The Economics of Cybersecurity: From the Public Good to the Revenge of the Industry

Danilo D'Elia(✉)

University of Paris VIII Vincennes-Saint Denis, Paris, France
deliadanilo@gmail.com

Abstract. In the aftermath of Edward Snowden's intelligence revelations, many governments around the world are increasingly elaborating so-called «digital sovereignty» policies. The declared aim is to develop trusted technologies to protect the more sensitive networks. The ambition of this article is to turn over the complex- and often contrasting- motivations and interests behind the industrial policy movements, explain how the dominant representation of cybersecurity as public good is impacting the public policy and analyse the dynamics between private and public players.

Keywords: Cyberspace · Public policy · Risk analysis · Critical infrastructures

1 Introduction

We live in the information age; everyone knows the advantages we enjoy from that. What is still blurred is the cost and the risk of our dependence upon the online life. As aptly stated by the philosopher Floridi, with the development and the massive penetration of ICTs in all advanced economies, people and engineered machines are now continuously connected with digital network and part of the same global environment made of information: the infosphere [1].

In addition, the same information infrastructure underpins the assets and services considered as vital to the essential functioning of industrialised economies, and make them interdependent. From power grids to banking systems, from traffic light controller to water distribution, the information assurance of data, networks and protocol of those infrastructures has become the central nervous system of our society. The internet of things (50 billion of devices to be connected to the internet in 2030) and the concept of smart city show the complexity of this interdependence that knows no sign of slowing.

Now, if the pervasiveness of ICTs in our daily life has many advantages because facilitate social and economic activities, there is also a downside. The infosphere has come with new risks that are changing the nature of cybersecurity from a technical issue for a restricted expert-community to a social-political one.

In fact at the origin, security was not a priority for the ICT's developer and this has led to two interrelated levels of risk. The first one is the danger of systems failure and the cascading effects. Due to the interdependence of critical infrastructures (CIs), the impact of an incident won't be limited to the original sector of activity nor to a national

A. Bécue et al. (Eds.): CyberICS 2015/WOS-CPS 2015, LNCS 9588, pp. 3–15, 2016.
DOI: 10.1007/978-3-319-40385-4_1

border. For instance, in November 2006 a shutdown of a high-voltage line in Germany resulted in massive power failures in France and Italy, as well as in parts of Spain, Portugal, the Netherlands, Belgium and Austria, and even extended as far as Morocco, affecting ten million customers in total.

The second risk is given by the potentially malicious actors exploiting technical vulnerabilities. Beyond the hacktivism (politically motivated) and criminal (monetization earning) threats, the major challenges come from the espionage - both political and economic- and sabotage. These threats raise a wide range of questions linked to national security (critical infrastructures protection), economic prosperity (security of business secrets) and privacy issues (data protection).

Over the course of the last decade, the increasing sophistication of attacks, the disclosure of large intrusions to corporate, and the latest revelation to the global public the massive network exploitation by Western intelligence agencies have considerable changed the threat perceptions. As a result, the cybersecurity has become a complex political question and is increasingly perceived as a public good by many governments [2].

Of the various consequences of this situation, one particular trend has emerged, especially in Europe: the need to implement industrial policy in order to develop national-base technologies to protect independently the critical information networks from the challenges aforementioned.

Rather than attempting a theoretical analysis, the ambition of this research is to start from a specific case study (the French experience) in order to point out some key trends and future challenges for the global debate on cybersecurity. In fact, over the past years academics from economics and public policy have already investigated theories on public good and cybersecurity[1]. Based on the concepts borrowed from such disciplines we analyze the recent dynamics on industrial policy through the multidisciplinary approach developed by the French Institute of Geopolitics [3]. This 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.

In the following, the arguments unfold as follows. First, we will outline the conceptualization approach: the meaning of the cybersecurity as representation of public good. We identify the changes in how, in the post-Snowden era, the cybersecurity discourse and the cyber security market are perceived.

