State-industry relations and cybersecurity governance in Europe

State-Industry Relations and Cybersecurity Governance in Europe

Antonio Calcara (University of Antwerp), Raffaele Marchetti (LUISS University)

Author's Accepted Manuscript (AAM) – Review of International Political Economy

Abstract

Recent analyses of international affairs highlight that states are increasingly exploiting the key position of some private industries in critical hubs of global economic networks to gain an advantage over their competitors. The key role of private companies in international competition has also significant implications in the cyber-domain, where private actors are the main owners of data and digital infrastructures. In contrast to those who see a transformative effect of cyber, this article draws on comparative political economy and defense policy to identify two different models of state-industry relations in the governance of cybersecurity. The theoretical framework distinguishes between public and private governance ecosystems and identifies different hypotheses on how states and industries interact in cybersecurity governance in France and in the UK. The French public governance is characterized by the presence of formal and informal relations between state and industries, a high degree of public investment in the private sector and centralized institutions. France has also used the EU mainly to advance its industrial interests. In contrast, the UK private governance is characterized by more arm's length relations between the state and industries and a less centralized system. Moreover, the UK, differently to France, has not used the EU channel to advance its industry-related preferences. These results confirm the macro-differences between public and private governance ecosystems and open new relevant avenues to investigate the interplay between political economy structures and European and international pressures in policy-areas with both economic and security implications.

Keywords: Cybersecurity; Europe; Governance; Political Economy; Security.

1. Introduction

Recent analyses of international affairs highlight that states are increasingly exploiting the key position of private companies in critical hubs of global economic networks to gain an advantage over their competitors (Farrell & Newman, 2019). Given the centrality of private actors in international competition, there is currently an important discussion about the evolving relations between the public and the private sector, between states and industries (Roberts, Choer Moraes & Ferguson, 2019; Gertz & Evers, 2020). This debate is particularly relevant in the cyber-domain, where private

companies are the main owners of data and digital infrastructures (Cavelty & Egloff, 2019). In this regard, experts and scholars argue that - due to the distinctive features of cyberspace linked to global information exchange and the diminishing relevance of the territory - the private sector is the key player in the governance of cybersecurity (Eriksson & Giacomello, 2006; Betz & Stevens, 2011, pp. 55-56). In contrast, others believe that the growing politicization of cyberspace is leading the private sector to a necessary alignment with public objectives (Matania, Yoffe & Goldstein, 2017; Barrinha & Renard 2020, p. 8; Gertz & Evers 2020). Overall, these contrasting positions seem to converge on one key point: either the distinctive features of cyberspace or its increasing politicization are in any case having a transformative effect on existing cross-national state-industry arrangements in economic and industrial policies, especially in the digital, telecommunications, information, and utilities issue-areas.

Drawing on this scholarly and political debate, this article aims to provide three contributions to the academic literature on the topic. First, contrary to those who see a transformative effect of cyber, this study demonstrates the ability of the existing models of comparative political economy to largely explain state-industry relations in the governance of cybersecurity.

Second, the article provides a parsimonious conceptual toolbox, integrating comparative political economy with the scholarly literature on defense policy. The theoretical framework distinguishes between public and private cyber-governance ecosystems. Moreover, it identifies three key properties of state-industry relations through which it is possible to compare different cyber-industrial ecosystems. Analyzing the degree of protection by the government, the interpenetration between public and private actors and the status and autonomy of procurement agencies from corporate influence allows to construct different hypotheses on how states and industries interact in cybersecurity governance.

Third, the article contributes to a better understanding of European cybersecurity. State-industry relations are particularly interesting in the cyber-domain because - being at the crossroads of security, economic and industrial policy - they are characterized by a complex governance system in which EU institutions, member states and industries constantly interact (Carr, 2016; Christou, 2019). Formally, cybersecurity remains in the hands of the member states, which have developed different domestic strategies and governance arrangements to govern this domain. However, European legislation can intervene or shape the states' cybersecurity political and institutional architecture, for instance through the Network and Information Security (NIS) directive or through European legislation on foreign investments in strategic sectors (Carrapico & Barrinha, 2017). Specifically, this

article focuses on state-industry relations in France and the UK. The case selection criterion is based on the most dissimilar cases. We select France and the UK because they have a significant international standing, but especially because they can be considered paradigmatic examples of respectively public and private governance ecosystems. Moreover, the fact that one of the two countries is no longer a member of the EU allows to better disentangle the potential influence of EU legislation and policy on state-industry relations.[1] The empirical analysis is based on primary and secondary sources and on 10 semi-structured interviews conducted between 2018 and 2020. For reasons of confidentiality, the interviews are anonymized.

The article is structured as follows: in the next section, we develop our argument on public and private governance ecosystems and theorize its impact on cybersecurity governance. Then, we investigate the French and British cases in detail. The last section summarizes the main findings of the research, it clarifies the contribution of this work to the scholarly literature and presents some possible research avenues for the future.

2. State-Industry Relations in Cybersecurity: A Theoretical Framework

State-industry cooperation is essential to ensure cybersecurity. Industries are crucial suppliers of cybersecurity systems, as they have the funds and expertise to invest in technological innovation and develop new products. An attack on industrial software owned by a private company may have also important consequences for national security, considering that critical infrastructures[2] in many (Western) countries (this is also valid for internet access and online service providers) are mostly privately owned. The private sector is therefore a key player in the regulation and governance of cyberspace (Eriksson & Giacomello, 2006). In this regard, scholars have noted how the distinctive characteristics of cyberspace altered the balance of power between public and private actors and that cyberspace's low barrier to entry dramatically lowered the transaction costs of private actors to organize (Farrell, 2006; Drezner, 2019). Farrell and Newman attribute the key role of the private sector in cyberspace to the liberal policies that characterized internet and digital governance in the nineties (Farrell & Newman, 2021).

[1] Our analysis takes into account the period both before and after the Brexit referendum in 2016.

[2] Critical infrastructures are systems or assets so vital to a country that any extended incapacity or destruction of such systems would have a debilitating impact on security, the economy, national public health, or any combination of the above. The most frequently listed examples encompass banking and finance, government services, telecommunication and information and communication technologies, emergency and rescue services, energy and electricity, health services, transportation, logistics and distribution.

In contrast, other experts and scholars argue that the increasing politicization of cyberspace is leading to a growing alignment between states and industries (Matania, Yoffe & Goldstein, 2017; Roberts, Choer Moraes & Ferguson, 2019). The idea is that close, cooperative relations between businesses and the government may act as a force multiplier and state power increases when firms are aligned with state goals and eager to work hand-in-hand with the government to achieve them (Gertz & Evers, 2020:117). For instance, China's recent National Intelligence Law compels China-based companies to support, assist in and cooperate in national intelligence work, should they be required to do so (Stevens, 2019). The US is also increasingly concerned about Chinese companies (Huawei and ZTE) building 5G networks around the world and having access to sensitive data because of the industry's proximity to the government (Kaska, Beckvard & Minàrik, 2019). Earlier on, at the time of the NSA scandal, the proximity between the tech giants and the US government suggested that some sort of synergy was already at work (De Vos, 2010). Overall, either the distinctive features of cyberspace or its increasing politicization is having a transformative effect on existing state-industry arrangements in the digital, telecommunications, information, and utilities issue-areas. This suggests that we need new theoretical tools to understand how states and industries are reconfiguring their relations in cyberspace. As summarized by Collier (2018, p. 13), "the lines between what is public and private, between what is global and local, are waning (…) Cybersecurity, therefore, requires refreshed thinking" (see also Kello, 2013).

Contrary to this emerging consensus on the transformative impact of cyber on state-industry relations, several studies are highlighting a substantial cross-case differentiation in how public authorities organize cybersecurity governance (Van den Hurk et al, 2015; Carr, 2016; Bossong & Wagner, 2017; Weiss & Jankauskas, 2019). A recent special issue has suggested that cross-national differences may depend on the type of "state-society relations in which various government agencies build and implement policies within bureaucratic politics, with input and challenges from societal actors including labour, consumers, interest groups, and IT firms" (Aggarwal & Reddie, 2018a:8). The variation in cybersecurity governance arrangements may reflect, in a sort of historic path dependency, distinctive domestic state-industry relations. For instance, in the US, the government has sought to integrate public appropriations into the private cybersecurity market via a series of venture capital efforts (Aggarwal & Reddie, 2018b). In contrast, China's cybersecurity governance has been mainly driven by government prerogatives (Cheung, 2018).

