BASC WORKING PAPER SERIES

INDUSTRIAL POLICY: THE HOLY GRAIL OF THE FRENCH CYBERSECURITY STRATEGY

Danilo D'Elia

Working Paper 2018-05

BERKELEY APEC STUDY CENTER
552 Barrows Hall
University of California
Berkeley, California 94720-1950
September 2018

This paper is part of a project "Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications," organized by Vinod K. Aggarwal and Andrew Reddie of the Berkeley APEC Study Center and funded by the Center for Long-Term Cybersecurity at the University of California, Berkeley. This work is funded by *Airbus Defense and Space-CyberSecurity* and supported by the *Chaire Castex de Cyberstratégie*. For conference support, the author thanks the contributions of the UC Berkeley's Center for Long-Term Cybersecurity, BASC, and Institute of East Asian Studies as well as UC San Diego's Institute on Global Conflict and Cooperation. For comments on previous articles, the author thanks Johannes Fritz, Michael Adams, Prof. Vinod Aggarwal, and Andrew Reddie. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of Airbus.

Industrial Policy: The Holy Grail of the French Cybersecurity Strategy
Danilo D'Elia
BASC Working Paper No. 2018-05

Abstract

The 2008 'White Paper on Defense and National Security' was the first major document to focus directly on national cyber threats as a key risk to France's sovereignty. It defined new priorities – such as cyberattack prevention and response – and established, in July 2009, the National Agency for the Security of Information System (ANSSI) as an inter-ministerial agency with national authority for the defense of information systems. In 2013, a new version of the White Paper reiterated that the capacity to detect and protect against cyberattacks was 'an essential component of [French's] national sovereignty and economic well-being'. The same year, the French government launched an ambitious program and invested considerable efforts and expenditure on cybersecurity industrial policy. This article captures structural characteristics of public-private partnerships and stylizes the different conflicts behind the industrial movements in the 2009-2015 period: representation of digital sovereignty versus corporate interest in global market, national defense champions versus start-up ecosystem.

Keywords: cybersecurity, industrial policy, France, risk management, geopolitics, territory

Danilo D'Elia[1]
Chaire Castex of Cyberstrategy
European Cyber Security Organisation

[1] Danilo D'Elia, Senior policy manager at the European Cyber Security Organisation, is a specialist of public-private strategies related to security issues. He has worked for EADS (now Airbus Defense&Space) on services business (e.g. training, MRO), business development of UAVs, marketing and strategy for the cybersecurity division. His current academic research focuses on the complex system of public-private partnership in the implementation of the French strategy of cybersecurity and he supports the multidisciplinary team of the Castex Chair of Cyberstrategy as research associate. He graduated with a Master in Defense Economics from the University of Paris Pantheon-Assas and is recently completed his PhD at French Institute of Geopolitics.

Introduction

Over the course of the last decade, public administration and private companies in all sectors and of all sizes have faced increasingly numerous, sophisticated, and targeted cyberattacks. Most are clearly motivated by profit, and some come with severe and highly-publicized consequences. They consist primarily of extortions conducted with ransomware, 'fake president' frauds, or the theft of personal data, bank information, intellectual property or trade secrets. Corporate and governmental information systems have also been widely compromised by intelligence activities and strategic espionage, widely documented by several reports and the Edward Snowden revelations in 2013 on the US National Security Agency's massive surveillance program. These increases in cyberattacks are considerably changing the perceptions of cyber risk in France.

At the strategic level, the movement towards a national cybersecurity strategy was launched in 2008. Responding to the need to adapt to an evolving strategic environment, French President Sarkozy initiated a broad review of defense and national security strategy. Thus, the 2008 French White Paper on Defense and National Security identified, for the first time, cyberattacks as one of the main threats to the national security. In addition, cybersecurity industrial capabilities are explicitly mentioned as part of the 'national areas of sovereignty for the maintenance of the strategic and political autonomy of the Nation', at the same level as nuclear deterrence and ballistic missiles [2].

Encadré 1. French White Paper on Defense and Security 2008

« 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 cybersecurity are amongst the priorities. » in French White Paper on Defense and National Security », p.306

Following that the French White Paper, many initiatives have since been launched. In 2009, a specialized agency, the French Network and Information Security Agency (ANSSI) was established under the *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN)*[3] to protectFrench government networks and the network of 'vitally important operators'. For doing that, the ANSSI serves as an inter-ministerial organization and is responsible for coordinating national cyber security effort across key industry and public authorities. In 2011, France published its first national 'Information Systems Defense and Security Strategy'. This document highlighted four major objectives as listed by Table 1 below. These objectives include: becoming a world leader in cyber defense, safeguarding France's decision-making ability through the protection of information related to

[2] France. 2008. 'French White Paper on Defense and National Security', La documentation Fransaise, Odile Jacop, p. 318.

[3] The SGDSN is in charge of assisting the Prime Minister with respect to all domestic and external security policy. Among his missions, the SGDSN 'proposes to the Prime Minister and implements the Government's policy regarding the security of information systems. Secrétariat general de la defense et de la sécurité nationale, 'Textes concernant le SGDSN' <http://www.sgdsn.gouv.fr/site_rubrique58.html>.

sovereignty, strengthening the cybersecurity of critical infrastructure, and ensuring security in cyberspace[4].

Table 1- 2011 French cybersecurity strategy

AMBITION	DETAILS
1. Becoming a world leader in cyber defense	Enhance and perpetuate our scientific, technical, industrial and human capabilities in order to maintain our independence but at the same time France must rely upon a network of allies with whom real-time information can be exchanged on vulnerabilities
2. Safeguarding the national ability to make decisions through the protection of information related to its sovereignty	Ensure the protection and the confidentiality of the national critical information network
3. Strengthening the cybersecurity of critical national infrastructures	Dissemination of technologies already used by the government but also by critical infrastructures
4. Ensuring security in cyberspace	Communicate, inform and convince to increase the understanding by the French population of the extent of the challenges related to information systems security and adapt French legislation to incorporate technological developments and new practices.

Nevertheless, French information systems continued to experience several major attacks against national critical infrastructures, corporate interests and personal data manifested through the operations against Turbomeca (2010), Areva (2011), the Minister of the Economy, Finances and Industry (2011), the Elysée (2012), Astrium (2012), and finally, the revelation of Edward Snowden of foreign intelligence operations – events that all worked towards proving the continued growth of the cyber threat.

In this regard, cybersecurity has become one of the most pressing national security issues. In particular, an analysis of the official declarations and speeches of public authorities and

[4] French Network and Information Security Agency (ANSSI). 2011. 'Information systems defense and security, France's strategy.

security corporate representatives in the 2009-2013 period highlights that cybersecurity is considered a national sovereignty issue for three different but converging scopes: independently securing critical information infrastructures networks is essential to protecting the national territory and the citizens' lives (from sabotage), the privacy of citizens (from foreign surveillance and cybercriminals) and safeguarding national enterprises, and boosting market prosperity (against the threat of economic espionage)[5].

The release of the 2013 White Paper on Defense and National Security is considered a point of crystallization for current French policy on cybersecurity. It was at that moment that cybersecurity became defined as an element of national sovereignty and thus, among the most immediate primary concern for the highest authorities. In addition, the 2013 White Paper underlines the efforts needed to achieve a secure cyberspace and calls for new resources to be dedicated to this domain. Importantly, it clearly states that the development of offensive cyber capabilities is a part of the French cyber defense strategy[6] and that industrial policy is part of the toolbox used to 'master and develop (…) a range of guaranteed trusted products and services'.