Then, through the in-depth analysis of the French case, we analyze the rivalries challenging the emergence of the national market on cybersecurity. We point out the conflicts between sovereignty, business interests and privacy. Dealing with national industrial policy of cybersecurity is ambitious because it means understanding the points of view of various players acting at different layers (local, national, global). Find the good path is thus complex and this article aims to help the understanding. In conclusion, we reflect on the definition of efficient public-private partnership and the new role of the citizen on the economics of cybersecurity.

[1] Some of main references in ecomics 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.

2 The Cyberspace as "Open-Bar Market" for Some Brothers

There is a common refrain about the cybersecurity origin: Internet and the information systems were not designed with security in mind. Therefore, this has led to the risk given by the potentially malicious actors exploiting vulnerabilities. These actors comprise generally four categories: state or state-sponsored actors, insiders, organized or individual criminals and politically motivated non-state actors.

2.1 The Risk of the Online Life

The sabotage and espionage are widely considered as the major challenges for the nation states [4].

For the former one, the growing interconnection with the Internet and the IP convergence result in the shift from largely proprietary isolated systems to highly interconnected and based on commercial-of-the-shelf hardware and software. That has left CIs vulnerable to cyber attacks. So far, Stuxnet malware in 2010 and the recent attack against a German steelworks remain the only publicly-acknowledged destructive attacks and unexpected disruptions of normal life are still more likely to come from accidents or natural hazards than from deliberate sabotage[2]. However, over the last five years, the number and the sophistication of the attacks doesn't stop to increase[3], thus the most demanding scenario is that where the risk is systemic: again, the hyperconnectivity of our society and existence of vulnerable supply chains raise the prospect of disruption having impact on the society as a whole.

Cyber espionage is the second serious threat. Here the main concern is on long-term consequences of massive exfiltration of trade secrets and confidential data for activities that are at the core of advanced economic development such as defence, finance, energy and high technology sectors. Moreover, the intelligence services worry because the information collected through targeted network attacks could facilitate a large scale attack during a conflict situation. Finally, the issue is not just economic but becomes of national security nature.

Beyond the vulnerability exploitation but strictly related to the risk of espionage, two additional features have to be detailed here: the contradictory roles of national authorities and the ambiguous role of tech-corporations handling personal data. Both of them have come to the foreground in June 2013 when the former NSA contractor Edward Snowden's revelation disclosed the Internet surveillance programs established by U.S. intelligence agencies and in cooperation whit their closer allies.

[2] According to the 2014 German IT Security Report released by Federal Office for Information Security, a cyber-attack that caused significant damage in an steel facility in Germany. For a detailed analysis see Robert M. Lee, ICS Cyber-Attack on German Steelworks Facility and Lessons Learned, 17 December 2014.

[3] According to research conducted by US ICS-CERT, in 2012, 197 cyber incidents were reported by asset owners or trusted partners to the US Department of Homeland Security. In 2013, the incidents were 257. Moreover, at every security conference, information technology experts disclose new vulnerabilities and demonstrate how sabotage of ICS got easier.

Protecting against the cyber threats has led to a contradictory practice and has revealed the schizophrenic conduct of national security authorities. In many countries (35[4]), intelligence services and defence agencies are developing offensive capabilities: to achieve that, they buy and exploit zero-day vulnerabilities in current operating systems and hardware. In addition, as revealed by Snowden, the US government, either cooperating with domestic internet companies or secretly, cracked existing and contributed to new vulnerabilities in widespread encryption systems. All these initiatives, launched for national security interests, are making cyberspace more insecure for everyone: the exploitation of vulnerabilities has the potential to undermine trust and confidence in cyberspace overall as backdoors could be identified and exploited by malicious actors and thus reduce the resilience of the entire system. This situation makes the cyber risk assessment clearly more complex.

In addition, the disclosure of June 2013 highlighted the political role of the big American platforms in collecting and retaining user's entire online life. We know as personal data have become the "crude oil" for the economy of the information society. As aptly analysed by the INRIA research team [5], the American giants in search engine, social networks, clouds, etc. have developed a business model based on network effect (both direct and indirect) and private data as "virtual currency" in exchange for services.

Thanks to their increasing ability to collect, store, analyse personal information, the most important internet services (like Google, Facebook, Twitter, Amazon, etc.) raised a dominant business position transforming users' data into added value: often in selling targeted online advertising reaching a global audience.

