-10-30;174!vig, accessed June 5, 2018.

MINISTRY OF ARMED FORCES - FRANCE (2014). *Introduction to the Cyberdefence Pact.* http://www.defense.gouv.fr/english/content/download/239577/2745144/Introduction%20to%20the%20Cyber%20Defence%20pact.pdf, accessed May 18, 2018.

MINISTRY OF ARMED FORCES – FRANCE (2017). *Strategic Review of Defence and National Security*. https://www.defense.gouv.fr/content/download/520198/8733095/file/DEFENCE%20AND%20NATIONAL%20SECURITY%20STRATEGIC%20REVIEW%202017.pdf, accessed May 18, 2018.

MINISTRY OF DEFENCE – FRANCE (2014). *Cyberdefence Pact*. http://www.defense.gouv.fr/english/content/download/239577/2745144/Introduction%20to%20the%20Cyber%20Defence%20pact.pdf, accessed January 31, 2018.

MINISTRY OF DEFENCE – France (2018a). *LPM 2019-2025 - Projet de Loi*. https://www.defense.gouv.fr/content/download/523151/8769287/file/LPM%202019-2025%20-%20Projet%20de%20loi.pdf, accessed February 10, 2018.

MINISTRY OF DEFENCE – France (2018B). *LPM 2019-2025 - Projet de Loi - Rapport Annexé*. https://www.defense.gouv.fr/content/download/523150/8769279/file/LPM%202019-2025%20-%20Rapport%20annex%C3%A9.pdf, accessed February 10, 2018.

MINISTRY OF HIGHER EDUCATION AND RESEARCH – FRANCE (2009). *Avis Relatif à Une Décision Portant Approbation de La Convention Constitutive Du Groupement d'intérêt Public Dénommé « Conseil Supérieur de La Formation et de La Recherche Stratégiques ».* https://www.csfrs.fr/sites/default/files/joe_20091117.pdf,accessed May 6, 2018.

NATIONAL AGENCY FOR INFORMATION SYSTEMS SECURITY (ANSSI) – France (2015). *French National Digital Security Strategy*. https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf, accessed February 2, 2018.

NATIONAL AGENCY FOR INFORMATION SYSTEMS SECURITY (ANSSI) – France (2011a). *Défense et Sécurité Des Systèmes d'information - Stratégie de La France*. https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf, accessed February 14, 2018.

NATIONAL AGENCY FOR INFORMATION SYSTEMS SECURITY (ANSSI) – France (2011b). *Information System Defence and Security - France' s Strategy*. https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf, accessed May 4, 2018.

NATIONAL AGENCY FOR INFORMATION SYSTEMS SECURITY (ANSSI) – France (2018a). *Organisation - Executive Office.* https://www.ssi.gouv.fr/en/organisation/executive-office/, accessed May 3, 2018.

NATIONAL AGENCY FOR INFORMATION SYSTEMS SECURITY (ANSSI) – France (2018b). *Formations.* https://www.ssi.gouv.fr/administration/formations/, accessed May 20, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – USA (2013). *Security and Privacy Controls for Federal Information Systems and Organizations.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, accessed March 10, 2018.

PARLAMENTO ITALIANO (2012). *Modifiche Alla Legge 3 Agosto 2007, n. 124*, http://www.parlamento.it/application/xmanager/projects/parlamento/file/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/Legge_7_agosto_2012.pdf, accessed June 4, 2018.

PARLAMENTO ITALIANO (2013). *Decreto Del Presidente Del Consiglio Dei Ministri 24 Gennaio 2013.*

http://www.parlamento.it/application/xmanager/projects/parlamento/file/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/DPCM_24_GENNAIO_2013.pdf, accessed June 4, 2018.

PRESIDENCY OF THE COUNCILS OF MINISTERS (2013). *National Strategic Framework for Cyberspace Security*. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf, accessed June 4, 2018.

SECRETARY GENERAL FOR DEFENCE AND NATIONAL SECURITY (SGDSN) (2018). *Strategic Review of Cyber Defence*, http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf,accessed May 22, 2018.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR) - (2007). *Law No. 124/2007*. https://www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html, accessed March 13, 2018.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR) - (2013). *National Plan for Cyberspace Protection and ICT Security.* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf, accessed June 4, 2018.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR) - (2015). *Direttiva 1 Agosto 2015* http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html, accessed June 5, 2018.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR) - (2017a). *Relazione Al Parlamento 2017*. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.pdf, accessed June 3, 2018.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR) - (2017b). *Piano Nazionale per La Protezione Cibernetica e La Sicurezza Informatica*. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf, accessed June 5, 2018.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR) - (2018a). *Decennale Intelligence* http://www.sicurezzanazionale.gov.it/sisr.nsf/comunicazione/decennale-intelligence.html, accessed June 3, 2018.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR) - (2018b). *Documento Di Sicurezza Nazionale - Allegato Alla Relazione Annuale Al Parlamento.* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.pdf, accessed May 5, 2018

SUCHIER, JM, C BLANCHER, JL BRUGUIERE, ET AL (2011) Contemporary Threats and Information Technologies, New Criminalities. In: Report of the Scientific Council of the High Council for Strategic Education and Research (CSFRS). Paris: CNRS Editions. https://www.csfrs.fr/sites/default/files/rcs_csfrs_v07_mai_30_2011%20v3.pdf, accessed May 5, 2018

UNITED NATIONS GENERAL ASSEMBLY (2013). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: 13.
http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf, accessed May 5, 2018

Websites

AGENZIA PER L'ITALIA DIGITALE (AgID) (2018) https://www.agid.gov.it/index.php/en/agency/about-us, accessed June 4, 2018.

BSA - THE SOFTWARE ALLIANCE (2018)
BSA EU Cybersecurity Dashboard (2015)
http://www.bsa.org/EUCybersecurity, accessed February 19, 2018.

CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (2018) Libro Bianco Sulla Cybersecurity.
https://www.consorzio-cini.it/images/Libro-Bianco-2018.pdf, accessed April 20, 2018.

COUNCIL OF EUROPE (2018)
Details of Treaty No.185 - Convention on Cybercrime. Treaty Office. https://www.coe.int/en/web/conventions/full-list, accessed May 20, 2018.
INTERNATIONAL TELECOMMUNICATION UNION (ITU) (2018)
The Global Cybersecurity Index (GCI) 2017
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf, accessed April 20, 2018.

MICROSOFT (2018)
The Need for a Digital Geneva Convention. Microsoft on the Issues. (2017)
https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/
accessed March 10, 2018.

MINISTERO DELL'ECONOMIA E DELLE FINANZE (MEF) (2018) Legge di Stabilità 2016.
http://www.mef.gov.it/focus/article_0014.html, accessed May 20, 2018.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (2018)
National Cyber Security Organisation: Italy (2015)
https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ITALY_032015_0.pdf, accessed June 4, 2018.

OXFORD ONLINE DICTIONARIES (2018)
Cybernetics | Definition of Cybernetics in English by Oxford Dictionaries. https://en.oxforddictionaries.com/definition/cybernetics, accessed February 22, 2018.

Laws

EUR LEX (2004). *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML, accessed March 10, 2018.

EUR LEX (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*, http://data.europa.eu/eli/dir/2016/1148/oj/eng, accessed May 29, 2018.

EUROPEAN PARLIAMENT (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* (Text with EEA Relevance), vol.119. OJ L. http://data.europa.eu/eli/reg/2016/679/oj/eng, accessed June 4, 2018.

LEGIFRANCE (2009). *LOI N° 2009-928 Du 29 Juillet 2009 Relative à La Programmation Militaire Pour Les Années 2009 à 2014 et Portant Diverses Dispositions Concernant La Défense*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020915137, accessed March 10, 2018.

LEGIFRANCE (2010). *Décret N° 2010-112 Du 2 Février 2010 Pris Pour l'application Des Articles 9, 10 et 12 de l'ordonnance N° 2005-1516 Du 8 Décembre 2005 Relative Aux Échanges Électroniques Entre Les Usagers et Les Autorités Administratives et Entre Les Autorités Administratives*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&categorieLien=id, accessed March 10, 2018.

LEGIFRANCE (2011). *Décret Du 16 Mai 2011 Portant Affectation et Élévation Aux Rang et Appellation de Général de Corps d'armée, Promotions et Nominations Dans La 1re et La 2e Section, Admission Par Anticipation et Sur Demande et Affectations d'officiers Généraux*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024009520, accessed March 10, 2018.

LEGIFRANCE (2013). *LOI N° 2013-1168 Du 18 Décembre 2013 Relative à La Programmation Militaire Pour Les Années 2014 à 2019 et Portant Diverses Dispositions Concernant La Défense et La Sécurité Nationale*. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id, accessed March 12, 2018.

LEGIFRANCE (2018). *Projet de Loi Relatif à La Programmation Militaire Pour Les Années 2019 à 2025 et Portant Diverses Dispositions Intéressant La Défense*. https://www.legifrance.gouv.fr/affichLoiPreparation.do;jsessionid=A5AC466FD795CE2842463CDF468089D3.tplgfr26s_3?idDocument=JORFDOLE000036584151&type=contenu&id=2&typeLoi=proj&legislature=15#, accessed February 9, 2018.

Department of Political Science

International Public Policies

Cybersecurity: The New Global Arena

A Franco-Italian Perspective

Summary

SUPERVISORS:

Prof. Raffaele MARCHETTI

Prof. Julien PIERET

MATTHIEU MAZERAT
Student Reg. No. 635592

CO-SUPERVISOR:

Prof. Roberta MULAS

Academic Year 2017-2018

Introduction and Literature Review

Topics related to the cyber-sphere have received much attention over the past decade. This sudden interest reflects shared feelings of both enthusiasm and fear. Indeed, while it can be said that the development of Information and Communication Technologies (ICTs) has brought about positive changes in our society, their ever-growing use and omnipresence raise a lot of concerns. All technologies relying on networks and more specifically on the so-called Internet infrastructure are bound to be, if it is not already the case, corrupted. An emblematic example of this pervasiveness occurred during April of 2007 in Estonia, which whole national internet network was paralyzed (The New York Times 2007). For some, this event has been described as Web War One (Blank 2008). While this statement can be discussed, the reactions it (has) triggered within the international community speak for themselves. Indeed, good examples are the establishment of NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn in 2008, the creation of the European Union Agency for Network and Information Security in 2014, or even the drafting of two Manuals on the International Law applicable to cyberwarfare and cyberoperations[1]. Yet, while these international initiatives received public attention, within states, governments also pushed forward laws and national strategies taking this new cyber threat landscape into account. As presented by Baumard (2017:12), most national cybersecurity strategies were implemented during the 2006–2016 period.

These implementations have been studied in many ways by tacticians, thinks tanks and political scientists. In this regard, we can point at two main methodologies. The first methodology draws upon various approaches, borrowing concepts from traditional international relations theories and laws. Based on hard facts, it mainly consists in listing the capabilities of a state, both offensive and defensive, following a framework built for that purpose or rely on non-scientific comparative analysis frameworks (Ball 2011; Cavelty 2014; Baumard 2017). Overall, this comprehensive method has proved beneficial in the comprehension of conventional warfare analysis. Yet, its main shortcoming is the inability to take into account the cyberspace multidisciplinary. The second central methodology draws upon constructivist theories, especially the securitization theory of the Copenhagen School, which explains how an issue becomes protected through discourse (Buzan, Wæver and De Wilde 1998). Most of the time, researchers noticed that national interest was put forward in the constructivist discourse to

[1] These manuals were respectively written in 2013 and 2017 as part of a NATO-commissioned initiative.

uphold political or military actions or explain states' behavior. In that regard, the securitization of cyberspace is not an exception and follows the same pattern (Kempf 2012:190).