Hence, 2013 represents a historic turning point in industrial capability policy in France. First, the government passed the 2014-2019 Military Programming Act which imposed, for the first time in Europe, cybersecurity rules on critical infrastructures. In addition, the same bill provided funding for €1 billion in technical and human resources. Paralleling this legislative action, the public sector launched a vast industrial policy program in 2013. Investments in R&D amounting to 150 million euros were made available and a civil-military Center of Excellence in cyber-defense was established in Brittany.

At the same time, the French government emphasized its willingness to boost national capabilities through the publication of the *Cyber Plan*. This document serves as a roadmap for cybersecurity industrial policy and calls for 17 specific actions split in 4 strategic objectives: increasing the demand of trustworthy cybersecurity solutions, developing a national offering of cybersecurity solutions, boosting the export of these solutions, and strengthening the national industrial ecosystem. These initiatives attest that, in a general context of budgetary restriction of public finances, the public authority is aware of the industrial stakes and decided to take action. Such activism is the first reason to investigate the French case.

The Colbertism Legacy

In addition to political action, the French case is also important due to a tradition of large public aid in the development of the national Information and Communication Technology market. One of the most famous examples is the development and deployment of a videotext terminal called 'Minitel' in 1981, offered by the state-owned *France Telecom*. This service, a precursor to the Internet, was text-based and free to French citizens which

[5] D'Elia D. 2017 « La cybersécurité des operatéurs d'importance vitale : analyse géopolitique des enjeux et des rivalités de la coopération public-privé, Ph.D. diss., Paris- University of Paris 8.

[6] French Government, 'French White Paper on National Defense and Security', 2013 <http://www.rpfrance-otan.org/IMG/pdf/White_paper_on_defense_2013.pdf>.

could use it to chat, make purchases, and conduct online banking. For a long time, Minitel has been the icon of the Colbertism approach to industrial policy. According to E. Cohen (1992) the 'high-tech colbertist tradition' consists of a set of industrial policies implemented during the 1970s and 1980s. Aiming to guarantee the national independence and sovereignty through technological and industrial excellence, high-tech colbertism is characterized by specific public interventionism with the purpose of dedicating resources to further innovation in a given industrial sector (e.g. telecom, aerospace, nuclear and defense), and directly rival among international competitors[7]. 'Grands projects', such as the deployment of optical fiber network or Minitel, have been channels for 'high tech Colbertism' through which the state has directly taken on the responsibility of developing an activity in the place of deficient private initiatives[8].

To summarize, ambition to become a world leader in cyber defense, political awareness of the strategic stakes involved with cybersecurity, and a long tradition for interventionism are key factors which have made the French case interesting in terms of comparing it to other cybersecurity strategies. But what does this emphasis on industrial policy mean? What are the stakes, ambitions and conflicts among the players in the 'industrial game'?

Methodology

Rather than attempting a theoretical analysis, this research aims to begin with the French experience in order to identify key trends and future challenges for the global cybersecurity debate. Over the past few years, academics from fields such as economics and public policy have investigated theories on public goods and cybersecurity[9]. Based on the concepts borrowed from such disciplines, I analyze the recent dynamics on industrial policy through the multidisciplinary approach developed by the French Institute of Geopolitics aiming to study rivalries of power and influence over a territory at various levels of analysis [10]. The Geopolitical approach is based on two main features: the study of conflicting perceptions used to reinforce or defy an established order and the power competition over territories between rival forces[11]. In particular, geopolitics provides us with an important tool for understanding rivalries of power through the analysis of representations. According to Yves Lacoste, representation 'is a construction, a way of seeing things, of assembling ideas in a more or less rational and coherent way with a function to play in geopolitical conflicts.

[7] Cohen, E. 1992, Le colbertisme high-tech. Économie du grand projet, Paris, Hachette Pluriel.

[8] Sachwald F. 1997. 'Colbertism in ICT. Lessons from the French experience', Institut français relations internationales

[9] Some of main references in economics of cybersecurity are: Moore, Tyler et al. 'The Economics of Online Crime,' Journal of Economic Perspectives, 2009; Anderson, Ross, 'Why Information Security is Hard: an Economic Perspective,' Proceedings of the 17th Annual Computer Security Applications Conference, 2001. In terms of market failure see Harris R. and James M. Carman, 1983 ' Public Regulation of Marketing Activitiy : Part I: Institutional Typologies of Market Failure', Journal of Macromarketing, 3:1, June, pp. 49-58.

[10] Lacoste Y, 2014 *La géographie ça sert d'abord à faire la guerre*, Paris : La découverte ,2014

[11] For the question related to the cyberspace as representation of a new form of territory (what are its boundaries, and what are the limits of sovereignty over such territory) please refer to the article of Alix Desforges « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, 2014/1 (No 152-153), p. 67-81.

Although it is based on objective facts, it retains a profoundly subjective character.' In this manner, representations are not neutral; they influence actors since they can serve the strategic aims of some to convince, disturb or mobilize others[12].

Through an in-depth analysis of the French case, I examine the challenges that lie ahead for the French public authorities in achieving the development of a national cybersecurity market. We point out the conflicts between sovereignty, business interests, and privacy — and also take into account the perspectives of various players acting at different levels of analysis (local, national, and global). In addition, the paper attempts to place the French case within the framework developed by Aggarwal and Reddie[13].

1.0 Market, Government or Public-Private Failures?

Two considerations are important here in order to understand perceived economic and political market failures – both by states and private actors. First, industrial policy on cybersecurity has gained a strategic importance at political level for three converging representation of the digital sovereignty. Politicians call for a national offering of cybersecurity solutions because of 'vital interest to protect autonomously national critical infrastructures' (operational side). In addition, the French national cybersecurity market, estimated to be €1.5 billion, is an important economic source of jobs and revenue for the national economy (commercial side). In the context of global competition in the high-tech markets, an indigenous and competitive industry is a factor to support the national economic prosperity. Lastly, the cybersecurity industry, mainly with regard to the military, is a powerful tool of influence, control, and sabotage in the context of geopolitical conflicts.

The second consideration focuses more so on market failures and the perception of why the market is not seen as mature and thus results in the requisition of public intervention.

1.1 Market not yet structured for Responding to Political Needs

In 2012, Senator Bockel released a report highlighting the political issues at the center of the construction of a coherent approach in industrial policy. Following precedents set by the United States and Germany, Senator Bockel suggested the prohibition of the purchase of routers and other network equipment from China which would pose a risk for national security[14]. Thus, industrial independence was put at the heart of France's cybersecurity strategy.

In 2014, Jean-Marc Ayrault, then Prime Minister, declared that: 'The strategy (of cybersecurity elaborated in 2013) responds to the need to strengthen our industrial and technological sovereignty and to support the French offer in terms of security products and services.' Beyond these statements, conveying the idea of an 'industrial reconquest',

[12] Douzet F. 2014 « La géopolitique pour comprendre le cyberespace », *Hérodote*, 2014/1 (No 152-153), p. 3-21.

[13] Vinod K. Aggarwal and Andrew Reddie, 2017 'Comparative Industrial Policy and Cybersecurity: A framework for analysis and the US case'.

[14] Bockel J.-M. 2012, « La cyberdéfense : un enjeu mondial, une priorité nationale », Commission des affaires étrangères, de la défense et des forces armées, n° 681 (2011-2012).

Guillaume Poupard, then director of information systems at the Ministry of Defense -DGA, describes the industrial problem as the impossibility of being able to ‘reproduce the entire supply chain (operating systems, microprocessors, servers, etc.) at national level,’ arguing instead that ‘for the State it is rather a question of developing a national control around a few critical technologies and of relying on integrators able to offer a system secure in its entirety.’[15]
Yet, designing and developing secure products is not a new issue for France. On the contrary, the Hexagon is historically part of the restricted ‘club’ of those who have the capacity to develop and implement, in full autonomy, a governmental cryptography (cyber protection)[16].