Building on these studies, we propose a parsimonious theoretical framework to compare different models of state-industry relations in the cyber-domain. Specifically, we argue that the comparative political economy scholarship may be a good starting point to shed light on how pre-existing state-

industry relations impact on cybersecurity governance. Already in 1965 Schonfield divided European capitalism into three models of national political economies, including France's statism, Britain's liberalism, and Germany's corporatism (Schonfield ,1965). Scholarly works in the following decades substantially confirmed and expanded these findings, specifying in greater detail the different varieties of European political economies (among others Hall & Soskice, 2001; Crouch, 2005; Hay, 2020). However, we need to integrate these considerations with the distinctiveness of a sector that lies at the heart of national security. In this regard, the scholarship on defense policy and military-industrial complexes has indeed long tried to disentangle both formal and informal interaction patterns between states and industries in a monopsonist defense market, characterized by one buyer and few players that directly contract with the government (De Vore & Weiss, 2014; Calcara, 2020; Gholz & Sapolsky, 2020).

Typically, two predominant patterns of state - defense industry relations have been identified. First, state-industry relations could be geared at vertical integration with state ownership and control over company strategy with a preference for domestic suppliers (Lundmark, 2011, p. 32). These institutional contexts are also characterized by a high degree of interpenetration between public and private actors. The close relations between industrial contractors, procurement executives, and the governmental officials facilitate the so-called “revolving doors” phenomenon, which refers to the flow of people from the public to the private sector and vice versa (Serfati, 2001; Goyer, 2011).

Second, state - defense firms’ relations could be market-oriented with competitive procurement contracts, no preference over domestic suppliers and arm’s length relations between state and industry. Elite networks are highly fragmented, and the inter-sectorial career path mobility is almost absent (Matelly & Lima, 2016, p. 74). This fragmentation is due both because formal competition regimes preclude collusion amongst elites and because the lack of intersectoral career mobility results in early career decisions canalizing individuals into sector-specific elite networks (DeVore & Weiss 2014, pp. 506-507). In these institutional contexts procurement agencies play a pure role of supervision, rather than the direction of defense-industrial policy. In other words, corporate strategies in private governance ecosystems focus less on informal contacts with government or bureaucratic officials, and more on formal competitive market arrangements.

Drawing on these two patterns of interaction, we derive three fundamental properties of state-industry relations:

a) the degree of protection by the government

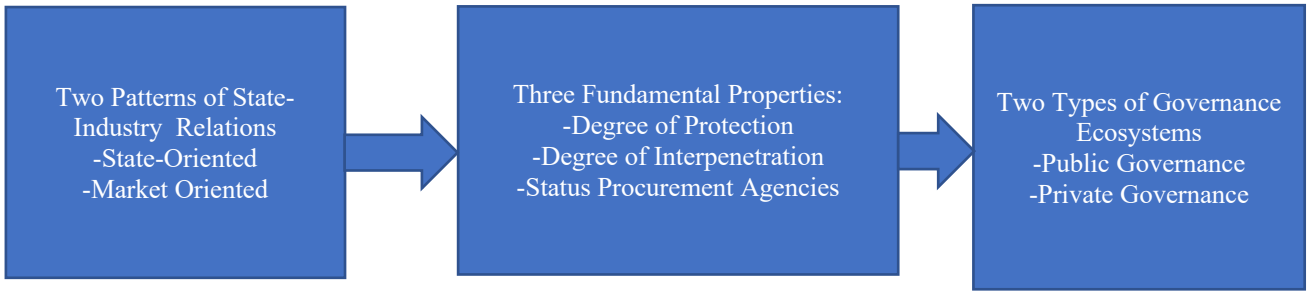
b) the degree of interpenetration between public and private sectors elite network

c) the status and autonomy of procurement agencies from the industry's influence

The three identified properties substantially overlap. However, the aim here is to disentangle various aspects of the relationship between the state and industries. Indeed, when these three properties are combined in the format of governance, two main types of governance ecosystems can be identified:

- *Public governance ecosystems* characterized by a high degree of government protection (also through the ownership or control of industries), a high degree of interpenetration between public and private actors (revolving doors), and a very close relationship between public procurement agencies and the private sector
- *Private governance ecosystems* characterized by a low degree of government protection, low levels of interpenetration between public and private actors and a more arm's length relationship between public procurement agencies and the private sector.

Fig. 1: From State-Industry Relations to Governance Ecosystems



The typological distinction between public and private governance ecosystems (see Table 1) serves the analytical purposes of reducing complexity and to sharpen the capacity for comparison without seeking to account for all empirical varieties on the ground (Streek, 2010; Amable, 2016). The aim is to identify "ideal types", "one-sided accentuations" to be used in the construction of the research hypotheses (Hay, 2020).

Table 1: Taxonomy of Public/Private Governance Ecosystems (Independent Variable)

	Public Governance Ecosystems	**Private Governance Ecosystems**

Degree of Protection by the Government	High	Low
Degree of Interpenetration between Public and Private Sector Elite Networks	Strong formal and informal networks between government and suppliers (revolving doors)	Distant – little government role in internal workings of suppliers and vice versa
Status and autonomy of Procurement Agencies from Industry's influence	Strong, but dependent from its relations with industry	Independent Agencies. Strength vis – à – vis industry

Overall, the article aims to understand whether the state-industry relations institutionalized in the overall governance ecosystem (independent variable) may also explain the type of governance that is set in place in the cybersecurity sector (dependent variable). The specific cyber domain obviously partially differs from the conventional defense market, characterized by the presence of a single buyer and a limited array of prime contractors. The cybersecurity market is indeed constituted by a larger number of big and small tech companies who sell cybersecurity products not only to the state but also to other companies or to individuals (think about your computer's anti-virus). The dual-use (civilian/military) character of cybersecurity technologies has led tech or civilian industry to equally invest in this sector. While defense companies usually work closely with military officials to develop products that will be purchased by the governments, a number of commercial corporations have been making significant private investments in the development of cybersecurity technologies to access and secure services market independently from governmental agencies (Boulanin & Verbruggen 2017, p. 105; Calcara, Csernatoni & Lavallée, 2020). Moreover, innovation in the cybersecurity market is linked to a virtuous integration of micro and small companies and by their collaboration with large companies, which remain critical for their organizational, distribution and managerial skills to bring the product to the market (Boyes, 2015). However, despite these structural differences, recent studies have shown that the public procurement of cybersecurity products is actually very similar to defence procurement. Ruhonen (2019) has noted that contracts for cybersecurity products are usually won by national industries and the amount of European cross-border procurement contracts is negligible (less than 20%). The results are actually very similar in the military domain (Masson et al, 2015). Moreover, some military industries are also top players in the cybersecurity industry. Almost

all the major European defense corporations, including Airbus, BAE Systems, Leonardo, Saab and Thales, operate in the cybersecurity market, in some cases via specific divisions (Boulanin, 2013).

These findings suggest that an extension of the public or private governance model to understand state-industry relations in cybersecurity may be a fruitful research avenue. Given the previous theoretical considerations, we expect the public/private governance ecosystems to develop distinct models of cybersecurity governance. In order to investigate such process, we need to find specific operationalizable points of reference. In this regard, following the scientific debate we indicate a number of parameters that arguably constitute the bulk of the cybersecurity governance (Van den Hurk et al, 2015; Carr, 2016; Bossong & Wagner, 2017; Weiss & Jankauskas, 2019). They are related to the following dimensions: decision-making, governmental support, specialized public agencies, and the relationship with the EU level of governance. Drawing on the theoretical framework so far presented, the following hypotheses will thus guide the empirical research in the two case studies:

1. *Decision-Making*

The nature of the governance ecosystems impinges on the *model of the decision-making in the cybersecurity domain*. Specifically, we expect that in public governance ecosystems, cybersecurity goals are jointly determined, there is a collaborative and consensus-based decision-making and that state-industry relations are shaped by trust-based and informal relations. In the case of private governance ecosystems, instead, we expect a more arm's length relationship between the state and the industry, in which the government set legal, technical and normative rules without necessarily involving the industry and there are more formalized relations between the two actors.