From a general point of view, cyberissues raise many questions: How does the cyber element push states to rethink their national defense strategy? What does it add to the equation? Does it constitute a new "cybersecurity dilemma" (Council 2007; Buchanan 2017)? What about the attribution of this attack (Tsagourias 2012)? In terms of results, there are two opposite sides to these questions: on one side, researchers tend to consider that this cyber element does not change the rules of the game and only adds a new modality to warfare that does not justify any changes from both states and the international community. On the other side, with whom we concur, the cybersphere is a new strategic domain that increases the complexity on the battlefield and brings up a whole series of new considerations to the fore. This entails a rethinking of the way we traditionally perceive warfare. All of these considerations help and push states to undertake strategies encompassing cyberspace.

That being said, the research question around which our work will revolve is the following: *To what extent does cyberspace constitute a way to reaffirm a country's national interests through the implementation of its cyberstrategy?* The aim of this research is to compare the implementation of cyberstrategy in France and Italy using a crossover approach. By applying a constructivist analysis of both national cyberstrategies, we aim at underpinning the underlying realists' interests involved in the discourse.

Theoretical Framework

The core of our thesis finds its roots in the securitization theory (Buzan, Wæver and De Wilde 1998) and especially in its application to cyberspace (Hansen and Nissenbaum 2009; Gorr and Schünemann 2013; Hjalmarsson 2013). In that regard, Hansen and Nissenbaum attached the three modalities of the securitization theory to the cyberdiscourse, namely hypersecuritization, everyday security practices and technification (Hansen and Nissenbaum 2009). However, because the aforementioned authors only provide modalities but do not provide a typology on which we can rely to assess the dominant cyberdoctrine followed by a country, we had to add another framework. Thus, we bridge the gap of existing literature by relying on Baumard's typology of national cyberdoctrines in order to determine in which cyberdoctrine category countries fall depending on the decisions they take (Baumard 2017).

Indeed, he establishes four different categories called *class* (Baumard 2017). The first class "Social order" (I) relies on a control at the source exerted by technical expertise—e.g. like the police— more than on a national vision, which if there is any, is often borrowed from another state. The second class is the "Technocrat" (II), which unlike the previous class aims at exerting a control by a normalization of the outputs. States that adopt this stance are mostly latecomers on the field and suffer from a delayed perception of technology change, still mainly inspired by an incident response philosophy. The third class "Societal Resilience" (III) encompasses states that focus their offensive capabilities on information warfare, monitoring and controlling public sphere where opinion movements can appear (e.g. civil hacktivist groups). The fourth class "Power-sovereign" (IV) gathers states obsessed with critical infrastructures. In order to protect them, they usually invest in large specialized units that can withstand state-sponsored cyber-attacks thanks to sustainable deterrence policies. However, when facing pattern changes or emerging hacking movements, this class can seem unprepared as its whole structure is rather rigid and does not foster reactivity to "distributed cognitive warfare" (Baumard 2017:69). Lastly, we also mobilize the concept of national interest as an all-encompassing idea. When the concept is uttered, states call upon this joker that enables them to resort to every means possible to protect what they conceive as belonging to their national interest.

Among all the works we consulted, Baumard's study of cyberdoctrines captured our attention. Drawing upon his work, we developed the idea of a comparative analysis between France and Italy as the two countries were latecomers in the field of cybersecurity (Kempf 2012:194). Following this starting point, our first hypothesis goes as follows:

> **H1:** *The securitization of French and Italian cyberspace aims at asserting their national interest.*

Nowadays, states are aware that ICTs change the rules of the game, and that fights are no more conducted on traditional battlegrounds. Indeed, conflicts are nowadays conducted remotely and on multiple theaters of war. Therefore, we expect to see securitization as a way to ease the implementation of actions and policies following the subsequent pattern. First, the identification of threats to the national interest components (population, territory [both public and private premises, but especially the vital infrastructures] and sovereignty); then, defining their impact on the referent object; and eventually, the adoption of actions. Secondly, within this logic, the leading securitization actor remains the state. This is why we adopt a stance we could see as a realist constructivism. Morevover, numerous studies refer to the securitization of cyberspace (Gorr and Schünemann 2013; Hjalmarsson 2013; Klingova 2013; Lobato and

Kenkel 2015). Consequently, we argue that the same phenomenon is applicable to France and Italy. Nevertheless, these studies do not delve into the relationship between national interest and cybersecurity matters, and above all, do not show that the interconnection between these two elements.

Then, based on similarities displayed by the two countries as well as the previous results of Baumard, we formulate two additional hypotheses (Baumard 2017):

> **H2:** *the French discourse on cyberspace leans towards hypersecuritization, meaning it belongs to the power-sovereign type.*
>
> **H3:** *the Italian discourse on cyberspace leans towards technification, meaning it belongs to the technocrat type.*

Regarding our H2, we expect that because France will fall into the power-sovereign type, it will protect its critical infrastructures, increase its cybercapabilities and its specialized units thanks to an hypersecuritization of its discourse. Contrariwise, our H3 suggests that Italy belongs to the technocrat type, meaning that its cyberstrategy is developed on regulations and rules and does not lean towards an hypersecuritization. We should bear in mind that the combination of these two frameworks is a novelty and we may therefore witness cyberdoctrine types overlapping with cyberdiscourses. In this regard, our categories are not mutually exclusive.