Table 2- Governmental Cryptography

CLUB Five-Eyes – using products Made in the US	**Country with industrial capacity of independent government cryptography**	**Countries using NATO certified technologies United States France Belgium**
U.S	France	Belgium
U.K.	Germany	Italy
Canada	Netherlands	Turkey
Australia	Japan	
New-Zealand	Israel	
	Swiss	

What are, then, the modern challenging factors? The convergence of two factors has made the industrial policy a new geopolitical issue. Firstly, there exists a technical-social aspect. ICT penetration in all aspects of society and the economy (industrial control systems/ICS, cloud computing, mobile internet, big data and embedded systems) has led to a change in the scope of cybersecurity which is no longer limited to the military spectrum but has also emigrated to civilian infrastructures. The question faced by public authorities is: how, then, can security solutions previously limited to the military and under national control be democratized? Here representations, including cybersecurity as a public good, play an important role in defining who could - or should - provide this good.

As mentioned by the Chief Information Security Officer of a French critical infrastructure in charge of design and implementing the internal cybersecurity strategy: ‘it is the eternal irony of cybersecurity: while the government has the financial means and the tools to protect its computer networks, for the most part, current attacks tend to be carried out on

[15] Security Defense Business review 2013 « Interview with Guillaume Poupard », N. 90 24 September 2013

[16] Pernot F. and Wolf P. 2016, *Cyberguerre et géographie,* Revue Géographie historique et questions militaires, N°8.

more vulnerable private sector networks. The IT departments of most of France's big corporations are reluctant to take on responsibility for aggressive cybersecurity and far-reaching network monitoring themselves, due to the complexity of the task and the need to use tools that were originally developed for the government'[17].
Another important element is that the state does not have all the necessary skills (R&D laboratories, marketing and business development experts) nor the financial means to protect its own critical infrastructures alone, especially during a period of economic crisis. For these reasons, cooperation with the private sector is essential. Patrick Pailloux, then Director of ANSSI, in his intervention at SciencesPo in 2013, explains that the 'State cannot do everything in the industrial field for all operators'.

The second aspect is the economic context characterized by privatization and globalization. France is integrated in the globalized economy with interconnected infrastructure open to a multiplicity of actors acting on different territorial scales: partners, subcontractors, employees, and users. In addition, private actors manage many critical infrastructures (50% in the case of France) and the sites of these infrastructures are often located on the territory of several nations: for example, Airbus Aviation has seven production and assembly sites in four countries European countries (not counting those in China and the United States).

Now the ICT economy is dominated by foreign players. France and Europe have missed the technological innovation of the 1990s. Thus, Senator Catherine Morin-Desailly referred to 'digital colony' in relation to the European countries which are dependent in technological terms from third countries, mainly the U.S and China. For political and economic players, there arises the question of how to guarantee the security of information, processes and networks in an ecosystem that is now out of control.

It is in this hostile context that the geopolitical question of the stakes of an industry defined as sovereign is inscribed: how can the imperatives of national security be reconciled with the commercial stakes of a globalized market in relation to the interdependence of the economic operators? Are the economic, financial and political instruments implemented up to the ambition of public authorities in order to become world leaders in this sector?

To decipher the complexity of this question and to ascertain the answer to the aforementioned questions, it is first necessary to explain why the market, and in particular, the supply is not mature and what exactly comprises the representation of a sovereign offering.

1.2 Market Analysis

Under only a cursory examination, the cybersecurity market is a heterogeneous market, comprised of highly innovative products and services. Except for certain products, this market is characterized by a global competition. It requires constant and heavy investments in R&D to cope with a rapid evolution and a complexification of threats and technologies. On the other hand, the development and deployment cycles
are very short: between three months and three years.

[17] Interview with the CISO of a electricity operators in France, June 2013 Paris.

In the 2009-2015 period, the market had been profoundly disrupted, both in terms of supply, which witnessed a long series of acquisitions and partnerships, and in terms of demand, which resulted in an increase of 20% over the 2011-2014 period and experienced the emergence of new barriers.[18]
In the early 2000s, the cybersecurity sector was composed, on the one hand, of a demand structured in three segments and on the other hand, by an extremely fragmented offering. In terms of demand, it is structured around three pillars:

a) *Business to Government*: this is the ‘high-grade’ market. Excluding the United States, the value of this segment is estimated between 50 and 100 million of Euros per year / per country. This segment corresponds to classic cyber protection. Sovereign cryptographic mechanisms are at the heart of the state's information systems as well as of weapon systems. The national IT and electronics industries and defense sector integrators like Lockheed Martin in the United States, Airbus in Great Britain and Thales in France play an important role in this market whose privileged clients are government agencies, armies, and intelligence agencies.

b) *Business to Business:* this segment is called ‘mid-grade’, the demand is constituted of large economic operators with strong security and defense needs. They do not have access to the first level due to high prices and inappropriate standards for commercial information systems. In France, this market involves high demand for critical infrastructures demand. In France in 2013, any security provider had a turnover exceeding 10 million euros. The market was dominated by US players with heavy investment in marketing and sales (Fortinet, Mandiant, etc.). In this regard, Joël Noirot, RSSI SNCF notes: ‘on sophisticated tools, the French offer remains limited. In terms of cybersecurity, it remains difficult to do without American technology.’

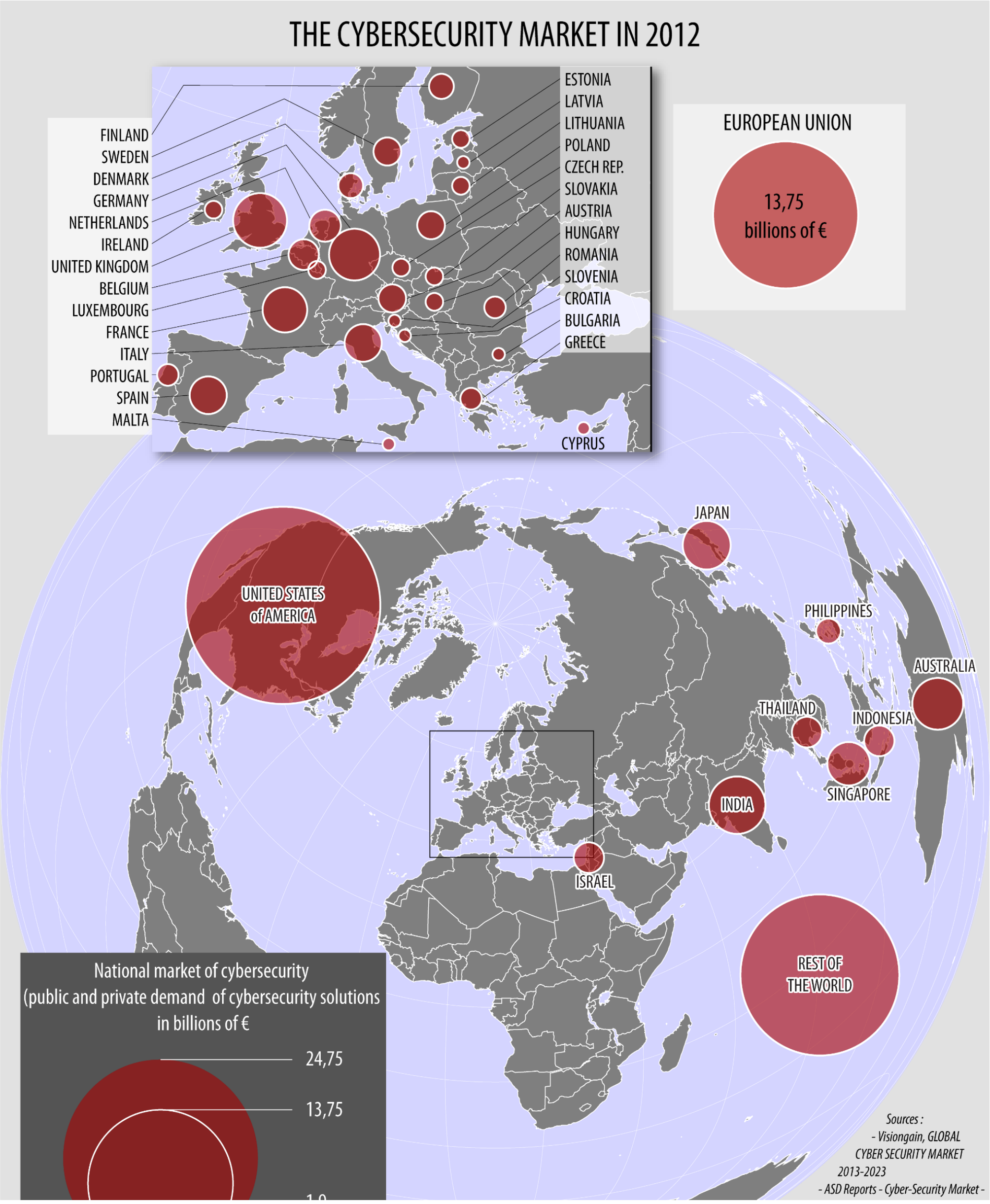
c) *Business to Customer:* here the demand for security is ‘low level’, where the purchase is guided by price / performance ratio and the reputation of the supplier. This segment corresponds in large part to the antivirus and firewalls market and concerns a vast majority of companies. US giants like McAfee (1.3 billion euros of revenue in 2012) and Symantec (2.7 billion euros in 2012) dominate this market segment which is already in the second phase of verticalization or integration in major software editors as demonstrated by the wave of acquisitions in 2010 Intel Security-McAfee (5.7 billion euros), HP-ArcSight (1.1 billion euros) and VeriSign-Symantec (1 billion euros).