2. *Dedicated Institutions and Agencies*

The nature of the governance ecosystems impinges on the existence of *dedicated public agencies and institution*s to sustain the cybersecurity private sector and the *degree of centralization* of these institutional structures. We expect the presence of dedicated agencies and institutions and a greater centralization in public governance ecosystems compared to private ones.

3. *Government Support*

The nature of the governance ecosystems impinges on the *degree of government support to the industries* that populate the cybersecurity sector. This government support can be direct (through funds, tax cuts, top-down industrial districts and so on) or indirect (through the development of national certifications, exclusion of foreign players from the market and so on). In public governance

ecosystems, we expect, given the close relationship between states and industries and their ability to capture states' preferences, a high degree of government support. We expect the opposite in private governance ecosystems.

4. *EU Institutions*

The nature of the governance ecosystems impinges on the *states' interactions with European institutions in cybersecurity*. In this regard, we expect public governance ecosystems to be more likely to use European institutions to advance their industry-related preferences, while countries with predominantly private governance ecosystems more likely to emphasize other preferences (mainly linked to strategic-operational issues), rather than industry-specific benefits, in their interaction with European institutions.

Table 2: Taxonomy of cybersecurity governance (Dependent Variable)

	Public Governance Ecosystems	**Private Governance Ecosystems**
Decision-Making	Consensus-based, informal relations	Arm's length relationship between the state and the industry
Dedicated Institutions and Agencies	Centralization	Decentralization
Government Support	High	Low
Relations with EU institutions	Emphasis on industrial benefits	Focused on strategic-operational issues

To probe our hypotheses, we zoom in on the French and British cybersecurity governance ecosystems. In this regard, both the comparative political economy and defense policy scholarships suggest that France and the UK can be considered as two examples of, respectively, public and private governance ecosystems. France, despite its formally state's strong centralization, it is actually deeply fragmented in practice (Clift, 2009). This ensures frequent capture by business interests and a pattern of business-government relations characterized by accommodation and co-optation (Jabko & Massoc, 2012). Recent analyses have confirmed that the interpenetration between the public and private sectors allows industries to convince the state to use the European playing field to promote their interests (Ansaloni & Smith, 2018; Clift & McDaniel, 2019). On the contrary, in the British governance ecosystem, the state is more able to autonomously impose its decisions without being excessively concerned by the interests of its business actors (Davis & Walsh, 2016; Weiss, 2020). Notwithstanding an increasing degree of state activism in the last decade, recent studies have confirmed that it is not at odds with the resilience of neoliberal principles in regulating financial, economic and industrial activities (Schmidt & Thatcher, 2013; Berry, 2019).

3. France: A Public Governance Ecosystem

3.1. Decision-Making

French cybersecurity governance is characterized by consensus-based, informal relations between the state and its domestic industry. The cybersecurity industry has been indeed able to significantly shape governance arrangements in this field. The French cybersecurity industrial sector is a mature market, in which there are around 700 companies, with five major corporations (Airbus, Thales, Atos, Orange and Sogeti) and more than 600 small and medium enterprises (SMEs) with fewer 20 employees. The five major corporations provide the full range of cybersecurity products, from traditional network protection solutions to network surveillance devices. Among these, Thales is the most important player and the historical supplier of cybersecurity services to the Ministry of Defense. Thales reported that the business generated about 900 million euros ($1.10 billion) in sales over 2017, up from 700 million euros a year earlier. It is also expected to grow by about 10% annually in the coming years (Rosemain, 2018) There are also a number of French companies that are particularly prominent in the area of cyber-surveillance. Alcatel Lucent[3], Aqsacom and Qosmos are important

[3] Thales has recently acquired Alcatel-Lucent's cyber security services activities

providers of network surveillance devices, while Vupen and Quarkslab are key actors in the business of zero-day vulnerabilities (Boulanin, 2018, p. 764).

Ever since there has been a concern by the French government towards cybersecurity, industries have been able to influence Paris' governance strategy. In 2010, the French Presidency created a national security strategic council, aiming at gathering a broad range of expertise - civilian and military, industrial and governmental - to conduct a "strategizing" function. Labelled "High Council for Strategic Education and Research" (CSFRS), the group concluded that "the penetration that affected French organizations showed without ambiguity that the systems of sensitization, of awareness, of understanding risks and of regulation and control are today neither efficient, nor understood or applied" (CSFRS, 2012, p. 46). For these reasons, the group suggested to massively invest in the cybersecurity industry. The CSFRS was led by Jean-Marc Suchier, member of the important security firm *Sage Défense Sécurité,* and also included other members of French defense firms, such as Cédric Blancher from Airbus or Stanislas de Maupoeou from Thales (Baumard 2017, pp. 57-58). The goal of the French firms, especially those already active in the defense field, was to promote a centralization of cybersecurity governance and the establishment of a privileged relationship between the state and the industry in a relatively new market sector.[4] The report called for the creation of a national observatory and a public-private coordination body (CSFRS, 2012, p. 48). A decisive role in shaping state's preferences has also been played by the *Alliance pour la Confiance Numerique*, a lobbying group representing French cybersecurity companies (Boulanin, 2018, p. 764) and by the CoFis (Security Industries Council), a dialogue group between state and industries, with the task of determining priorities, avoid overlaps and reconcile offer and demand (D'Elia, 2014, p. 75). The "Cybersecurity plan" designed by the Ministry of Economy's "*Nouvelle France Industrielle*" (New Industrial France) programme, aimed to sustain cybersecurity-related firms and the development of new technologies in this sector. In the recent French Big Investment plan 2018-2022, the government committed to spend roughly €5 billion to improve business innovations in artificial intelligence, mega data, nanotechnology and cyber security.[5] These centralized programs to sustain industry are also closely linked to the French position on Artificial Intelligence. In March 2017, the French education and research ministry published "France AI", a report that included recommendations from expert working groups, in which there was a significant industry's presence. The document was followed a year later by 152-page strategy in which there is a clear emphasis on industrial autonomy and protection of the cybersecurity market (Villani, 2018). The French cybersecurity governance has been

[4] Interview French cybersecurity firm representative 12/07/2019
[5] French Government, The Big Investment Plan 2018-2022. Retrieved from: https://www.gouvernement.fr/en/the-big investment-plan-2018-2022

therefore constantly driven by the industry's desire to develop cooperative channels between the state (as regulator, client and investor) and the industrial suppliers.[7]

3.2. Dedicated Institutions and Agencies

French cybersecurity governance is based on a high degree of institutional centralization. At the strategic level, the idea of a national cybersecurity strategy was launched in 2008. Responding to the need to adapt to an evolving international environment, President Sarkozy initiated a broad review of defense and national security strategy. In February 2008, the French Senate prepared a report, titled "Cyber defense: a new national security issue", warning that Paris was not prepared to identify potential cybersecurity threats (Baumard 2017, p. 56). Shocked by the Estonia cyberattacks in 2007, the report's warnings were successively addressed in the 2008 White Paper on defense and national security. The White Paper listed cybersecurity, for the first time, as a national security priority (White Paper 2008). In order to tackle this new threat, it included a series of recommendations, such as the adoption of a national cybersecurity strategy and the creation of a centralized agency for cybersecurity (Baumard 2017, p. 56). In 2009, the government established the French centralized agency for cybersecurity, the *Agence Nationale de la Securite des Systems d'Information* (ANSSI), located within the Prime Minister's office and attached to the Secretary General of defence and national security (SGDSN) (Boulanin 2018, p. 763). The ANSSI is responsible for assisting the state's institutions on cybersecurity, for organizing standards for industries and critical infrastructures, but it is not responsible for investigating cybercrime and cyberterrorism (a responsibility that rests with the Ministry of Interior). The ANSSI does not also conduct cyber-defense activities, which fall within the remit of the Ministry of Defense. On the military side, cybersecurity governance revolves around the activities of the *Direction Générale de l'Armement* (DGA), which has the task of coordinating industry's effort in the production of cybersecurity-related products.