But what it isn't always clear is that beyond the economic effects, there are also important strategic consequences. These corporate know more that anyone about people's commercial interest, their political and societal preferences, their networks of friends and wishes…and all that without any security clearance. For this reason, intelligence services that are generally prohibited by law from asking private data without a judicial authorisation, are extremely interested in enjoying the same network effects of the internet companies and thus in having access to the users' data. The sale rationale is behind the proliferation of surveillance programs like those revealed in June 2013 [7].

If seen on the political level, it's clear if one nation relies mostly on foreign Internet platform, this leads to let a large amount of their data be exploited outside their jurisdiction. According to the INRIA research (Fig. 1), the result is strong information asymmetries between those who (U.S.) import the "raw material" and transform in gold and those who (European countries) sell for free their resources.

This explain why the information advantage on data harvesting make the domination of US-based companies a threat to sovereignty and why the topic has come under scrutiny by European states.

2.2 June 2013 as Starting Point for Shaping an Industrial Policy

In addition to the European dependency on ICT developed and based elsewhere for the data gathering, another important risk came up in the last years. Many consulting

[4] This is the analysis made by the McAfee expert, Jarno Limnéll, NATO's September Summit Must Confront Cyber Threats, 11 August 2014.

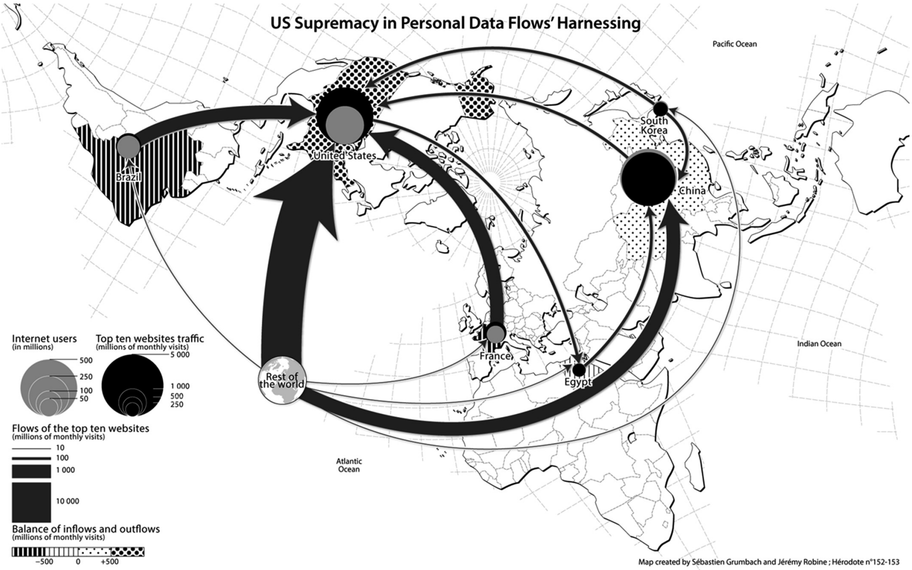

US Supremacy in Personal Data Flows' Harnessing
Pacific Ocean
United States
Brazil
South Korea
China
France
Egypt
Rest of the world
Indian Ocean
Atlantic Ocean
Internet users
(in millions)
500
250
100
50
Top ten websites traffic
(millions of monthly visits)
5 000
1 000
500
250
Flows of the top ten websites
(millions of monthly visits)
10
100
1 000
10 000
Balance of inflows and outflows
(millions of monthly visits)
−500
0
+500
Map created by Sébastien Grumbach and Jérémy Robine ; Hérodote n°152-153

Fig. 1. Geopolitical Map on US Supremacy in personal data flow's harnessing (S. Frénot and S. Grumbach, Les données sociales, objets de toutes les convoitises, in Hérodote, n° 152–153, Paris 2014.)