[18] Our resources are : Magic Quadrant for Global MSSPs, The Cyber Security Market 2012-2022 – Visiongain; « La cybersécurité Enjeux et perspectives d’un marché en pleine mutation », Xerfi, 2012 ; « Forecast: PCs, Ultramobiles, and Mobile Phones, Worldwide, 2010-2017, 4Q13 Update », Gartner, 2013, IC insights, Major 2013 IC Founderies, 2013 ; Marché des smartphones : Samsung n°1, Apple n°2 au Q3 2013 ~ IDC, Eco Conscient ; Industrial Control Systems (ICS) Security Market Market Forecast & Analysis (2013 - 2018), Market and Market, 2013 ; « La Cybersécurité Europeenne : de l’importance d’une politique industrielle », Jeremy Labarre report to the Council of the European Union 2014

From a geographic point of view, the breakdown of this demand is focused in three major blocks in Western markets: the United States (45%), Europe including Israel (25%), and the rest of the world (30%).

In terms of supply, the market structure is highly fragmented. The players are companies of variable sizes and endowed with numerous niches. The most important ones reaching the billions of euros in turnover are American. Depending on their specialization and their orientation (products / services), we can summarize the typology of the actors around seven categories: software vendors (TrendMicro, Kaspersky), computer hardware manufacturers (CISCO, IBM), technology providers (Qosmos), telecom operators (Orange, BT), consultants and IT service providers (Atos, Sogeti, CrowdStrike), defense players (BAE Systems, Airbus DS, Thales), and companies specialized in a particular market segment (Secunet, Ercom).

Concerning business specialization, we can classify the players according to the capabilities of the cybersecurity cycle: protection (encryption, Identity and Access Management), monitoring and analysis (SOC & NOC, forensic), and detection and reaction (detentions sensors and audit services).



1.3 Market not yet structured for Responding to Operational Needs

This market underwent a turning point in the mid-2000s. Based on a retrospective review of the sector's movements conducted for this paper, since 2008, we have seen a net acceleration of acquisitions, mergers and strategic partnerships.

This movement concerns two main categories of players. First, defense companies, which in a context of restraint of public defense spending, seek to diversify their revenues through partnerships with companies, often SMEs, specialized in a segment of computer security such as detection, consulting or risk management. This was the case in 2008 with the acquisition of Detica - a consulting firm specializing in fraud, risk and financial market security - by BAE System.

Secondly, major editors and integrators embark on a frenetic phase of M&A and partnerships to expand their portfolio. This was the case in 2011 with the acquisition of SecureWorks - a specialist in intrusion prevention and detection - by Dell, a computer manufacturer. This movement is now experiencing a second wave of alliances and acquisitions as evidenced by several moves: e.g. CISCO-Sourcefire (2013), FireEye-Mandiant (2014), and in France, Orange-Atheos (2014).

Such frenzied consolidation of supply can be explained by the awareness of the need for a new type of security. This starts first in the United States following the wave of attacks in 2005 affecting the private sector, including the defense sector. In France, this awareness of cybersecurity issues follows attacks in Estonia (2007) and Georgia (2008). Public actors associated with defense and security are the first to respond followed, albeit slowly, by the private sector in 2013.

Hence, the initial consolidation of the market demonstrates that the supply is not yet mature. No ‘turnkey’ solution exists. Faced with the evolution of a perceived threat as increasingly complex and affecting the industrial control systems, cloud computing, mobile Internet, Big Data, and embedded systems, solution providers are forced to adapt their proposal by considering new areas. For example, anti-virus vendors such as Symantec need to quickly review their strategy, as their solutions prove ineffective against new threats that are classified as ‘persistent and stealthy’ for businesses and critical infrastructures.

In addition, the way in which companies and administrations protect themselves has evolved. We have moved from the concept of perimeter protection (preventing intrusions) to the dynamic concepts of cyber-resilience and defense in depth: security must be carried out from the inside to the outside, through the establishment of multiple lines defense in order to slow down and weaken the attacker.

We argue that the change in the perimeter of cybersecurity and the perception of a more sophisticated threat has resulted in the constitution of a new economic barrier/obstacle that a company must overcome to enter the ‘reshaped cybersecurity market’. Here the major obstacle lies in the need to build a global vision on the overall security of the information systems of the potential customer. This is a first explanation of the dynamism of the market.

Thus, the classic defense providers, especially from the world of C4ISR, embark on the 'democratization' of the solutions developed thus far exclusively for traditional customers (defense, intelligence, etc.). The new approach towards traditional defense companies may be caused by the diversification of their market in time of restrictions on the budgets of the Ministry of Defense. However, it is also a question of adapting and designing a new commercial offer, particularly for critical infrastructures. From a vendor's perspective, this requires going beyond the limited world of defense protection and instead attempting understand new customers (coming from the private sector) in relation to their different priorities (in terms of time and availability). It also requires complete solutions at an acceptable price and with a global vision on business functions, new threats, and technological applications.

From a business model point-of-view, cheap security composed of superimposed layers, like a *mille-feuille* pastry, of 'off-the-shelf' technologies (routers, firewalls, etc.) is no longer valid in the face of greater needs to anticipate, detect and react to evolving and technically sophisticated security threats. In this context, we can explain the partnerships in the world of computer security by examining both defense actors and computer integrators.

1.4 Need for Trusted Solution

Paralleling the need for a global vision, there is another element in France that has taken a major role since 2013: the representation of digital sovereignty which conveys the need for 'trusted service providers'.

The security of information systems, both for public administration and for critical infrastructure, includes elements of confidentiality, integrity, and resilience that affect critical activities at the heart of a company's operations. However, almost all computer systems and associated services are designed and developed in third-party countries, particularly in the United States. Given this situation, how can the French government trust these systems? How can they be defined as effective and robust solutions?