A centralized institutional framework constitutes an advantage for French industries, because they can lobby through well-oiled institutional channels. This governance structure has been indeed strongly shaped by the very close relationship between the state, bureaucracy and private firms, especially because the lobby groups that represent cybersecurity industry are well acquainted in the French political and institutional systems (D'Elia, 2014; Baumard, 2017; Boulanin, 2018). In this regard, another decisive factor to understand state-industry relations in cybersecurity is to look at the degree of interpenetration between public and private actors. There is an established literature on the degree of interpenetration between members of the DGA and French industries (Serfati, 2001; DeVore & Weiss, 2014, pp. 507-509; Faure, Joltreau & Smith, 2019). Similar relationships can also

be found between the centralized ANSSI agency and the cybersecurity industries, especially because the top managers that populate the French cybersecurity agencies share a common academic background (usually graduated from the *École Polytechnique*) and they usually have a previous professional experience in the Ministry of Defense or in adjacent sectors. To make only a striking example, Dr. Guillaume Poupard graduated from *École polytechnique and i*n 2006, he joined the Ministry of Defence. In November 2010, he was appointed Head of the Cybersecurity Division within the Technical Branch of the DGA, responsible for expertise and technology policy in the field of cybersecurity. On March 2014, he was appointed Director General of the ANSSI.

3.3. Government Support

Given the privileged relations between state and industries, the effective lobbying campaign of the latter convinced Paris to pursue two main goals: promoting public investments in cybersecurity industrial capabilities and protecting the French market from possible foreign interference.

The 2008 White Paper explicitly addressed cybersecurity industrial capabilities as integral part of national areas of sovereignty, at the same level as nuclear deterrence and ballistic missiles (White Paper, 2008, p. 306). France has also issued in 2011 the "Information Systems Defence and Security Strategy", to lay out a series of concrete measures designed to maintain industrial autonomy in cyberspace. Similarly, in 2012, France's Senator Bockel released a report highlighting the political priority of developing a coherent industrial approach in cybersecurity. For instance, following a precedent set by the US, Bockel suggested the prohibition of the purchase of routers and other network equipment from China which could pose a risk to French national security (Bockel, 2012). Following this approach, the French parliament has recently approved a law on the security of 5G equipment that aims to exclude non-European industries (especially Huawei) from the French market (Vergara, 2019). Cybersecurity industrial autonomy has been a key concept also in the 2013 White Paper (White Paper 2013:100). These initiatives went hand-in-hand with a parallel centralization of state investment to sustain cybersecurity industry. Between 2013 and 2014, the government launched a vast industrial program, with Research & Development (R&D) investments amounting to €150 million. The Programme for Future Investments (2013) invested €20 million to drive investment in R&D related to digital security. From 2014 to 2019, the French government has committed to invest €1 billion in cybersecurity. The military procurement agency DGA has tripled its resources to support R&D, feasibility studies and specific acquisition programs (Boulanin 2018:764). The French government has also established a Centre of Excellence on Cyber defense in Brittany and the DGA now directly supervises specialized cybersecurity research centers, especially in the Bretagne region.

In this context, the Information Assurance Division of the DGA (DGA/MI) is a central part of the cybersecurity cluster involving industry, academia and government to develop technological innovation in this sector. Recently, the Defense Minister Florence Parly has allocated a budget of €130 million until 2025 to further develop the district in Brittany, supporting large and small companies established in the region (giants like Orange and Thales, or young start-ups as Secure-IC) (du Guerny, 2019). The French public investment in cybersecurity has been positively welcomed by the national industrial base. For these companies, the emergence of an internal market estimated to be 1,5 billion euros and projected to grow at a 15-20% rate per year has been hailed as an "Eldorado" (D'Elia, 2018, p. 397).

French industries also lobbied to protect the market from potential external competitors. Given that European legislation sets limits to a complete prohibition of foreign investment in strategic sectors related to cybersecurity, the French government has developed indirect tools to protect its domestic market. For instance, Paris has introduced a certification label "France cybersecurity", managed by ANSSI, in order to create a network of reliable government suppliers for cybersecurity supply-chain. The introduction of this certification has been clearly supported by the industry. For instance, the aforementioned CSFRS proposed a process of "national certification involving the French regulatory organization ANSSI and approved certification organizations" (CSFRS, 2012, p. 48). The label "French cybersecurity" has had a significant impact on the market, especially for its high costs for companies. A low-level certification audit costs nearly €60.000, which is way above the cost of similar product certifications in the US or Germany (Baumard, 2017, p. 63). These high costs have deterred many cybersecurity start-ups that simply left France to reinstall their activities abroad. The total of these "certified suppliers" were less than 25 in 2017 and most of these certified cybersecurity providers are large French incumbents: Cassidian Cybersecurity (now Airbus Defense and Space), Bull, CGI, CS, Ernst and Young, Steria, Orange, PWCA, Sogeti and Thales. Guillaume Poupard, first director of ANSSI and then cybersecurity responsible for the DGA, has admitted that the certification process "isn't necessarily cheap for the firms that take part", but it is "definitely worthwhile – not only for the firms themselves that need a set of standards to apply and benefit from the ability to show that they are up to standard, but also to their clients who have the peace of mind knowing that they are working with a firm that has met such high standards" (quoted in Mew, 2016). The costs of certification are leading to high entry barriers in this market, especially for those incumbents that could be interested in the technologically innovative and profitable cybersecurity market. Young, R&D intensive, innovative cybersecurity start-ups are in fact clearly outnumbered, and this led many experts to conclude that the "logic of club" to the advantage of the insiders was superseding the certification logic (Baumard, 2017, p. 63). French small and medium companies have therefore raised

concerns about the excessive regulation of the cybersecurity market. The AFDEL (*Association Francaise des Editeurs de Logiciels et de Solutions Internet*) has noted that the certification process is very expensive and small and medium-sized companies with low human and financial resources might find it difficult to sustain these costs, especially compared to industrial giants like Airbus and Thales (D'Elia, 2018, p. 401).

3.4. Relations with EU institutions

The French government, in its cybersecurity-related documents, has often mentioned the EU as the preferred context in which develop cybersecurity capabilities (White Paper, 2013; White Paper, 2018; Villani, 2018). Paris has also strongly influenced the governance of European cybersecurity as it was the European country that first imposed mandatory measures on public and private infrastructures, a measure that was then included in the EU's NIS directive

France seems to prefer a clear division of labor between EU and NATO in addressing cybersecurity issues (Baumard, 2017; D'Elia, 2018). Indeed, Paris differentiates between cyber security (economic and protection of critical infrastructures) and cyber defense (military and intelligence) when it comes to prioritizing cooperation with NATO and the EU. NATO is mentioned specifically in the Cyber Defense Pact, while the EU is not. However, economic and industrial cybersecurity standards are favored to be discussed within the EU. France triggered a consensus-building movement, acting as a policy entrepreneur - together with the European Commission - to promote a European approach to cybersecurity industry issues (Terpan & Saurugger, 2020). Paris sees the EU context as the ideal one to advance its industry-related preferences and to give a competitive advantage to European products and services vis-à-vis extra-European competitors (French Ministry for Foreign Affairs, 2019). This approach is clear when it comes to concretely participate in EU collaborative cybersecurity programs. For instance, in the newly relaunched PESCO framework, France acts as the coordinator of the European Secure Software Defined Radio (ESSOR), that aims to develop common cybersecurity technologies for European military radios, with a clear interest by Thales. Similarly, Thales is very much involved in the Integrated Unmanned Ground System (UGS), with the goal of developing cyber secure autonomous navigation capability for route and mission planning. The French company CS Communication & Systèmes (CS) received substantial funding from the European Investment Bank (EIB), as part of the Juncker Plan to promote innovation and support innovative companies. As stated in the press document, this funding perfectly suits with "the objectives of the French Government's investment plan and it is one of the first projects to put this plan into practice" (EIB, 2017). Paris has also played a leading role in the most important European institutions working on cybersecurity, also

being able to hold top bureaucratic positions. At the time of writing (January 2021), French representatives chair both the European Union Agency for Cybersecurity (ENISA) and the European Cyber Security organization (ECSO)[6]. French industrial representatives are also well represented in the ENISA advisory group and in the ECSO. As noted by D'Elia, "in terms of industrial policy, there is a strong implication of the French players, including public administration (ANSSI and the Brittany region) and private sectors in the establishment of the European Cyber Security Organization" (D'Elia, 2018, p. 404).