It must be pointed out that the types chosen for each country are not random, but they derive from the analysis Baumard had done on national cyber-crime doctrines over the period 1994–2017 (Baumard 2017:14). While Baumard positioned each document per year on the matrix, we seek to demonstrate a trend of the dominant cyberdoctrine for each country throughout a greater range of documents. Furthermore, although we link a predominant cyberdiscourse to a cyberdoctrine, we may find elements of other modalities in the same cyberdiscourse. Indeed, we should not forget that "cyber security is a terrain on which multiple discourses and (in) securities compete" (Hansen and Nissenbaum 2009:1162).

Methodological Framework

Our research design draws upon the mixed-methodological approach following a sequential exploratory design (Creswell and Creswell 2009). This entails a threefold process. The first phase is dedicated to the qualitative data collection and analysis, while the second phase introduces the quantitative tool-the lexicometry software TXM. The second phase builds

on the results found in the first one, hence the name exploratory (Creswell and Creswell 2009:211). As our work involves two countries, the final stage entails a comparative analysis. Based on Baumard's cyberdoctrine theory (2017) as well as Hansen and Nissenbaum's work (2009), we elaborated a mixed framework to determine into which cyberdoctrine type each country would fall and consequently which cyberdiscourse they would tend to use (Hansen and Nissenbaum 2009; Baumard 2017). To determine the type of cyberdoctrine embraced by our two states, we used the four categories previously presented, i.e. Social order (I), Technocrat (II), Societal Resilience (III) and Power-sovereign (IV). However, since Baumard did not specify the steps to follow to obtain these four categories, we decided to merge the two socials to only get one Societal category[2].

This merging allows us to get a perfect match for our two frameworks presented above, namely the cyberdoctrine and cyberdiscourse frameworks. Thus, we obtain three categories: Societal (I), Technical[3] (II), and Power-sovereign (III). Each category follows different decision patterns: (I) societal rooting, (II) technical and jurisdictional cyberdefence and (III) national cyberdefence (see appendix 1). Furthermore, we also built a framework for our first qualitative part (appendix 2). As far as the cases are concerned, we selected France and Italy for two reasons. First, taking part in a one-year exchange in Italy has been the occasion to adopt a dual perspective on the thesis. Second, as said above, the two countries followed a similar pattern. Indeed, they were latecomers in the field of cybersecurity and have both undertaken the development of a cyberstrategy after 2007 (Kempf 2012:194; SISR 2018).

Analysis

To undertake our analysis, French and Italian national cyberstrategies have been first analyzed separately from 2008 to 2018. To do so, we start with a qualitative analysis of France and Italy and then we undertake a quantitative examination. This combined approach strives to offer a complete analysis, taking advantage of both qualitative and quantitative methods. Moreover, the main purpose of the lexicometry is to help us corroborate the qualitative in-depth. The last step consists in comparing our results.

[2] The author has been contacted and confirmed our first assumption that the theory was not based on any previous works.
[3] To not get confused with Baumard's original framework, we used the term technical instead of technocrat for our merging.

France

Our findings show that the French national cyberstrategy followed a gradual evolution. The first phase can be described as the wakening phase (2008–2013) and was marked by the cyberattacks in Estonia. The probability of an upcoming cyberwar became the driving force of the cyberstrategy implementation and allowed France to adopt a discourse of hypersecuritization, using cyberthreats as the main reason. From that moment one, all the background work as well as the establishment of legal foundations were carried out. This phase was accompanied by the creation of the state's tool to protect its information systems, the National Cybersecurity Agency of France (ANSSI). Indeed, the ANSSI was established with the 2009 decree, which set down in writing the national agency and its abilities. During this first phase, the challenge was to build the foundations. France turned inward to better reassert its sovereignty, redefining its national security, its national interest, and its underlying components.

The second phase was the expansion (2013–2015). It consisted of two aims: ensuring that the current institutions were strong enough to face future attacks and broadening the scope of their mission. Slowly, the scenario of cyberwar faded away to leave room for the growing threats of massively coordinated cyberattacks and daily cybercrime. In other words, without forgetting the worst-case scenario, France refocused its effort on better prevention and resilience in the face of daily cybercrime. Nevertheless, French authorities continued to use the specter of a cyberthreat to further develop their military capacities (more people) as well as capabilities (both software and hardware). In addition, they also enhanced their legal framework, expanding by the same token the range of their sovereignty. Yet, as the challenge to protect the country was high, France had to develop new ways to keep up the pace with cyberthreats. In this respect, the operational reserve was one of them. In parallel, a lot has been undertaken in this matter, such as the creation of the cyber center of excellence, with the aim of creating a French cyberculture as well as partnerships with schools to ensure the future of this field of research.

The last ongoing phase is the consolidation (2015-nowadays). Indeed, the securitization of cyberspace has allowed France to protect its sovereignty by protecting every referent object related to it. In the beginning, France was essentially focusing its attention on state and critical infrastructures, but time has proved these were not the main targets of cyberattacks. Recently, the shift towards more inclusion was engaged and is now taking its roots in society. Indeed, there is a clear distinction between the roles of each institution. On the one hand, the ANSSI

takes care of the prevention, raising the awareness of all actors in society and monitors the critical infrastructures. On the other hand, if France is under attack, the Analysis Centre for Cyber Defensive Operations (CALID) takes over to contain and then solve the situation. Overall, the institutionalization of cyberdefence as a field has been effective, but the very structure was still too centralized from the beginning onwards. Thus, French authorities started a decentralization of its infrastructure towards the regions by setting a coordinator in each of them. At the same time, numerous online platforms of the ANSSI have enabled to diffuse its conception, good practices and keep the monopoly on information.