The competitive industrial base which emerged in the United States during the 1990s has given the U.S. a prominent position in the digital economy and has established a strategic gap between the U.S. and other countries - apart from Russia and China, countries which have opted for a wait-and-see attitude towards disruptive technologies. The American industrial supremacy results in an informational advantage exploited for the purposes of economic warfare and during political conflicts (for example, the infamous Stuxnet virus). The United States, thanks also to their industrial supremacy, is and remains the only western 'cyber power'.

1.5 French Market

The analysis conducted by the Alliance de la Confiance Numerique and CoFis (Council of Security Industrial Base) confirm the break-up of the French offer. Still in 2014, the French industrial base is made up of more than 800 actors (100 publishers, 100 equipment manufacturers, and 600 consulting companies), with five major corporate (Airbus, Thales, Atos, Orange, and Sogeti) and more than 600 SMEs with a turnover often less than 5 million of Euros with less than 20 employees. Added to this relatively small industrial base, is the near absence of mid-size companies, with the rare exception of Bertin Technologies.

Although this ecosystem has excellent niches such as the design, manufacture, and validation of security components (Thales, Airbus, CS, BULL) or smart cards (Gemalto, Morpho, Oberthur), it is extremely fragmented. The commercial offer is completely absent in several sectors, such as the supervision and management of attacks, defined as strategic for national security.

In this context, cybersecurity has become a very sensitive political issue. This position, in accordance with the strategic objective to become a world power in cyber-defense, helps explain the French proliferation of political declarations emphasizing the need for 'trustworthy providers' and the launching of numerous initiatives in order to guarantee an autonomous cybersecurity policy. Elite policy-makers encourage the emergence of suppliers capable of developing and deploying controlled solutions (by the public administration) and ensuring a relationship of trust with the customer, particularly with regard to critical infrastructure.

The first question we should investigate is as follows: what are the functions and characteristics of these trusted solutions?

2 INVENTORY of MEASURES Structuring a Complex Dialogue

2.1 Seeking Trusted Solutions

The first pattern of the French intervention in the cybersecurity market involves the government as a participant in the cybersecurity market and in particular as market creating player. The definition of a 'trusted' solution can be found by reading official French government documents[19]. From the point-of-view of national security authorities, a sovereign solution is synonymous with integrity and the highest levels of security: namely, the assurance of the absence of built-in backdoors which would ensure the protection of sensitive information and systems. For that to occur, the government requires 'an evaluation process under the control of the National Network and Information Security Agency'. But, integrity and high-grade requirements alone are insufficient criteria for assuring the commercial success of these solutions.

In fact, the demand for cybersecurity has evolved with the commercialization of the Internet and the pervasiveness of information systems in the industrial world. Since the current demand for security solutions consist mainly of civilian infrastructures, a two-fold need has emerged. Customers are requiring comfort-designed solution compatible with operational technology in conjunction with competitive pricing. As a result, these so-called 'trusted solutions' must be suitable to meet this new demand. The challenge, however, is in achieving the right balance between a commercial solution and high-grade technology solution. To resolve this issue, French authorities have developed a policy based on four pillars illustrated by the Carman & Harris framework: conventional rulemaking,

[19] The following are the referenced documents: Loi de Programmation Militaire 2014-2019, art. 22.; Programme d'Investissements d'Avenir 2013 – Développement de l'Économie Numérique, « Cœur de filière numérique-Sécurité numérique », Octobre 2013; Le guide pour la qualification de Prestataires d'audit de la sécurité des systèmes d'information (PASSI).

organization of public-private partnerships, an R&D funding campaign, and a certification process.

Beginning in 2013, we have witnessed a proliferation of initiatives - both public and private - to structure this ecosystem. Faced with this voluntarism, important questions remain unanswered. Have the resources deployed matched the ambitions displayed? Is the national scale sufficient for the development of an industrial ecosystem? Is the desire to impose national rules consistent with the security needs of private companies?

FRENCH CYBER RESILIENCE EQUATION				
Domain	***Initiative***	***Description***	***Carman & Harris categories***	***Intensity[20]***
Security standard	Working group on ICS security	Working group established by ANSSI (national authority on cyber security) and bringing together all the stakeholders involved in CIIP. Focusing on: security standard, risk management and trusted solutions.	Market Facilitating	++
	Military Program Act 2014-2019 article 22	Security Standards and legal measures to be imposed to CIs: mandatory cartography of the critical information systems; mandatory and regular audits of information systems and networks; mandatory declaration of cyber incidents; implementation of certified sensors.	Market modifying	+++
Education & Training	French Centre of excellence for fight against cyber	The Centre is a PPP focusing on training and involving four companies (CEIS, Microsoft, Orange, Thales) three universities and the Gendarmerie.	Market Facilitating	++

[20] The methodology to define and measure the intensity of industrial policy activities is based on the quantitative and qualitative research made for my Ph.D dissertation. The methodology consist in three steps: 1. Monitoring the 2008-2013 official declarations and speeches of politicians and C-level manager of critical infrastructures operators and cybersecurity providers as well as the initiatives (bills, alliances, industrial partnerships, Memorandum of Understanding etc 2) clustering the 147 declarations and 68 initiatives according to three capabilities (information sharing, material, education&training) and fours territorial scale : local, regional, national and international. 3) evaluating the intensity of the intervention by the state in a specific capability by considering the amount of investment in terms of time (e.g. for passing a bill) and budget, the number of public declarations.

	crime			
	Cyberdefense Cluster	Private company from telecom sector as well as from security and defense will jointly cooperate with the main research laboratories and MoD agencies in promoting innovation and training the future experts.	Market creating	+
			Market facilitating	+
	Chaire Thales Cyber Defense	Research Program founded by private sector (Thales&Sogeti) in cooperation with the MoD. Focusing on cyber defense and developing courses and training for military.	Market facilitating	+
Awareness	Network of cyber defense reservists	Network of reservist made up of about 100 citizens helping in raising awareness, debating and suggesting, organising and establishing events that contribute to making cyber defense a national priority.	Market facilitating	+
	Awareness campaign led by DIRISI	In 2012 the Joint Direction of Infrastructure Networks and Information Systems (MoD) lunched an awareness campaign on cyber risk targeting CIs employees and managers.	Market facilitating	+
	Chaire Airbus Cyber strategy	Research centre founded by Airbus Foundation in cooperation with and the Institute of Advanced Studies in National Defense. Focusing on geopolitics of cyber security and aiming to create a national community of researchers on cyber security issues.	Market facilitating	+
Trusted solutions	Industrial Cyber Plan	ANSSI is in charge to release a road map in order to boost the national cyber industrial base. The aim is to develop a sovereign industrial ecosystem and to develop a strategy in cooperation with the private sector.	Market creating	++
Information Sharing	Club des Directeurs de Sécurité des Entreprises	French Club of Security Managers is a non-profit organization allowing CIOs, risk manager to meet, work and exchange information.	Market facilitating	+
	CERT- FR	French government CSIRT. As such, CERT-FR is the point of contact for all computer-related	Market facilitating	+

		security incidents regarding France.		
Exercise	Piranet	Part of a series of national level crisis management exercises organised by the SGDSN. The aim is to test the crisis prevention and management plans. More than 500 public & private participants.	Market facilitating	++

A coordinated public procurement policy

The second pattern, market making, represents the traditional Colbertims model of government-private sector interaction, even if much more limited in term of market scale. The government as provider of regulation and standard (see below) that condition, or should condition, the French cybersecurity market in proscribing specific activities. In 2013, France passed a law (*Loi de Programmation Militaire-LPM 2014-2019*/ Military Programming Law) that imposed mandatory measures on public and private critical infrastructures. This law, the first of its kind in Europe, required cartography of critical information systems, enforced regular audits of information systems and networks by certified third parties, required a declaration of cyber incidents, and resulted implementation of certified detection sensors. The government simultaneously released internal regulation to impose the purchase of trusted solutions by public agencies.