However, there have been also cases where the EU proposed measures that were perceived as harmful to French industrial interests. For instance, the EU – in the context of the new Cybersecurity Act – has pushed to introduce an EU-based cybersecurity certification process. This initiative created some discontent in Paris. As highlighted by Poupard, director of ANSSI, "the system should be more than just an agreement between member states to recognize each other's national certification. Instead, their agencies need to actually share the same criteria to define security levels. It would be *a kind of nightmare* if some countries approve weak safeguards for products before they are sold in other member states" (quoted in Stupp, 2018). The French concerns are linked to the possible penetration by foreign companies (also from the EU) in the domestic market. This would negatively impact, we hear, on the main objective of French cybersecurity governance, namely the industrial autonomy in this sector.

Table 3: French Cybersecurity Governance

	France
Decision-Making	Consensus-based, informal relations between state and industry
Dedicated Institutions and Agencies	Centralization (ANSSI - DGA)
Government Support	High (Public Investment, Label France Cybersecurity)

[6] The ECSO represent the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP).

Relations with EU institutions	Emphasis on industrial benefits

4. The UK: From Laissez-Faire to a Mixed Regulatory Landscape?

4.1. Decision-Making

Contrary to the French case, state-industry relations in the UK are characterized by less tight interactions. At a first glance, this could seem counterintuitive given the similarities between the British cybersecurity market and the French one. The British sector consists indeed of a handful of large companies, such as BAE Systems, BT and Qinetiq, and a myriad of micro and small enterprises. In particular, the British giant BAE Systems (one of the three most important military contractors in the world), through a very active strategy of acquisitions, is present in all of the segments of the cybersecurity market and it is listed as one of the top twenty providers of cybersecurity solutions globally (Boulanin 2018, p. 770). However, the British system, deriving from the specific government-industry relation that consolidated over the years in the UK, remains significantly different from the French one.

The British interest towards cybersecurity initially focused on cyber-defense in relation to state-sponsored cyber-attacks and was very much influenced by the 2007 attack on Estonia (Christou, 2016, p. 64). With the 2011 "UK National Cyber Security Strategy", the government implemented many measures to enhance its cooperation with industries. Since the state cannot effectively respond to cybersecurity threats without direct involvement of the private sector, the strategy referred to the Government Communication Headquarters (GCHQ) as the main institutional actor to facilitate the exchange of information between public and private actors. However, contrary to the French case, the UK cybersecurity strategy involved businesses not only at the level of information sharing but the overall strategy remained "business-led" (Guitton, 2013, p. 27). More precisely, the UK expected the businesses to operationalize the cyber strategy and induce transformations in cybersecurity. The broader idea was not to interfere with market forces, leaving the protection of critical infrastructure entirely to the private sector. The fact that the UK government initially left cybersecurity management in the hands of the private sectors was not part of a concerted public-private sector interaction, but it was a product of an autonomous state's decision (Carr & Tanczer, 2018:4). As revealed by a representative of the British cybersecurity industry, "our contacts with the state have been sporadic,

especially during the phase between 2011 and 2016. Nothing comparable to what happened in countries where industries have massively shaped the government's decision-making".[7][8]

However, the market-oriented approach of the British government and the arm's length relations between the UK and the industry slightly changed after the 2016 UK National Cyber Security Strategy (Carr & Tanczer, 2018, pp. 4-5). While in 2011 the idea that the market would "drive the right behavior" was central, by 2016 it was explicitly acknowledged that the combination of market forces and government encouragement has "not been sufficient in itself to secure our long-term interests in cyberspace at the pace required" (UK Government, 2016, p. 27). Indeed, the market-oriented approach of British cybersecurity governance had to give way to a mixed regulatory framework, characterized by a gradual institutional centralization, by increasing public investments to support the private sector but also by the lack of an active policy of market protection comparable to the French one.

4.2. Dedicated Institutions and Agencies

As outlined in the 2011 "UK National Cyber Security Strategy", the British governance structure was highly decentralized and characterized by the lack of dedicated institutions and agencies which the specific task to support the private sector. Overall, unlike the French case, there were several institutions with cybersecurity-related competencies, including the Cabinet Office, the Department for Business, Energy and Industrial Strategy (BEIS), the Department for Digital, Culture, Media and Sport (DCMS) and the Department for International Trade (DIT). There was also some confusion among the actors who were in charge to exercise leadership between the Security Minister in the Home Office and the Minister for the Cabinet Office and Cyber Security. In the specific case of state-industry relations, the GCHQ was the main contact point between the public and the private sector, but some experts noted a lack of coordination and information flowing from GCHQ to the industry (Christou, 2016, pp. 68-73).

A decisive change was promoted by the aforementioned 2016 UK National Cyber Security Strategy, which developed a more centralized system in order to react to market failures, poor investments by the private sector and, more broadly, to the difficult coordination between the public and the private sector (Carr & Tanczer, 2018). As emphasized in the new strategy: "a market-based approach to the promotion of cyber hygiene has not produced the required pace and scale of change; therefore, Government has to lead the way and intervene more directly by bringing its influence and resources

[7] Interview with a British cybersecurity industry representative 14/11/2019

to bear to address cyber threats" (UK Government. 2016, p. 13). London finally opted for a more centralized cybersecurity governance, through the creation of the National Cyber Security Centre (NCSC), to ensure the management of national cyber incidents and to set the policy and regulatory framework of critical national infrastructure operators. Launched in October 2016 as part of the GCHQ, the NCSC provides a single point of contact for the industry and it has brought together expertise from the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure. As noted by the interviews conducted with representatives of the British cybersecurity industry, this increasingly centralization of the cybersecurity governance and the creation of the NCSC has significantly improved state-industry relations and has promoted more state support to the private sector.[8]

4.3. Government Support

The degree of government support from the British government to the private sector has increased over time. The initial British market-oriented approach gave way to a more decisive state involvement and a gradual centralization of institutional structures, including greater public investments. However, this did not lead to a protection of the domestic market comparable to the French one, leaving the requests of the British cybersecurity industries partially unsatisfied. As highlighted by Christou (2016:68), the British government aimed to incentivize the private sector rather than establishing mandatory cybersecurity regulations. For instance, and this is a crucial difference with France, the UK government has constantly refused to develop a UK cybersecurity label, as Paris did to give a competitive advantage to its domestic industry. In this regard, Pauline Neville-Jones, former Minister of State for Security and Counterterrorism, made it clear that the government was against the idea (Guitton 2013, p. 28). British industrial players have always been particularly worried about the government's market-oriented approach and the lack of direct and indirect mechanisms to protect the market from possible foreign penetrations. Large companies (especially those also established in the defense market) aimed to penetrate and secure the new and profitable cybersecurity market and preferred to be protected by their own government. For instance, BAE Systems, explicitly complained about poor protection by the government: "the increasing use of Commercial Off-the-Shelf products and dependency on internet protocol (as opposed to proprietary) networks will have brought a wider range of vulnerabilities into MoD systems, some of which will already be knows to attackers" (quoted in House of Commons 2012-2013, pp. 18-19). Yet, the British government did not show any particular concerns to procure cybersecurity equipment and network components "off-the-shelf". The

[8] Interview with a British cybersecurity industry representative 14/11/2019; Interview with a British industry representative 17/11/2019

Minister for the Armed Forces acknowledged there was a potential risk, but this had to be balanced with cost, speed and efficiency of delivery, the urgency with which the equipment is needed, "and the extent to which you have any known concerns about the product that the supplier is potentially going to supply to you" (Defence Committee, 2012-2013). The Minister also highlighted that "there is no reason why you wouldn't" use commercial off-the-shelf products in cyber-defence systems, subject to advice from the National Technical Authority about whether the specific product was appropriate for the job" (Defence Committee, 2012-2013). The idea was that the private sector, in the absence of mandatory regulations and market protection, would have been forced to autonomously address cybersecurity threats more quickly and efficiently than they would with the burden of government intervention.[9]