To conclude on our analysis, the French cyberstrategy has undergone various changes over the past decade. Still, not only does France seem to follow the path of the type power-sovereign but also to translate it through a dominant hypersecuritization discourse. Nevertheless, the two are not mutually exclusive. France may display a behavior of type power-sovereign but can also adopt decisions falling into the categories of the two other types, namely societal and technical. What we detect here is a trend, and the same applies to the discourses. Indeed, while the hypersecuritization is pervasive in all discourses, we inferred that if the power-sovereign does characterize France as a long-term trend, the state also took decisions oriented towards the two other types. It is important to remind that the cyberstrategy/cyberdoctrine is the combination of the three types.

Italy

Despite being a latecomer in the cyberfield, Italy succeeded in catching up with its European partners. The cornerstone of the Italian cyberstrategy is the law no. 124 of 2007. The reform of the Italian architecture was also decided after the changes occurring on the international stage. Thus, we can also say that the first phase Italy has gone through was the awakening. From the beginning onwards, the President of the Council of Ministers was the central piece of the Italian cyber-architecture. Indeed, the year 2007 marked the formation of an entire new ecosystem for Italy, namely Italy's Intelligence System for the Security of the Republic (SISR). The SISR gathers six different actors: the President of the Council of the Ministers (PCM), the Interministerial Committee for the Security of the Republic (CISR), the Delegate authority, and the three components of Italian secret services, namely the Security Intelligence Department (DIS), the External Intelligence and Security Agency (AISE) and the Internal Intelligence and Security Agency (AISI). Soon enough, the Italian authorities decided to frame what they understood to be critical infrastructures and to create an institution placed

under the Ministry of the Interior, the Computer Centre for the Protection of Critical Infrastructure (CNAIPIC). However, the legislative decree of 9 January 2008 was not part of the cyberstrategy. Then, came the decree of May 2010 and the two new bodies (Political Strategic Committee [COPS] and Interministerial Situation and Planning Unit [NISP]) to better deal with crisis management. Again, this did not change a lot the Italian cyber-landscape. Indeed, we must wait for the laws 133 and 134 in 2012, amending the 2007 law, to observe a change in the Italian structure. These two laws brought about two main changes. First, a growing role for the CISR, which had to be consulted before the decision-making process goes through the DIS. Second, we witnessed the creation of the Agency for Digital Italy (AgID) to achieve the Italian digital agenda, foster growth and innovation as well as "support digital innovation and promote the dissemination of digital skills, [this] in collaboration with international, national and local institutions and bodies" (AgID 2018).

In 2013, Italy entered the second phase that we could call realignment. This realignment began with the decree of the PCM of 24 January 2013 in which it was stated that it was necessary to define a national strategic framework "because of the features of the cyber threat being a risk to national security" (Parlamento 2013). The crucial point here is to see that Italy based its framework on the active involvement of both private and public stakeholders. In the analysis, we saw that the framework reshuffled the functions within the Italian cyber-architecture. As part of its biannual program (2014–2015), the Cyber Security Unit (NSC) was put under the DIS, whereas the management of the cyberdefence was improved. This was achieved through the creation of a Command and Control Structure and two Computer Emergency Response Team (CERTs)—one for the national level and another one for the public administration, as well as a Computer Incident Response Capability (CIRC). This alignment has continued with the 2015 directive on the inter-ministerial coordination that has strengthened the role of the CISR, which has become crucial in times of crisis. Furthermore, the 2016 stability law has provided a budget for the national cyberdefence.

Finally, regarding the last document we analyzed, the National Plan for Cybernetic Protection and Information Security was released in 2017. Its content aims at fortifying the role of the CISR, which now has the role of raising the country information security awareness by issuing guidelines. In this mission, it is assisted by the technical section of the CISR and the DIS. In addition to this main measure, the two CERTs were strengthened, and a National Evaluation and Certification Centre was set up to verify the reliability of the infrastructures, while the range of essential operators is also expanded, including essential service operators and digital service

providers. The 2017 framework was also the opportunity for Italy to reassert its willingness to include stakeholders within the society. It calls for more collaboration between civil society and private sector but also encourages academicians to carry on research on cyber-related topics. Finally, the offensive-defensive capabilities were reinforced with the establishment of the Joint Headquarters Cyber Operations (CIOC) in charge of protecting ministries' networks and systems. To improve the cyber-skills of its combatants, a cybercell was also put in place within the Telecommunications School of the Armed Forces of Chiavari, located in Genova.

By going in detail into the Italian case, we have seen that the construction of the Italian strategy has been different. Indeed, we expected that Italy would adopt more technical and legal measures to implement its cyberdoctrine. However, the lexicometry did not enable us to confirm our hypothesis. Nonetheless, as we previously stated it in the analysis introduction, the qualitative analysis prevails over the quantitative one. Thus, even though the Italian discourse seems to lean towards hypersecuritization, we argue that it is mainly based on a combination of societal and technocrat types. The reason behind our statement stems from the qualitative analysis of the Italian case and is twofold. First, in the framework we have built for that purpose, we saw that there are more actions and decisions falling into the technocrat and societal types. Second, it is hard to tell if Italy has entered the third phase of consolidation in 2017 because much of what is done remains classified. Indeed, we do not have any information on the annual budget or the workforce of the different institutions we mentioned. Is it part of the Italian strategy not to display all its assets or does it reflect a still burgeoning cyberfield? It would require a deeper analysis to shed light on these phenomena.

Comparison

After going through a decade of documents, we delineated the main differences and similarities between our two countries.