The aim of these actions, defined as market-modifying, is to raise the demand for national solutions and promote the development of a broad selection of options, thus limiting dependence on foreign suppliers. This action was carefully supported by the national industrial base consisting of a few big corporations (Airbus, Thales, Orange, Sogeti, Bull-Atos) and a large complex of 600 SMEs. For these players, the emergence of an internal market estimated to be €1.5 billion and projected to grow at a 15% to 20 % rate per year has been hailed as an ‘Eldorado/gold mine.’ It is important to note, however that market growth (globally estimated at €68 billion[21]) is occurring in an environment of financial crisis and large public administrative cuts throughout France as well as in Europe. Thus, better structuring the market is seen as an economic opportunity for both the public and private sector[22].

Structuring the public-private partnership

This pattern represents a peculiar interaction between government andprivate action in the new field of cybersecurity in comparison to the traditional industrial policy (e.g. telecom, ICT, nuclear). The democratization of information systems and the interdependence of network infrastructures have resulted in order to meet government needs to develop a coordinated approach between different players involved in cybersecurity, to include

[21] The Future of Global Information Security, Gartner Security Scenario Research 2014.

[22] D’Elia D. 2016, ‘Public-private partnership: the missing factor in the resilience equation. The French experience on CIIP’, In: Panayiotou C., Ellinas G., Kyriakides E., Polycarpou M. (eds) *Critical Information Infrastructures Security. CRITIS 2014. Lecture Notes* in Computer Science, vol 8985

private infrastructure operators, industrial control systems (ICS) providers, maintenance firms, security companies, and many more actors[23].

The French authorities were already aware of this in 2008 when the White Paper on Defense and Security Policy recognized that the State no longer had the full power to take action against threats it faced and as a consequence, needed to develop a better relationship with the private sector. In 2010, ANSSI conducted a series of interviews on ICS security with CI operators, security suppliers, and ICS vendors. A long process was thus initiated to address the following question: how to develop and maintain a trusted information system based on (a few) national and international technological bricks?

The aim of the interviews was to draw a shared understanding of the limits of the current solutions and where the best practice was to be found. Thus, the information sharing within the selected players contributed to the understanding of the future requirements, so that national authorities can establish new standards and industry can work to offer tailored solution for CIs.

However, during the first year, language and culture differences among infrastructure operators, public authorities, and security providers emerged and strengthened the need for a permanent exchange. Financial efforts were thus accompanied with reorganization of the public authorities in charge of the information security. In 2011, ANSSI recognized this need, and therefore created a department dedicated to fostering cooperation with the private sector around twelve defined critical sectors as well as established an office dedicated to the industrial policy. Additionally, moving beyond different languages and interests, in 2012, a permanent exchange platform was established with 25 players (SCADA Working Group). On a voluntary basis, ANSSI brought together the main stakeholders from government (ANSSI and MoD representatives) and industry (SCADA providers, national CIs and security suppliers) to develop supply chain risk management best practices that can apply to CIs. The long-term goal of the SCADA WG is to be able to label the next ICS and prepare the CIs for the standards imposed in 2013.

Additionally, another important initiative should be mentioned, one which aims to encourage cooperation and dialogue between public and private players: the establishment of the Council of Security Industrial Base (*Comité de la filière des industries de sécurité-COFIS*). In response to demand from the private sector, the Prime Minister launched the COFIS in 2013, an initiative that brings together all stakeholders involved in the security industry, from government agencies to trade federations and CI representatives, in order to meet the needs of the market and to structure the security supply chain.

The most recent initiative is the Cybersecurity Industrial Roadmap, referred to as the 'Cyber Plan.' This broad policy program, consisting of seventeen actions around four strategic goals is designed to boost 'the national demand of trusted solutions, development of a national offer, structuring the export approach, and consolidating the national industrial complex.' The group hoping to implement this plan, while led by ANSSI, is comprised of both private and public-sector representatives. Again, the main goal of this initiative is to

[23] D'Elia D., i*bidem.*

bring together a wide spectrum of players interested in industrial policy: providers, users, shareholders, regulators, customers, and investors.

The common goal of these actions is to pursue the mutual understanding of various interests and the convergence of opinions and perspectives to adopt minimum-security standards. In the process, these initiatives aim to reduce the gap between the government's lack of technology and the operators' lack of security to contribute to a better assessment of future needs for security providers.

The certification activity as process of clarification about the market

The certification process, led by ANSSI in its capacity as national authority, is viewed as a strategic way to ensure confidence on trusted solutions. According to the official declaration, the certification and qualification activities led by ANSSI aim to help users choose 'trustworthy solutions' by providing them with the necessary information to clarify their needs and then identify the appropriate robust and trustworthy solutions. The certification and qualification activities are thus supporting the implementation of the 2013 legal framework by CI operators. ANSSI, supported also by third-party IT security evaluation facilities, tests the integrity of security solutions and vendors with the aim of bringing transparency to suppliers that should be embedded in the CIs. In this way, ANSSI, through the expertise acquired on the field, promotes and drives the development of a trusted supplier base, and evaluates and produces services to determine which should be commercialized. As part of this process, potential customers choose their trusted solutions among the catalogue established by the national authority. With these trends in play, the public authority aims to structure the offer available on the national market. In particular, three specific security segment are targeted by the certification process: audit (*Prestataires d'audit de la sécurité des systèmes d'information -PASSI*) incident response (*Prestataires de réponse aux incidents de sécurité qualifiés - PRIS*), and detection (*Prestataires de détection d'incidents de sécurité PDIS).*

The certification process aims to demonstrate the robustness of product that has been evaluated through extensive penetration testing and in-depth analysis to ensure that solutions are compliant with the corresponding standards and to demonstrate the product's resistance to a given level of cyber-attack.

The qualification process aims to attest the compliance with the regulatory, technical and security requirement promoted by ANSSI (e.g. 2013-2019 Military Programming Law, General Security Terms of Reference-RGS). It can be defined as the French state's recommendation of cybersecurity products or services that have been proved and approved by ANSSI.

In parallel—and to promote the certificated solutions—ANSSI established a label 'France Cybersecurity' and a related catalogue that facilitates marketing towards the consumers. According to official statement, 'The France Cybersecurity Label is the guarantee for end users that the certified products and services are made in France and possess clear and well-defined functionalities, with a level of quality established by an independent panel.' The final goal of this accreditation is to be able to index and promote French cybersecurity solutions for the internal and export market. Since the accreditation's official launch in January 2015,, it has been awarded to more than 70 products (firewalls, encryption and identity management tools, application security, etc.)[24].

The outcomes of these initiatives directly impact risk factors: elaborating the secure design of new solutions leads to reduce the technical vulnerabilities. On the other hand, the implementation of trusted products, as detection sensors, generates more countermeasures and a broader view of frequency and gravity of cyber-attacks. Finally, this means fundamentally promoting national solutions labelled and reduce risks for the network infrastructure.