A related problem for the British industry was related to the lack of state protection in the event of cyberattacks. As noted by the European Aeronautic Defence and Space Company (now Airbus) in a memorandum on UK cybersecurity threats, "at present it is not clear who owns the coordinated response to a national cybersecurity incident" (House of Commons, 2012-2013, p. 41). Indeed, there have been little direct governance of critical national infrastructures: as these are largely owned and operated by private industry, its governance resembles a form of macro-management through oversight via formal and informal statutory regulators and legal bodies. This seems in line with neo-liberal practices that promote minimum state intervention (Stoddart, 2016, p. 1082). The UK government has been explicit that this responsibility lies with the boards, owners and operators of the private entities themselves. While this position specifies that the government is not directly responsible for the cybersecurity of private corporations and their infrastructure, UK policy is also slightly ambiguous on this point. An initial reading of this statement seems to infer a contradiction with another policy statement: that ultimate national cybersecurity responsibility lies with the government. Indeed, the UK government recognizes that, although key sectors of economy and cyber infrastructure are in private hands, the government is ultimately responsible for "assuring their national resilience and (…) maintenance of essential services" (UK Government, 2016, p. 27). There is ambiguity between acknowledging the government's responsibility to ensure the safety of critical infrastructures (digital or otherwise) and not being involved in private companies' decisions.

In recent years, however, there has been an increase in public investments to support the private sector. The greater centralization of British governance appears therefore driven by the distinctive

[9] Interview British Defence Official 15/10/2019

traits of the cybersecurity market, in which there is a very close relationship between systems integrators and micro and small enterprises. The government needs to help the formation of industrial districts to better integrate these players, both financially and through a more direct involvement in the regulatory framework. The government has indeed incentivized the development of industrial districts of micro and small-sized companies, especially in the East London area. For instance, since 2012, almost three hundred new firms have been incorporated within the sector, representing a 58% increase in the number of firms overall. This has been driven mostly by micro firms (typically fewer than nine employees) with modest growth in medium and large firms. British policy has also probably changed to give greater weight to British industry exports in this sector. In 2018, the Department for International Trade produced its "Cyber Security Export Strategy" in which it projects export growing to 2.6 billion pounds by 2021 (Department for International Trade, 2018). According to the recent "Security Export Strategy", UK cybersecurity companies had a 95% increase in exports from 2012 to 2018. Moreover, cybersecurity represents currently the largest single security export category in 2018, just like it was in 2017; it is up from 38% to 40% (UK Government, 2019a). Yet, the British market still remains open to cybersecurity industries that want to do business, given that the UK outsource more than 30% of its cybersecurity spending (PWC, 2017).

4.4. Relations with EU institutions

The UK has not used, as noted in the French case, the European framework to specifically support its industry-related benefits. Between 2011 and 2016 there was a clear contrast between the UK market-oriented approach and the more decisive regulatory policy developed in Brussels. The European Commission already noted in 2001 that "market forces do not drive sufficient investment into security technology or security practice" (European Commission, 2001). In this regard, the lack of mandatory regulations for critical infrastructures' owners and the need for close cooperation and exchange of information between the public and private sectors were the basis of the EU's proposed NIS Directive. It is interesting to note that the UK has tried to shape the European directive, bringing its own market-oriented approach in its calls for reducing costs related to the proposed scope (including only critical infrastructure providers and not providers of information society services) (Christou 2016, p. 79). Other European countries, France in the first place, preferred a more centralized and regulatory approach. Perhaps also for this reason, the UK has set a clear preference for NATO to regulate state-industry relations. London was the main proponent of the NATO Industry Cyber Partnership, which left companies freer to regulate themselves than its EU counterparts (Christou 2016, p. 81). Indeed, the NATO defense-industrial partnerships are built to impose very soft regulations on individual states. This is in line with successive regulation-averse UK governments

The NIS directive has anyway put pressure on the UK to comply with European standards. Establishing the NCSC as the national technical authority and introducing more robust regulation for critical national infrastructures were both important steps in this direction. Before the NIS came into force, regulation of critical national infrastructures was broadly divided into economic regulators tasked with overseeing market competition issues (for example, the energy regulator Ofgem and the water regulator Ofwat) and regulators with statutory powers specifically to oversee security practices (for example, the Office for Nuclear Regulation).

Given the increasing regulatory activity of the EU in cybersecurity, it is important to investigate the impact of Brexit for UK cybersecurity. At the moment, there are concerns that Brexit can bring lowering investments in the UK by corporations, and a reduction in the number of cyber security professionals coming from Europe to work in the UK (Stevens and O'Brien, 2019, p. 23). The UK will also probably continue to be influenced by European legislation in this sector, given, for example, the recent transposition of NIS into the British legislative system. Moreover, as noted by Carr and Tanczer (2018, p. 8), the UK's transposition of the General Data Protection Regulation (GDPR) into a new Data Protection Bill in 2018 acted as a profound market modifying measure that will affect the UK beyond its exit of the EU. The 2016 UK cybersecurity strategy refers to the GDPR as a lever to "drive up standards of cyber security" (Cabinet Office, 2016, p. 27). The UK government stipulates that this approach does not mandate a specific set of cybersecurity measures. Rather, it places the expectation on organizations to take appropriate action, leaving the responsibility for managing risk in the hands of the private sector. This is consistent with the British approach towards cybersecurity, leaving the private sector the obligation to regulate itself, without putting in place very intrusive regulatory mechanisms. Recently, the Department for Digital, Culture, Media & Sport issued a Call for Views on the certification scheme currently anticipated by Regulation (EU) 2019/881 (the Cybersecurity Act) after Brexit. On this issue, the UK supports some form of soft cooperation on cybersecurity certification, but only on a case-to-case basis and probably without an overarching agreement (UK Government, 2019b). This may negatively affect UK industry's interests, as its cybersecurity firms export almost the 50% of products in Europe (over double the next largest region) (UK Government, 2019a).

Brexit is also strongly impacting on the sensitive issue of 5G, where the UK and EU member states are both facing a difficult choice in selecting industrial suppliers for this key digital infrastructure. On the one hand, the British government had initially assessed the 5G issue from a purely market perspective, in which Chinese companies (also because of Huawei's strong position in the UK market) seemed to have a decisive comparative advantage. On the other hand, however, the British

government realized that this choice could have negative consequences for the relationship with the US and the very strong intelligence relations between these two countries and their allies (Stevens 2019). This decision is complicated by the fact that Brexit is harming the ability to coordinate the UK position with the EU's attempts to find a coordinated approach on this strategic decision (Stevens & O'Brien, 2019).

Table 4: UK Cybersecurity Governance

	UK
Decision-Making	Arm's length relationship between the state and the industry
Dedicated Institutions and Agencies	Slowly Centralized around the NCSC
Government Support	Medium - Public Investment but not UK cybersecurity label
Relations with EU institutions	Both cooperative and competitive patterns, but mainly focused on strategic-operational issues

5. Comparing French and UK Cybersecurity Governance

As shown in the empirical analysis, it is possible to identify two different models of state-industry relations in cyber-governance.

French cybersecurity governance is based on consensus-based and informal relations between the state and the industry. There is a high government's support for the development of cybersecurity industrial capabilities and a high degree of institutional and bureaucratic centralization. The distinctive relations between state and industry in public governance ecosystems, as discussed in the theoretical framework, provide also strong insights on how France behave in the European context, given that Paris has consistently used EU institutions to advance its industry-related preferences. Our analysis shows the convergence of the French and the European Commission approaches to cybersecurity, with a special focus on internal market protection from extra-European suppliers. This approach was contested in Europe, where other states (including Germany) had different policy-preferences (Terpan & Saurugger, 2020).