Firstly, as far as political responsibility is concerned, the results are relatively similar for both France and Italy. While in the French case, the Prime Minister bears the political responsibility, in the Italian case, it is the President of the Councils of Ministers (PCM), as we have seen with the 2007 law. Furthermore, the definition of the cyberstrategy in Italy is elaborated by the PCM, who has to consult the Interministerial Committee for the Security of the Republic (CISR), whereas in France, the President of the Republic, being the head of the state, has a word with the Ministers and his Prime Minister, who then apply the decision. In both cases, it is a rather

top-down approach. All along the French case, we observed that the national interest was determined by the population, the territory, the critical infrastructures, and sovereignty. In the Italian case, there is no such discourse, except on intellectual property. With regards to national infrastructures, both countries have adopted legislative dispositions stating what is intended as such in the past decade or earlier (Regulation of 2 June 2006 and white paper [2008] for France and Legislative decree no. 101 [2008] for Italy). In addition, a very interesting point concerns the deterrence. Italian authorities do not rule out cyberdeterrence, they even conceive it as "a disincentive to potential adversaries and criminals" (PCM 2013:25). On the contrary, for France, notably to former Foreign Minister Le Drian, there is no such thing as cyberdeterrence, as only nuclear power matter in terms of deterrence (Le Drian Jean-Yves 2016). Regarding the role of the Italian state in the cyberdefence field, the question was an observation rather than a choice. Indeed, the state is one of the main actors in cyberspace because the infrastructures mentioned are located on its territory, and because it is one of the only actors having sufficient resources to organize and manage cyberdefence (SISR 2013:14). For France, from the very beginning, the state has been the sole responsible actor of cyberdefence (SGDSN 2018).

Secondly, our comparison deals with the institutions. On both sides, there are institutions to monitor and defend the state but also to counter attacks if needed. For operational centers in the public sector, we have the Agency for Digital Italy as well as the CERT for the public administration on the Italian side, which also deals with the private sector. In France, it is the ANSSI especially and the National CERT that plays the prevention role. Concerning the defensive part, Italy can count on its national CERT, while France relies on the ANSSI as well as its operational reserve. As far as the offensive operational centers are concerned, France's counterattack capabilities lie in the hand of the Analysis Centre for Cyber Defensive Operations (CALID), which is under the responsibility of the Ministry of Defense and DGA, and the cyber commandment (COMCYBER). In Italy, this task goes to the Joint Headquarters Cyber Operations (CIOC), placed under the responsibility of the Minister of Defense. Eventually, both countries are also endowed with an institution protecting their critical infrastructures. In Italy, this matter is managed by the Computer Centre for the Protection of Critical Infrastructure (CNAIPIC), and under the responsibility of the Minister of the Interior and the National CERT, while in France, it is again managed by the ANSSI.

Thirdly, both academic and military training has been set up in the two countries. Looking at the public part, we mainly encounter academic and computer sciences studies that include a deeper emphasis on security matters. In the case of France, many universities have accounted

for governmental recommendations and have included a core knowledge that should be shared by all students and future professionals. This initiative is called *SecNumedu*. Furthermore, as far as military training is concerned, Italy has established tabletops at the Telecommunications School of the Armed Forces of Chiavari, in Genova. We can assume that this kind of knowledge was acquired by means of its active participation to the NATO. In France, we saw in the analysis that the CALID in Brittany acts as a center of excellence within the formation organized with the Information Assurance Division of the DGA. Finally, France also set up an online platform called *CyberEdu* to diffuse good practices and common knowledge on cybersecurity to the public.

Now, with respect to our hypotheses, we obtained mixed results. Regarding our first hypothesis (H1), namely that the securitization of French and Italian cyberspace aims at asserting their national interest, we saw that it was confirmed for France and partly confirmed for Italy. As previously stated, we understand national interest as an all-encompassing set of things a state is ready to defend, both material and immaterial, even by means of violence if needed. Thus, for both countries, we observed that national interest has been wielded in the face of threats endangering the population, the territory, the sovereignty, the critical infrastructures or even intellectual property. Indeed, for France, we noted that, early on, in the 2008 White Paper, French authorities were stating that "the internet will need to be considered as critical infrastructure and considerable effort will be made to improve its resilience" (Mallet and France 2008:174). As the French national interest is made up of its population, its territory, its sovereignty and its critical infrastructure, we can effectively confirm this hypothesis. For the Italian case, the argument put forward is that cybercrime is "a threat of primary importance" (PCM 2013:13) which endangers "innovation [which is] at the cornerstone of [Italian] growth and competitiveness" (PCM 2013:5). In both study cases, it is necessary to slightly stretch the meaning, but we do discern the connection between the implementation of such far-reaching policies and the use of threats to the national cyberspace that encourage their achievement.

Then, the second and third hypotheses have also been to some extent confirmed. For the French case, based on the decisions taken by the French authorities during the past decade, we assumed that France adopted a cyberdoctrine of type III—that is Power-sovereign—and therefore should follow a cyberdiscourse of hypersecuritization. This is effectively confirmed by the quantitative results supporting our assumption. Indeed, our findings, both qualitative and quantitative, show that France has had a dominant hypersecuritization cyberdiscourse which confirms our hypothesis (H2). For the Italian case, the results of the qualitative analysis suggest that Italy

gathers a combination of societal and technical visions of cyberdoctrine. As our main documents were decrees and laws, we also assumed Italian authorities would use a technical cyberdiscourse to implement societal decision. However, the lexicometry analysis shows that the Italian cyberdiscourse from 2013 to 2017 was also leaning towards a hypersecuritization cyberdiscourse. Yet, in this case, the analysis *per se* cannot be compared to what we obtained with the French analysis, as we had lesser documents over a shorter period of time. The main reason is that Italy has not released as many documents as France did, and the few documents available are mainly listing decisions and orientations, which makes difficult to detect a trend in the discourse. Consequently, the hypothesis (H2) is not validated for the case of Italy, as far as the quantitative analysis is concerned. For the qualitative one, we still argue Italy employs a technical cyberdiscourse to implement societal decision.