Orienting the R&D

To ensure continuous investment in R&D, the state has increased its efforts with regard to both civilian and military investments. The Ministry of Defense has tripled research credit (€30 million in 2014) over a two-year period. In parallel, the *Program for the Future Investments* (2013) has called for projects categorized as 'Digital Security' which has thus far yielded 18 distinct proposals. Through a fund of €20 million, this initiative aims to guide investment in R&D and thus promote the development of offers that have been absent thus far. This includes the implementation of capacity requested by the LPM 2014-2019. In continuation of this strategy, the Cyber Plan envisages a new wave of calls for projects for 2015 in order to develop two to three new deals per year.
In addition, a flagship project was announced and funded by the Minister of Defense in 2013. The project aims to structure a regional cluster focused on the cyber defense in Brittany and based on the concept of triple helix. Private company from telecom sector as well as from security and defense will jointly cooperate with the main research laboratories and MoD agencies in promoting innovation and technological development. On the one hand, the private sector will drive scientific developments; on the other hand, the public sector will shape the innovation through supporting policies and relevant research. In fact, a comprehensive approach cannot disregard the academia contribution: cybersecurity needs continuous research and education, mission and task normally belonging to the academia. In parallel, training of future experts will find an important place in the Cyber Defense Cluster: private servants are participating with national authorities in drafting the cybersecurity syllabus for national cyber defense center of excellence. The possible impact of this policy on the cyber risk is clear: the public-private cooperation aims to reduce the vulnerabilities (in process and human action) and to develop (human) countermeasures.

3.0 State-Society Dynamics

The aim of this section if to investigate the problem associated with the government intervention in the market to address market failures analyzed in the first section. In particular, we scrutinize the main challenges associated with the implementation of the industrial policy as seen by public authorities through the lens of the framework developed by Vinod K. Aggarwal and Andrew Reddie 2017.

[24] The catalogue is available via the following link : https://www.francecybersecurity.fr/wp-content/uploads/2017/01/FCS_Catalogue_2017_WEB.pdf

3. 1 The Limits of the High-Tech Colbertism

The analysis of the initiatives launched in the 2009-2015 period stresses the legacy of the 'French High Tech Colbertism'[25]: the post II World War strategy of catching up on industrial backwardness based on the idea of mastering major technologies. This model, developed for thirty years, was structured around large projects basically based on public order. This was itself supported by the national preference for the emergence of national champions benefiting from public funding in research. In particular, the French economist E. Cohen identifies the main patterns of the Colbertism approach. First, the State initiative is led by the creation of a specific administrative body (e.g. the reorganization of the Telecom Ministry for the development of telephone equipment during the 70s). A second feature is the large R&D investment by the state to the 'grand project' (e.g. Militel). Third, there is a pattern for innovation-industry integration through the public capacity to impose national goals to corporate through technology transfers, public procurement, and export promotion.

This paper has demonstrated that cybersecurity, in the 2000s, became a top political priority, thus initiating an ambitious catching-up effort beginning in 2013. The analysis of industrial policies addressing cybersecurity highlighted as France's vision and policies in cybersecurity have been strongly influence by the traditional structure of its innovation policy, with some elements in common with the past Colbertism approach. However, the success is not easily replicable since both the geopolitical (including internationalization and privatization of critical sector of activities) and technological context have changed. From the economic point of view, technologies, as well as demand are much more uncertain and ANSSI does not possess the necessary entrepreneurial and commercial abilities.

Hence, cyber industrial policy depends on many other variables that public can impact only through a coordinated approach with private players. Therefore, comprehensive policy is needed, policy that requires the implementation of various actions at different levels in order to structure the market. These actions include: implementing law to boost demand, developing education and R&D to structure expertise and capabilities, and the organization of dialogue and the certification process to support a trusted offer. In addition, as demonstrated by the evolution undertaken by ANSSI in 2009-2013, dealing with cybersecurity requires to be adaptive. In such way ANSSI covers different roles: being the police man (conducting the inspection), the conventional rule-maker (boosting the demand and helping the market to understand the measures to be implemented) or the facilitator (to develop the technical solution). However, a more in-depth analysis reveals important tensions that might be potentially damaging the implementation of the industrial policy.

3.2 Sovereignty versus Business Interests

On the private side, an increasing number of critics have been condemning the regulatory-based approach without taking into account market drivers. Due to the deregulation of the public sector in the 1980s and globalization in the 1990s, the private sector is now owning

[25] Cohen E. 1992, Le colbertisme high-tech. Économie du grand projet, Paris, Hachette Pluriel.

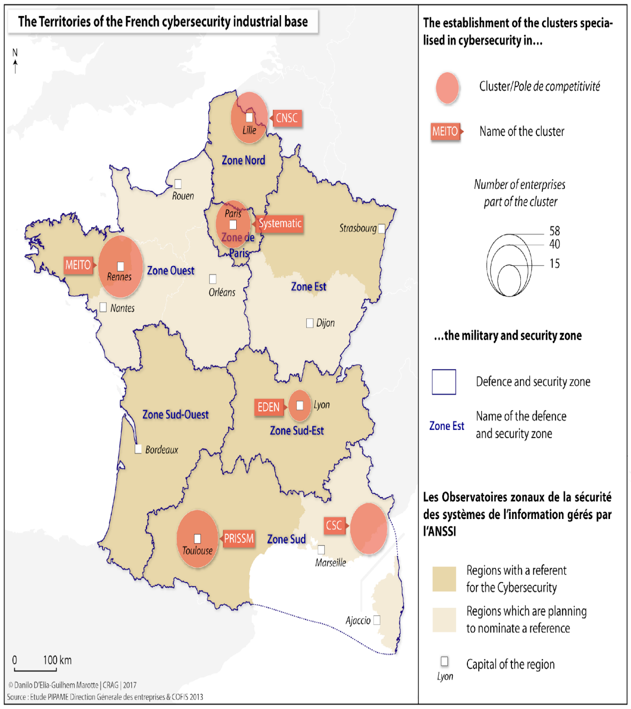
or controlling the majority of vital infrastructure, many of which have multi-domestic sites. Thus, the primary interest of CI operators is to employ solutions broadly adequate for their multinational plants.

At the same time, for security suppliers, their concern is focused on developing solutions that can be sold on the international market while simultaneously amortizing R&D costs. This is where corporate interests clash with national security and highlight the need for more international cooperation. Since cybersecurity is defined as matter of national sovereignty, governmental powers are imposing new constraints to CIs. In addition, they are influencing the development of national technologies that should fulfill national standards with high-grade requirements demanding a lot of investment. The consequences are relevant with regard to the private sector: limitation of foreign investment, increasing cost to implement a multitude of national standards and more constraints on the development of national solutions.
Given that national demand and the R&D budget are a fraction of the multibillion-dollar budget of the American and Asian market, security vendors are calling for decreased regulation and a more business-oriented, balanced, and neutral regulation framework. Regarding the last element (neutral regulation framework), some industry associations like AFDEL (*Association Française des Editeurs de Logiciels et de Solutions Internet*) have revealed that the certification process could be an economic burden. Firstly, this economic burden may arise since many of the French players are SMEs with low human and financial resources, and thus are unable to complete the long and costly certification process. On the other hand, from a (political) marketing point of view, the certification released by ANSSI could be a double-edged sword: it could be a sponsor for the countries/critical infrastructures looking for 'NSA-proof' solutions, but on the other hand, it still means that a public authority – in this case the 'French brother'- will control the technical specification of the French solution. This leads to the following political question: what exactly is the most appropriate scale for international cooperation and how can a 'good' partner be defined? Is the European Union the most appropriate level for cooperation or would it be more valuable to establish a trusted group of partners on the basis of mutual acceptance of national standards? Nevertheless, cybersecurity for national strategic assets remains a national responsibility and in the case of sensitive domains such as cryptography, this would mean continuing the development of country-specific solutions. Hence, there is a strong link between cybersecurity solutions and sovereignty matters for the Member States which result in lack of cooperation and lead to increased market fragmentation. The issue is complex, and the debate is still on-going in Europe (ref. the article of Paul Timmers on the European Industrial Policy in this same special issue)

3.3 When the Size of the Market Matters

Small and medium enterprises (SMEs) are the engine of innovation in the cyber domain. Due to their structure and innovative nature, they are an essential element necessary to combat the extremely rapid evolution of threats and technologies. This reason explains the importance of the relationship between SME and big corporations in building the cybersecurity ecosystem. Although it is not specific to the cyber domain, this point becomes important for the French case because of the current situation and fierce competition in international markets.