London seems reluctant to move more forcefully on cybersecurity market regulation and, by default, continues to rely on market forces to improve operators' cyber resilience, despite recognizing the previous failure of this approach. Under the government's previous policy of "light touch" regulation, only a handful of critical national infrastructures sectors had regulators with specific statutory powers to ensure cybersecurity. This has resulted in what the British government described as a "mixed" regulatory landscape, with the civil nuclear and financial services sectors possessing strong regulatory frameworks and other sectors lacking "backstop powers to intervene" or "clear cyber security standards", or both (Joint Committee on the National Security Strategy, 2018). Overall, there has been a low governmental support to the UK firms and a low level of centralization of public institutions and agencies. However, the British government has also recognized the need to intervene to address market failures and poor private sector investments (Carr & Tanczer, 2018). The UK was not comfortable with the EU focus on market protection, but it was not able to successfully advance its liberal policy-preferences in Brussels. After Brexit, the UK is also realizing the difficulties to find some sort of concerted approach with European partners outside the EU framework to deal with the sensitive issue of 5G network.

The French governance remains much more based on an intermingled relationship between the industry and the government, whereas the UK preserves a certain distance between the two counterparts. Push toward centralization is much stronger in France than in the UK, as well as public funding and indirect public support through governmental certifications.

Table 5: Comparison between French and UK Cybersecurity Governance

	France	**UK**
Decision-Making	Consensus-based, informal relations between state and industry	Arm's length relationship between the state and the industry
Dedicated Institutions and Agencies	Centralization (ANSSI - DGA)	Slowly Centralized around the NCSC
Government Support	High (Public Investment, Label France Cybersecurity)	Medium - Public Investment but not UK cybersecurity label
Relations with EU institutions	Emphasis on industrial benefits	Both cooperative and competitive patterns, but mainly focused on strategic-operational issues

6. Conclusions

The study aims to contribute to the debate on state-industry relations and cybersecurity. Contrary to those who see a transformative effect of cyber on cross-national state-industry arrangements in economic and industrial policies, we show that existing political economy models may well explain how states and industries interact in the governance of cybersecurity. Drawing on an original interplay of comparative political economy and defense policy scholarships, we distinguish between public and private cyber-governance ecosystems. This theoretical framework allows to identify three analytical properties through which it is possible to compare different state-industry relations: the degree of protection by the government; the degree of interpenetration between public and private sectors elite network; the status and autonomy of procurement agencies from the industry's influence. In public governance ecosystems there is a high degree of government protection, a high degree of interpenetration between public and private actors and a very close relationship between public procurement agencies and the private sector. In contrast, in private governance ecosystems, there is a low degree of protection by the government, low levels of interpenetration between members of the public sector and those in the private sector and an arm's length relationship between public procurement agencies and the private sector. These theoretical considerations led also to different hypotheses on how public and private governance ecosystems developed different models of cybersecurity governance.

Focusing on the French and British cases, two examples respectively of public and private governance ecosystems, our hypotheses have been largely confirmed. The French cybersecurity governance is characterized by the presence of formal and informal relations between state and industries, a high degree of public investment in the private sector and centralized institutions. France has also used the EU mainly to advance its industrial interests. In contrast, in the UK there are more arm's length relations between the state and industries (which in fact have repeatedly complained about poor government's protection) and a less centralized system. Moreover, the UK, differently to France, has not used the EU channel to advance its industry-related preferences. These results confirm the macro-differences between the French and British respectively public and private governance models.

We have also highlighted that from 2016 onwards there has been a slow convergence between these two governance models. France has begun to adopt more business-oriented measures, seeking to ease the regulatory tightening on the cybersecurity market that characterized the period between 2008 and 2016. In contrast, the UK government has started to more decisively intervene in cybersecurity, both through a greater centralization of institutional structures and agencies, and through a more decisive

support to the domestic market. Although the two models remain clearly distinct, we believe that rather than outright challenging our argument, this observation nuances it. Indeed, the observed convergence between the two models allow to better refine the theory taking seriously into account functional reasons linked to the structure of the cybersecurity market. Differently from defence procurement, the cybersecurity market is very much dependent on the technological innovation produced by micro and small companies and by their collaboration with large companies, which in turn possess the industrial capacity to sell finished products to the market. For this reason, both in France and in the UK, the governments have sustained new financial and institutional channels to develop industrial districts, in order to facilitate the collaboration between small and large companies. As noted in the empirical analysis, government interest in developing districts and industrial-technological clusters in Brittany for France and East London for the UK is certainly a paradigmatic example of this argument. The conceptual distinction between public and private governance is therefore analytically useful for comparative purposes, but new research may also expand our argument, trying to further integrate the specificities of this evolving market within the framework of public and private governance ecosystems.

The added value of this research lies in the original interplay of comparative political economy and defense policy to explain state-industry relations in cybersecurity. This study, we believe, also opens two additional avenues for future research: first, it would be beneficial to integrate our theoretical framework on the domestic determinants of cyber-governance with a systematic assessment on how domestic and international drivers simultaneously impact on state-industry relations in this domain (Cavelty & Egloff, 2019). Recent studies have, for instance highlighted how international pressures shape economic policy initiatives focused on the domestic domain, not least in the high-technology arena (Drezner, 2019; Weiss & Thurbon, 2020; Weiss, 2020). This may also well be the case in cyberspace.

Second and related point, new research can integrate the study of state-industry relations in cybersecurity by systematically taking into account the EU pressure in this domain. The EU regulatory approach on cybersecurity is indeed intensifying over the past few years, especially after the launch of the EU Cybersecurity Act in 2019. In 2020, EU member states and institutions created the Cybersecurity Competence Centre and Network to explicitly reinforce the competitiveness of the Union's industry and support procurement of cybersecurity products and solutions. In these documents and initiatives, the EU - in line with the French preferences - explicitly aims to support the private sector through the protection of the internal market from foreign suppliers. Perhaps exacerbated by COVID-19 (see Carrapico & Farrand, 2020), there is the perception in Brussels that

European companies' risk being left behind if they are unable to defend their market shares and to become dependent on non-European products. The US-China competition and the consequent creation of two distinct "techno-spheres", each with its own products and standards, may lead to Europe's risk of being caught in between these two spheres and constantly being pulled to one side or the other. These considerations are currently at the top of the agenda of the new "geopolitical Commission" in terms of industrial policy and technological sovereignty (European Commission, 2019b). These considerations are also linked to the still strong relation of European states with the American security and defense sector. Through NATO and other security arrangement like the Five Eyes arrangement, the French and especially the UK systems remains tightly integrated to and to a large extent dependent on the US system. From this perspective, a certain pattern of convergence between France and the UK might be the result of both political and intellectual exogenous pressure to align with and remain integrated to the US system, even more if eventually the decoupling and polarization with the Chinese industry will increase. Overall, works that take into account both different models of political economy and international drivers of cyber-governance would certainly help our understanding of current international affairs.

Acknowledgments

We thank Andre Barrinha as well as the anonymous reviewers and the editors of *Review of International Political Economy* for comments and suggestions on earlier versions of this article. Antonio Calcara thanks the Department of Political Science of LUISS University for a scholarship on "Cybersecurity Governance" (2019-2020) and the Research Foundation – Flanders (FWO) G054221N grant on "Competition and cooperation in European defence: private versus public governance and EU policy outcomes".

References

Aggarwal, V. & Reddie, A. (2018a). Comparative industrial policy and cybersecurity: a framework for analysis. *Journal of Cyber Policy*, 3(3), 291-305.

Aggarwal, V. & Reddie, A. (2018b). Comparative industrial policy and cybersecurity: the US case. *Journal of Cyber Policy*, 3(3), 445-466.

Amable, B. (2016). Institutional complementarities in the dynamic comparative analysis of capitalism. *Journal of Institutional Economics*, 12(1), 79–103

Ansaloni, M. & Smith, A. (2018). The neo-dirigiste production of French capitalism since 1980: the view from three major industries. *French Politics*, *16*(2), 154-178.

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *International Affairs*, *96*(3), 749-766.

Baumard, P. (2017). *Cybersecurity in France*. Springer, Cham.

Berry, C. (2019). From receding to reseeding: industrial policy, governance strategies and neoliberal resilience in post-crisis Britain. *New Political Economy*, 1-19.

Betz, D. J., & Stevens, T. (2011). *Cyberspace and the state: Toward a strategy for cyber-power*. Abingdon, UK: Routledge.