Conclusion

Our research aimed to study to what extent cyberspace constitutes a way to reaffirm country's national interests through the implementation of a cyberstrategy. Drawing upon two theoretical frameworks (Hansen and Nissenbaum 2009; Baumard 2017), we built our own theoretical framework, not only to determine the kind of cyberdoctrine adopted by states but also to unveil the type of cyberdiscourse that accompanied it.

Thus, we found the following results:

(1) France and Italy did securitize their cyberspace to assert their national interest, but for different reasons.
(2) The French discourse on cyberspace does lean towards hypersecuritization and has adopted a power-sovereign type cyberdoctrine
(3) The Italian discourse on cyberspace does not lean towards technification and does not belong solely to the technical type.

For the first hypothesis, as we have concluded in the comparison section, both countries have been using their national interest to start the implementation of a cyberstrategy, but for different purposes. We explained that the starting and turning point was the wave of attacks in Estonia and that the idea of being paralyzed as the Estonian systems had been in 2007, pushed France and Italy to devise a comprehensive cyberstrategy. Furthermore, our results for the second and third hypotheses were divergent. While the second hypothesis was confirmed by our two-step

analysis, qualitative and quantitative, we found sufficient support to confirm the third hypothesis only for the qualitative part.

We argue that our work contributes to the flourishing field of cybersecurity studies and allows to update data on a phenomenon which is still not widely addressed. Indeed, the relevance and strengths of this thesis can be summed up in three points. Firstly, the cases selected for this comparative analysis (France and Italy) and the domain (securitization of the cyberstrategy) have not been studied together so far, at least not to our knowledge and not in this fashion. Secondly, the frameworks used for conducting the analysis have been updated, including not only the original criteria but also new inputs built especially for this analysis, drawing upon both realist and constructivist theories. Not only does such a combination allow to provide more tools to portray the reality, but it also contributes to the development of the cybersecurity field. Additionally, we improved the framework devised by Baumard (2017) as we provided an exhaustive list of actions that could fall into each category. Thirdly, political science literature on cybersecurity does not present many studies using a realist-constructivist framework coupled with a discourse-theoretical approach. Thus, adopting a crossover theoretical approach provides avenues to a topic that is growing in the literature and shed a different light upon a current phenomenon as well as better explain state behavior as far as (cyber-) national defense is concerned.

Nonetheless, our thesis work is not exempt from drawbacks. One of the main criticisms concerns our mixed-methodological approach. Indeed, conducting both qualitative and quantitative analyses required considerable time. In that matter, the preparation of the texts for the lexicometry software was time-consuming and invisible to the eye of the reader. This proves to be even more frustrating when the analysis does not bear its fruits, as it was the case in Italy. On that matter, the availability of data was problematic. Indeed, unlike the French case, it was harder to find relevant and comprehensive documents for the Italian case. The French White papers are clear and straightforward while the Italian documents were vague and far from the details of the French ones. Another criticism that could be raised against our methodology could be the split we made in the qualitative part. Indeed, it may appear too descriptive at first glance. Nevertheless, we think this division was more appropriate insofar as it accounted for the evolution of each country's cyberstrategy by reaching for their bedrocks.

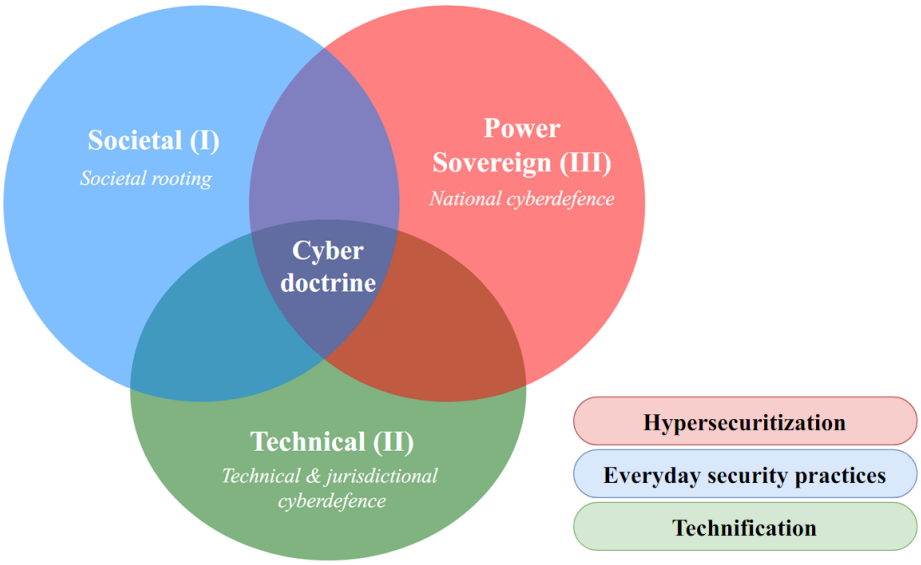
When it comes to highlighting future avenues of research, it must be said that cyber-related studies are flourishing alongside the expansion of our use of ICT technologies. Every single

item we add to the collection of this interconnected world could be the subject of a thesis on his own. First, our analysis has shone a light on the growing role of the private and research sectors. Thus, adding further documents to the Italian analysis might bring interesting results. For instance, linking the annual *Relationze al Parlamento* to a similar analysis of our own, especially the lexical one, could display interesting discourse elements. Moreover, other documents such as the Cyber Intelligence and Information Security (CIS) reports elaborated by the *Università Sapienza di Roma* might help in anticipating future orientations of the Italian cyberstrategy. Another interesting perspective would have been to participate in conventions or annual events linked to cybersecurity in order to collect firsthand account through interviews of cybersecurity representatives. Eventually, for both France and Italy, it might bring more weight to make a comparative analysis with the Estonian case as it is the index case in the field of cyberstrategy.