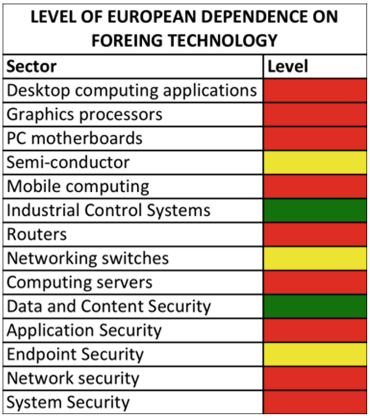
studies (Table 1) confirm global suppliers, mainly form U.S., Asia and Israel, are dominating the cybersecurity supply chain market while European nations are straggling behind.

At the political level this problem has been addressed as a strategic issues by national and European documents[5]. If securing critical infrastructures networks is essential to protect lives (from sabotage) and privacy of citizen (from surveillance) and to boost the market prosperity (against economic espionage), the dependency on foreign technologies without full confidence that the devices do not include built-in backdoors or are applying the same level of quality requirement is a strategic issue.

Now what changed with Snodwen's affair is the increasing perception that technology control means sovereignty. On one hand, the disclosures of three particular NSA programs (PRIMS, MUSCULAR and TEMPORA) revealed an embarrassing relationship between the major U.S. internet corporates and the American national security agencies providing the NSA with access to the data of their services. The result, confirmed by many political declarations, was a loss of confidence in U.S. based companies. According to some reports, a first economic consequence was the lost revenues (22–35 billion of dollars) in cloud outsourcing business for many American

[5] According to the 2013 European communication on «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace» "there is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers".

Table 1. Red color means "totally dependent on", yellow color means Whit low position within the global market <10 %; green color means with good position within the global market >10 %. The table takes in consideration the regional origin (EU-US-ASIA-ISRAEL) of the leading companies and their stakes for each market segment. The data come from a cross-analysis of several studies: 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 and Analysis (2013–2018), Market and Market, 2013; «La Cybersécurité Europeenne: de l'importance d'une politique industrille», Jeremy Labarre report to the Council of the European Union 2014.



LEVEL OF EUROPEAN DEPENDENCE ON FOREING TECHNOLOGY	
Sector	**Level**
Desktop computing applications	🟥
Graphics processors	🟥
PC motherboards	🟥
Semi-conductor	🟨
Mobile computing	🟥
Industrial Control Systems	🟩
Routers	🟥
Networking switches	🟨
Computing servers	🟥
Data and Content Security	🟩
Application Security	🟥
Endpoint Security	🟨
Network security	🟥
System Security	🟥

companies[6]. The political reaction from European countries was focusing on data localization policies: many proposals were on national e-mail, undersea cables, localized routing and data storage, aiming to limit the harvesting and processing of digital data to specific U.S. companies and jurisdiction.

While those technical and legal initiatives have already been analysed [7, 8], we would highlight another trend: the dynamics on industrial policy seeking to promote cyber-security sector. The leak about the adoption by RSA, a major cyber security company, of two encryption tools developed by the NSA in order to increase its ability to eavesdrop on Internet communications, was a wake-up call for the need to strengthen the industrial security capabilities.

How a country aiming to be independent on cyber-security can provide cyber security facing a market dominated by foreign and strong competitive companies? What are the obstacles? In order to answer these questions, the second part of the article will focus on the French experience developed over the last years.

[6] An in-depth analysis was made by Danielle Kehl, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom and Cybersecurity*, New America's Open Technology Institute, 2014.

3 Structuring a Complex Dialogue

In accordance with the strategic objective to become a world power in cyberdefence, France has put many resources in and launched numerous initiatives aiming at ensuring independently its security. Industrial policy is part of the toolbox used in order to "master and develop (…) a range of guaranteed 'trusted products and services" [9].

3.1 Trusted Solution Wanted

The definition of trusted solution can thus be found through the reading of official documents[7]. A sovereign solution is firstly synonymous with integrity: namely, the assurance of the absence of built-in backdoors ensuring the protection of sensitive information and systems. For that, the public powers require " an evaluation process under the control of the National Network and Information Security Agency (ANSSI)". But the integrity and high-grade requirements are not sufficient criteria for assuring the commercial success of the solutions.