Figure 2: The territories of the French cybersecurity industrial base


The Territories of the French cybersecurity industrial base
N
CNSC
Lille
Zone Nord
Rouen
Paris
Systematic
Zone de Paris
Strasbourg
MEITO
Rennes
Zone Ouest
Orléans
Zone Est
Nantes
Dijon
Zone Sud-Ouest
EDEN
Lyon
Zone Sud-Est
Bordeaux
CSC
PRISSM
Toulouse
Zone Sud
Marseille
Ajaccio
0 100 km
The establishment of the clusters specialised in cybersecurity in...
Cluster/Pole de competitivité
MEITO
Name of the cluster
Number of enterprises part of the cluster
58
40
15
...the military and security zone
Defence and security zone
Zone Est
Name of the defence and security zone
Les Observatoires zonaux de la sécurité des systèmes de l'information gérés par l'ANSSI
Regions with a referent for the Cybersecurity
Regions which are planning to nominate a reference
Lyon
Capital of the region

© Danilo D'Elia-Guilhem Marotte | CRAG | 2017
Source : Etude PIPAME Direction Générale des entreprises & COFIS 2013

In the 2009-2015 period, our research observed the emergence of six clusters specialized in cybersecurity which together are gathering more than 400 companies. The clusters are based at regional level and following a specialization in cybersecurity (see map below). The challenge for the public-private cooperation is to ensure coherence between the regions to avoid wasting resources and to be more competitive in the different segments. According to the representatives of the clusters confirms that the presence of several clusters feeds rivalries between regions (Bretagne Vs. and Nord-Pas-de-Calais) for position itself as a leader at national level and attract European funding. The French market alone is not sufficiently structured to guarantee cohabitation between national competitors and these rivalries could limit a coherent approach to export.

In fact, the national market is too tight, and despite the presence of many innovative SMEs, they are not able to reach a critical mass due to the lack of the national demand. According to an AFDEL representative: 'French cybersecurity vendors don't ask for much more investment in R&D, what we still miss is national administration and infrastructures purchasing French solutions.' In this context, national market seems to be too limited to be competitive, but how States and industry can build confidence between nations and develop a larger 'Single market'? What can Europe do through regulations and interventionism to consolidate the market? These questions are pressing, because foreign technologies dominate the national market and are consolidating their position. Moreover, the absence of a culture adapted to the new market is at the heart of the difficulties of coordination between SME and big corporations to bid jointly: times and methods of development, sales channels and culture management are not the same on cybersecurity market. Additional complexities arise in the case of acquisitions or mergers of SMEs: French large industries have difficulty in managing the integration of staff and maintain innovative technologies for SMEs. The result is that many SMEs are acquired by foreign competitors or they stop investing altogether.

5. Conclusion

In conclusion, the French case is striking for a least two reasons. Firstly, in France, which is the first case among Western countries to impose new rules on critical infrastructure operators, there are a number of reasons behind the implementation of industrial policies which include market fragmentation, corporate interests, and national security, reasons that are coupled with the ever-increasing issues of technological independence and privacy protection. It is important to keep in mind the different and often conflicting arguments supporting such actions.

Secondly, a dynamic analysis reveals, on the one hand, the willingness of public authorities to control the cybersecurity mechanism, and on the other hand, also demonstrates the limits of public interventionism. In addition, the French case highlights the need to find the balance between national sovereignty and business interests at the international level. Given that industrial policy needs to take in account market driven objectives (to be competitive) and equally important objectives linked to societal (data protection) and technological independence concerns (the protection of CIs through trustworthy technology), the research regarding finding this balance is a hard task. It is further complicated by the fact that businesses operate across borders while law enforcement agencies are nation-based.

In the end, the traditional Colbertist policies are not adopted anymore and public control over corporations has become more and more difficult to achieve. Such context explains a fundamental reaction of industrial policies since national market and national resources have become insufficient to guarantee competitive solutions. Both public authorities and private players have acknowledged the consequence of globalization, and reaction has been to turn to the European market which is investigated further in this journal.

REFERENCES

Anderson R., “Privacy versus government surveillance: where network effects meet public choice”, Presented at the 13th Workshop on the Economics of Information Security, Jun 2014, Pennsylvania State University, United States. [Online]. Available: http://weis2014.econinfosec.org/papers/Anderson-WEIS2014.pdf

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," BASC Working Paper Series, 2018-01.

Aggarwal, Vinod and Reddie, Andrew (2018) "Comparative Industrial Policy and Cybersecurity: The U.S. Case," BASC Working Paper Series, 2018-02.

Bloma M., Castellaccia F., Fevoldenb A.M., “The trade-off between innovation and defense industrial policy: A simulation model analysis of the Norwegian defense industry”, in Technological Forecasting and Social Change, Volume 80, Issue 8, October 2013, Pages 1579–1592

Buigues P-A. and Sekkat K., I*ndustrial Policy in Europe, Japan and the USA Amounts, Mechanisms and Effectiveness*, Palgrave MacMillan, New York, 2009
Castelluccia C., S. Grumbach, L. Olejnik. (2013, June) “Data Harvesting 2.0: from the Visible to the Invisible Web”. Presented at the 12th Workshop on the Economics of Information Security, Jun 2013, Washington, DC, United States [Online]. Available: https://who.rocq.inria.fr/.../WEIS13-CGO.pdf

Cohen, E. 1992, Le colbertisme high-tech. Économie du grand projet, Paris, Hachette Pluriel.

D’Elia D., “Public-private partnership: the missing factor in the resilience equation. The French experience on CIIP”, In: Panayiotou C., Ellinas G., Kyriakides E., Polycarpou M. (eds) *Critical Information Infrastructures Security. CRITIS 2014. Lecture Notes* in Computer Science, vol 8985.

Desforges A. 2014 « Les représentations du cyberespace : un outil géopolitique », *Hérodote*, 2014/1 (No 152-153), p. 67-81.

Douzet F. 2014 « La géopolitique pour comprendre le cyberespace », Hérodote, 2014/1 (No 152-153), p. 3-21.

Dunn Cavelty M., *From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse*. International Studies Review, 15(1), 2013, 105-122. A. Friedman, *Economic and Policy Framework for Cybersecurity Risks*, Brookings, July 2011.

Eliasson G, “Industrial policy, competence blocs and the role of science in economic development”, in Journal of Evolutionary Economics (2000) 10: 217- 241

Floridi L., *Information: A Very Short Introduction*, Oxford University Press, 2010.

Floridi L., *The Online Manifesto, Being Human in a Hyperconnected Era*, Springer, 2015

France White Paper on Defense and National Security, La documentation Francaise, Paris, 2008, p.174.

Hathaway M. Demchack C, Kerben J. McArdle J. and Spidalieri F. 2016. "Frane Cyber readiness at a glance", Potomac Institute for Policy Studies.

Lacoste Y., *La géographie ça sert d'abord à faire la guerre*, Paris : La découverte ,2014.

Maurer T., Morgus R. and Skierka I., "Technological Sovereignty: Missing the Point?, An Analysis of European Proposals after June 5, 2013.

Omand D., *Securing the State*, London Hurst 2010.

Rid T., *Cyberwar will not take place*, Oxford University Press, 2013.

Schneier B., A Fraying of the Public/Private Surveillance Partnership, available at https://www.schneier.com/blog/archives/2013/11/a_fraying_of_th.html (accessed on 30 November 2013) and The Battle for Power on the Internet, The Atlantic. Available at: http://www.theatlantic.com

Vinod K. Aggarwal and Andrew Reddie, 2017 "Comparative Industrial Policy and Cybersecurity: A framework for analysis and the US case".