In conclusion, many contextual events must be faced by both countries. From a legal point of view, both countries have to implement the NIS directive and the General Data Protection Regulation (GDPR) (EU) 2016/679 (European Parliament 2016; The European Commission 2018). From a political perspective, the Italian elections gave Italy a new government which may have other priorities than securing the cyberspace. In France, the new Military Programming Law (LPM) was approved by the Senate, while the dedicated budget to the Defense sector already raises questions among the political sphere (Reuters 2018). Only the future knows where cybersecurity is headed.

Appendixes

Appendix 1: Qualitative cyberdoctrine framework



Note: Elaborated by our care.

Appendix 2: Operationalization of the qualitative concepts

Concepts	Dimensions	Indicators
Cyberdoctrine	Societal (I)	Actions falling under the societal rooting such as • Sensitive to opinion movements; • influence of the public space actors (including. hacking civil groups) to a certain extent Europe; • Have an "information warfare" active component; • Weak or borrowed national vision • Inclusion of the society through awareness campaign or good practices diffusion • Education
	Technocrat/Technical (II)	Actions falling under the technical and jurisdictional cyberdefence • incident-Response philosophies; • technocratic and delayed perception (also offensive) • domination of the technical expertise (ie. Police); • vertical walls and jurisdictional response;
	Power-sovereign (III)	Actions falling under the national cyberdefence: • Creation or expansion of large specialized units or military corps; • Obsessed with critical infrastructures; • development of offensive and defensive capabilities;
National interest		Definition of the national interest or Delimitation of the geopolitical, economic and information assets of a country viewed as critical sectors Threats to: • components of the State, • the sovereignty, • survival of the state, • cyberspace and its components,

Note: Elaborated by our care.

Bibliography

AGENZIA PER L'ITALIA DIGITALE (AgID) (2018)
https://www.agid.gov.it/index.php/en/agency/about-us, accessed June 4, 2018.

BALL Desmond (2011). "China's Cyber Warfare Capabilities". *Security Challenges*, 7(2), p. 81–103.

BAUMARD Philippe (2017). *Cybersecurity in France*. Basel: Springer International Publishing AG, 106p.

BLANK Stephen (2008). "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy*, 27(3), p.227–247.

BUZAN Barry, Ole WÆVER, and Jaap DE WILDE (1998). *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers, 300p.

CAVELTY Myriam Dunn (2014). *Cybersecurity in Switzerland*. Basel: Springer International Publishing AG, 75p.

CRESWELL John W. and J. David CRESWELL (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. London: Sage publications, 304p.

EUROPEAN PARLIAMENT (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* (Text with EEA Relevance), vol.119. OJ L. http://data.europa.eu/eli/reg/2016/679/oj/eng, accessed June 4, 2018.

GORR David and Wolf J. SCHÜNEMANN (2013). "Creating a Secure Cyberspace: Securitization in Internet Governance Discourses and Dispositives in Germany and Russia". *International Review of Information Ethics*, 20(12), p.37–51.

HANSEN Lene and Helen NISSENBAUM (2009). "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly*, 53(4), p.1155–1175.

HJALMARSSON Ola (2013). "The Securitization of Cyberspace. How the Web was Won", *Lund University*, http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=3357990&fileOId=3357996 accessed June 6, 2018.

KEMPF Olivier (2012). *Introduction à la Cyberstratégie*. Paris : Economica, 235p.

KLINGOVA Katarina (2013). "Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia". *Central European University, Budapest, Hungary*. http://www.etd.ceu.hu/2013/klingova_katarina.pdf, accessed June 7, 2018.

LE DRIAN Jean-Yves (2016), Déclaration de M. Jean-Yves Le Drian, ministre de la défense, sur la cyberdéfense, in Bruz on the 13 December 2016, http://discours.vie-publique.fr/notices/163003632.html, accessed February 14, 2018.

LOBATO Luísa Cruz and Kai Michael KENKEL (2015). "Discourses of Cyberspace Securitization in Brazil and in the United States". *Revista Brasileira de Política Internacional*, 58(2), 23–43.

MALLET Jean-Claude (2008). "President of the republic France, and Ministry of Defence France: French White Paper on Defence and National Security". http://archives.livreblancdefenseetsecurite.gouv.fr/2008/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html, accessed February 8, 2018.

PRESIDENCY OF THE COUNCILS OF MINISTERS (2013). *National Strategic Framework for Cyberspace Security*. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf, accessed June 4, 2018.

REUTERS (2018). "France-Le Sénat adopte la programmation militaire 2019-2025". Reuters, May 29. https://fr.reuters.com/article/frEuroRpt/idFRL5N1T03Q1, accessed June 7, 2018.

SECRETARY GENERAL FOR DEFENCE AND NATIONAL SECURITY (SGDSN) (2018). *Strategic Review of Cyber Defence,* http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf,accessed May 22, 2018.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR) - (2018a). *Decennale Intelligence* http://www.sicurezzanazionale.gov.it/sisr.nsf/comunicazione/decennale-intelligence.html, accessed June 3, 2018.

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA (SISR) - (2013). *National Plan for Cyberspace Protection and ICT Security.* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf, accessed June 4, 2018.

THE EUROPEAN COMMISSION (2018). "The Directive on Security of Network and Information Systems (NIS Directive). Digital Single Market". https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, accessed May 29, 2018.

THE NEW YORK TIMES (2007). "A Cyberblockade in Estonia". *The New York Times, June 2*. https://www.nytimes.com/2007/06/02/opinion/02sat3.html, accessed April 6, 2018.

TSAGOURIAS Nicholas (2012). "Cyber Attacks, Self-Defence and the Problem of Attribution". Journal of Conflict and Security Law,17(2), p.229–244.