As discussed above, the cyber security demand has evolved with the commercialisation of Internet and the pervasiveness of the information systems in the industrial world. Since the current demand consists mainly of civilian infrastructures, a twofold need, therefore, has arisen. The customers are requiring ergonomically designed solution compatible with operational technology and simultaneously marketed at competitive price. As result, the offer of trusted solutions needs to be suitable for the new demand. The difficult is thus achieving the right balance between commercial solution and high-grade technology solution.

For doing that, the French authorities developed a policy based on four pillars: the conventional rulemaking, the organization of the public-private partnership, the R&D funding campaign, and the certification process.

3.2 A Coordinate Public Procurement Policy

In 2013 the government passed a law (*Loi de Programmation Militaire-LPM 2014–2019*/LPM) and imposed mandatory measures on public and private critical infrastructures. The rules consist of mandatory cartography of the critical information systems, mandatory and regular audits of information systems and networks by certified third parties; mandatory declaration of cyber incidents; implementation of certified detection sensors. In parallel, the government released an internal circular to impose the purchase of trusted solution on the public agencies.

The aim of those moves is to boost the internal demand to consume national solutions and thus to promote the development of a broad offering and limit the

[7] Three are the reference 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).

dependence on foreign suppliers. This move was carefully supported by the nation industrial base consisting of a few big corporates (Airbus, Thales, Orange, Sogeti, Bull-Atos) and a large SME complex (600). For these players the emergence of an internal market estimated to be 1.5 billion of euros and projected to grow at a 15 % to 20 % rate per year has been hailed as an Eldorado. What should be noted is that the market growth (globally estimated at $73 billion[8]) is happening in an environment of financial crisis and large cuts across the public administration in France as well as in Europe. Thus, helping in the structuring the market is seen as an economic opportunity for both the public and private sector [10].

3.3 Structuring the Public-Private Partnership

The democratization of information systems and the interdependence of the networks infrastructures have risen the need- for the government- to develop a coordinated approach between the different players involved in cyber security: private infrastructure operators, industrial control systems (ICS) providers, maintenance firms security companies, etc. [10].

The French authorities were aware of that already in 2008, when the White Paper on Defence and Security Policy recognizes the State no longer has all the essential levers it could need to take action against the threats it faces and it needs to develop better relationships 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 in order 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, the differences of language and culture emerged and strengthened the need for a permanent exchange. In 2011 ANSSI was aware of that and created a department fully dedicated to foster cooperation with the private sector around the twelve sectors defined as critical and an office dedicated to the industrial policy. Additionally, to move beyond the 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.

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

On the same level, and shaped by the aim to encourage the cooperation and the dialogue between public and private players, another initiative should be mentioned: the establishment of the Council of Security Industrial Base (*Comité de la filière des industries de sécurité-COFIS,* 30). Strongly wanted by the private sector, the Prime Minister launched the COFIS in 2013. This initiative brings together all the stakeholders involved in security industry from government agencies to trade federation and CI representative in order to match the needs of the offer and the demand and so to structure the security supply chain.

The latest initiative is the Cybersecurity Industrial Roadmap dubbed "Cyber Plan": a broad policy program consisting of seventeen actions around four strategic goals: boosting the national demand of trusted solutions, development of a national offer, structuring the export approach, consolidating the national industrial complex. The working group aiming at the implementation of the plan was led by ANSSI but composed of the representatives of private and public sector. Again the main goal was to bring together the whole spectrum of players interested in the industrial policy: providers, users, shareholders, regulators, customers, and investors.

The common achievement of these moves is the mutual understanding of various interests and thus the convergence of opinions in adopting minimum-security standards. In doing that, these initiatives reduce the gap between the government lack of technological path and the operators lack of security path and contributes to better assess future needs for security providers.

3.4 The Certification Process

The certification process, led again by ANSSI, is seen as a strategic way to ensure confidence on trusted solutions. In order to help the public authority to state how well CIs have implemented the new legal framework passed in 2013, the labelling process assesses the audit companies as independent evaluators. In addition, it tests also the integrity of security solutions and vendors aiming to bring transparency to the suppliers that should be embedded in the CIs. In this way, ANSSI through the expertise acquired on-the-field of incident-response and recovery, promotes the development of trusted suppliers evaluating products and services should be commercialized. Thus, potential customers could 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. Moreover, in order to promote the certificated solutions, ANSSI established a label "MADE in FRANCE" that will facilitate the marketing toward the customers.

The outcomes of these initiatives directly impact the 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 less risks for the network infrastructure.

3.5 Orienting the R&D

To ensure continuous investment in R&D, the state has increased its efforts in both the civilian and military investments. The Minister of defence has tripled in two years the research credit (€30 million in 2014). In parallel, in the framework of the *Program for the Future Investments* 2013 a call for projects entitled "Digital Security" has received 18 proposals. Through a fund of €20 million, this initiative aims to guide investment in R&D and thus promote the development of an offer so far absent. This will include the implementation of capacity requested by the LPM 2014–2019. In continuation of this strategy, the Cyber Plan envisages a new wave of call for projects for 2015 in order to develop two to three new ranges of deals per year.

In addition, a flagship project was announced and funded by the Minister of Defence in 2013. The project aims to structure a regional cluster focused on the cyber defence in Brittany and based on the concept of triple helix. Private company from telecom sector as well as from security and defence 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: cyber-security 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 Defence Cluster: private servants are participating with national authorities in drafting the cyber-security syllabus for national cyber defence centre of excellence. In doing that, the impact 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.

4 The Limits of the High-Tech Colbertism

The analysis of the initiatives launched in France stress how industrial policy depends on many variables that public and private players can impact only through a coordinated approach. Therefore, a comprehensive policy is needed. That means the implementation of various actions at different level in order to structure the market: the law to boost the demand, the education and R&D to structure the expertise, the organization of the 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 the evolution of cyber security means to be adaptive: being the police man (conducting the inspection), the conventional rulemaker (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.

4.1 Sovereignty Versus Business Interests

On the private side, increasing critics have been heard condemning the regulatory-based approach without taking in account the market drivers.

Due to the deregulation process of many public sectors in the 80s and the globalization of 90s, the private sector is now owning or controlling the majority of vital infrastructures many of them with multidomestic 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 more for developing solutions able to be sold on the international market and amortize R&D costs. Now here is where corporate interests clash with national security and highlight the need of more international cooperation. Since cyber-security is defined as matter of national sovereignty, public 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 for 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 the national demand and R&D budget are a fraction of the multibillion-dollar budget of the American and Asian market, the security vendors are complaining for less regulations and a more business-oriented, balanced and neutral regulation framework.

That leads to the question of the right scale of international cooperation: how to define a good partner? The European Unions is the most appropriate level or it would be more valuable to establish a trusted group of partners on the basis of mutual acceptance of national standards? Nevertheless, cyber-security of national strategic assets remain a national responsibility: in sensitive domains like cryptography, this would mean to continue developing country-specific solutions. Hence, there is a strong link between cyber-security 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.

4.2 When the Size Market Matters

SMEs are the engine of innovation in cyber domain: due to their structure and innovative culture, they are an essential element to face the extremely rapid evolution of threats and technologies. This reason explains the importance of the relationship between SME and big corporate in building the ecosystem of cyber-security. Although it is not a specific to the cyber domain, this point becomes important for the French case because of the current critical situation and the fierce competition in international markets.

However, the national market is too tight and although the presence of many innovative SMEs, these are not able to reach a critical mass because of lack of the demand. 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 cyber-security market. In addition, more complexities rise in case of acquisition or merger of an SME: 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.

4.3 The Paradox of a Schizophrenic World

On the political side, there are also some complications. As the Snowden affair revealed to the global public, the State organization suffer schizophrenia: promoting and implementing defences while actively attacking is no longer sustainable with the concept of resilience. This applies to the U.S. as well as to the other states developing offensive capabilities like France. Keeping secret vulnerabilities, cracking encryption standards and installing backdoors means increasing technical vulnerabilities for everyone and thus mining the trust of society in the global information infrastructure and the public authorities.

However, the schizophrenia is also on the citizen's side: we accept that the State needs pre-emptive intelligence in order to anticipate the major threats as the terrorism [11]. This explains the reaction of law enforcement agencies such as the FBI and the GCHQ to the strengthening of encryption technology by social network companies[9]. For intelligence agencies adding extra layers of security that prevent national authorities from gaining access to information stored by service providers means more difficulties in the fight against threat using these technologies.

5 Conclusion

In conclusion, the French case is striking for a least two reasons. First, there are a number of reasons behind the implementation of industrial policies: market fragmentation, corporate interests, and national security 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, the dynamics analysed reveal on the one hand the willingness of public authorities to control the cyber-security mechanism and, on the other hand, they underscore the need to find the balance between national sovereignty, business interests and privacy. Given that the 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 of the balance is hard task. It is even more complicated because businesses operate across borders while law enforcement agencies are national based.

We are now only at the very beginning of the important international debate about the dynamics within the infosfere. As the Online Manifesto has observed, "the

[9] For the official declarations see: R. Hannigan, *The web is a terrorist's command-and-control network of choice,* The Financial Times, November 3, 2014, and A. Thomson and A. Satariano Silicon Valley Privacy Push Sets Up Arms Race With World's Spies, Bloomerg, Nov 5, 2014.

repartition of power and responsibility among authorities, corporate agents, and citizen should be balance more fairly" [12]. This situation pushes States and especially law enforcement agencies to openly explain their activities –without revealing security recipes- to the citizens and work more closely with personal data protection agencies. We need to move from what Bruce Schneier names "corporate-government surveillance partnership" to the public-private debate partnership [13]: in order to continuously entrust the security to public powers, the citizen, whose confidence is fundamental for the resilience, has to be involved in the cyber-security equation.

Acknowledgements. This work is funded by *Airbus Defense and Space-CyberSecurity* and supported by the *Chaire Castex de Cyberstratégie*. 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.

References

1. Floridi, L.: Information: A Very Short Introduction. Oxford University Press, Oxford (2010)
2. Dunn Cavelty, M.: From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse. Int. Stud. Rev. **15**(1), 105–122 (2013). Friedman, A.: Economic and Policy Framework for Cybersecurity Risks. Brookings, July 2011
3. Lacoste, Y.: La géographie ça sert d'abord à faire la guerre. La découverte, Paris (2014)
4. Rid, T.: Cyberwar Will Not Take Place. Oxford University Press, Oxford (2013)
5. Castelluccia, C., Grumbach, S., Olejnik, L.: Data Harvesting 2.0: from the Visible to the Invisible Web. Presented at the 12th Workshop on the Economics of Information Security, Washington, DC, United States, June 2013. https://who.rocq.inria.fr/…/WEIS13-CGO.pdf
6. Anderson, R.: Privacy versus government surveillance: where network effects meet public choice. Presented at the 13th Workshop on the Economics of Information Security, Pennsylvania State University, United States, June 2014. http://weis2014.econinfosec.org/papers/Anderson-WEIS2014.pdf
7. Hill, J.F.: The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders. Lawfare Research Paper Series, vol. 2–3 (2014)
8. Maurer, T., Morgus, R., Skierka, I., Hohmann, M.: Technological sovereignty: missing the point? In: An Analysis of European Proposals after 5 June 2013
9. White Paper on Defence and National Security, La documentation Fransaise, Paris, p. 174 (2008)
10. D'Elia, D.: Public-private partnership: the missing factor in the resilience equation. The French experience on CIIP. In: Stefanowski, J., Panayiotou, C.G., Ellinas, G., Kyriakides, E. (eds.) CRITIS 2014. LNCS, vol. 8985, pp. 193–199. Springer, Heidelberg (2016). doi:10.1007/978-3-319-31664-2_20
11. Omand, D.: Securing the State. Hurst, London (2010)
12. Floridi, L.: The Online Manifesto, Being Human in a Hyperconnected Era. Springer, Berlin (2015)
13. Schneier, B.: A Fraying of the Public/Private Surveillance Partnership. https://www.schneier.com/blog/archives/2013/11/a_fraying_of_th.html. Accessed 30 November 2013, The Battle for Power on the Internet, The Atlantic. http://www.theatlantic.com