Bockel, J. M. (2012). La cyberdéfense, *Revue Défense Nationale*, June.

Bossong, R. & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change*, 67(3), 265-288.

Boulanin, V. (2013). Cybersecurity and the arms industry. *SIPRI Yearbook 2013: Armaments, disarmament and international security* (pp. 218–226). Oxford: Oxford University Press.

Boulanin, V. (2018). Cyber Capabilities. In Meijer, H. and Wyss, M., *European Defence Policies and Armed Forces* (pp.760-778). Oxford: Oxford University Press.

Boulanin, V. & Verbruggen, M. (2017). Mapping the development of autonomy in weapon systems. *Stockholm International Peace Research Institute*. November 2017.

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review*, *5*(4), 28.

Cabinet Office (2016). *The UK Cyber Security Strategy 2011-2016 Annual Report*. Retrieved from:

Calcara, A. (2020). *European Defence Decision-Making: Dilemmas of Collaborative Arms Procurement*. Routledge.

Calcara, A., Csernatoni, R., & Lavallée, C. (2020). *Emerging Security Technologies and EU Governance: Actors, Practices and Processes*. Routledge.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs,* 92(1), 43-62.

Carr, M. & Tanczer, L. (2018). UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions. *Journal of Cyber Policy*, 3(3), 430-444.

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor?. *JCMS: Journal of Common Market Studies*, *55*(6), 1254-1272.

Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of COVID-19: The case of EU Cybersecurity Policy. *Journal of European Integration*. (online first view).

Cavelty, M. D., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review*, *15*(1), 37-57.

Cheung, T. M. (2018). The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy*, 3(3), 306-326.

Christou, G. (2019). The collective securitisation of cyberspace in the European Union. *West European Politics*, 42(2), 278-301.

Clift, B. (2009). 'Second Time as Farce? The EU Takeover Directive, the Clash of Capitalisms and the Hamstrung Harmonisation of European (and French) Corporate Governance', *Journal of Common Market Studies*. 47(1), 55-79

Clift, B. & McDaniel, S. (2019). Capitalist convergence? European (dis?) integration and the post-crash restructuring of French and European capitalisms. *New Political Economy*, 1-19.

Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance*, *6*(2), 13-21.

Crouch, C. (2005) *Capitalist Diversity and Change: Recombinant Governance and Institutional Entrepreneurs*. Oxford: New York: Oxford University Press.

CSFRS (2012). *CSFRS National Strategy Report*. Paris: CNRS Editions.

D'Elia, D. (2014). La cybersécurité: de la représentation d'un bien public à la nécessité d'une offre souveraine. *Securite et strategie*, 19(4), 72-80.

D'Elia, D. (2018). Industrial policy: the holy grail of French cybersecurity strategy?. *Journal of Cyber Policy*, 3(3), 385-406.

Defence Committee (2012-2013). MoD networks, assets and capabilities. Retrieved from: https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/10605.htm

Department for International Trade (2018). *Cyber Security Export Strategy*. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/693989/CCS151_CCS01188101241_Cyber_Security_Export_Strategy_Brochure_Web_Accessible.pdf

DeVore M. & Weiss M., (2014). Who's in the Cockpit? The Political Economy of Collaborative Aircraft Decisions. *Review of International Political Economy*, 21(2), 497–533.

DeVos, S. A. (2010). The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed. *Fordham Intellectual Property, Media & Entertainment Law Journal* 21(1):173-228.

Drezner, D. W. (2019). Counter-Hegemonic Strategies in the Global Economy. Security Studies, 28(3), 505-531.

du Guerny, S. (2019). Rennes devient la place forte des soldats de la cyberdéfense. *Les Echos*. Retrieved from: https://www.lesechos.fr/pme-regions/bretagne/rennes-devient-la-place-forte-des-soldats-de-la-cyberdefense-1142331

EIB (2017). France: Juncker Plan – First EIB financing for cybersecurity in France. European Investment Bank. October. Retrieved from: https://www.eib.org/en/press/all/2017-261-plan-juncker-1er-financement-de-la-bei-dans-le-domaine-de-la-cybersecurite-en-france

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory?. *International political science review*, *27*(3), 221-244.

European Commission (2001). *Network and information security: proposal for a European policy approach*. Brussels: European Commission.

European Commission (2019a). European Cybersecurity Act. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Farrell, H. (2006). Regulating information flows: States, private actors, and E-commerce. *Annual Review of Political Science 9*, 353-374.

Farrell, H. & Newman, A. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42-79.

Farrell, H. & Newman, A. (2021). The Janus Face of the Liberal International Information Order: When Global Institutions are Self-Undermining. *International Organization* (forthcoming).

Faure, S. B., Joltreau, T., & Smith, A. (2019). Who governs defense companies? A sociological approach to contemporary capitalisms in France and Britain. *Revue internationale de politique comparee*, *26*(1), 11-45.

French Ministry for Foreign Affairs (2019). *France and cyber security*. Retrieved from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/

Gertz, G., & Evers, M. M. (2020). Geoeconomic Competition: Will State Capitalism Win?. *The Washington Quarterly*, *43*(2), 117-136.

Gholz, E., & Sapolsky, H. M. (2020). The Many Lines of Defense: The Political Economy of US Defense Acquisition. *Journal of Global Security Studies*.

Goyer, M. (2011). *Contingent capital: Short-term investors and the evolution of corporate governance in France and Germany*. Oxford: Oxford University Press.

Guitton, C. (2013). Cyber insecurity as a national threat: overreaction from Germany, France and the UK?. *European Security*, 22(1), 21-35.

Hall, P. & Soskice, D. (2001). *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage*. Oxford: Oxford University Press

Hay, C. (2020). Does capitalism (still) come in varieties?. *Review of International Political Economy*, *27*(2), 302-319.

House of Commons (2012-2013). *Defence and Cyber-security: Sixth Report of Session 2012-2013.* Retrieved from: https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf

Jabko, N. & Massoc, E. (2012) "French Capitalism under Stress: How Nicolas Sarkozy Rescued the Banks," *Review of International Political Economy. 19(4):* 562-585

Joint Committee on the National Security Strategy (2018). *Cyber Security of the UK's Critical National Infrastructure Third Report of Session 2017–19*. Retrieved from: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf

Kaska, K. Beckvard, H. & Minárik, T.(2019). Huawei, 5G and China as a Security Threat. *CCDCOE: Nato Cooperative Cyber Defence Centre of Excellence*. Retrieved from: https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), 7-40.

Lundmark, M. (2011). *Transatlantic Defence Industry Integration: Discourse and Action in the Organizational Field of the Defence Market*. Thesis (Ph.D). Stockholm University

Masson, H., Martin, K., Quéau, Y., Senior, J. (2015). *The Impact of the "Defence Package" Directives on European Defence. European Parliament's Subcommittee on security and defence.* Brussels: European Parliament. Retrieved from: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549044/EXPO_STU(2015)549044_EN.pdf

Matania, E., Yoffe, L., & Goldstein, T. (2017). Structuring the national cyber defence: in evolution towards a Central Cyber Authority. *Journal of Cyber Policy*, *2*(1), 16-25.

Matelly, S., & Lima, M. (2016). The Influence of the State on the Strategic Choices of Defence Companies: the Cases of Germany, France and the UK after the Cold War. *Journal of Innovation Economics & Management*. 20(2), 61-88.

Mew, B. (2016). ANSSI – the people behind the French National Digital Security Strategy. *Compare the Cloud*. Retrieved from: https://www.comparethecloud.net/articles/anssi-the-people-behind-the-french-national-digital-security-strategy/

PWC (2017). *Cyber security: European emerging market leaders / January 2017.* Retrieved from: https://www.pwc.co.uk/deals/assets/cyber-security-european-emerging-market-leaders.pdf

Roberts, A., Choer Moraes, H., & Ferguson, V. (2019). Toward a Geoeconomic Order in International Trade and Investment. *Journal of International Economic Law*, *22*(4), 655-676.

Rosemain, M. (2018). France's Thales sees more cybersecurity sales after strong 2017. Reuters. Retrieved from: https://www.reuters.com/article/us-thales-cyber/frances-thales-sees-more-cybersecurity-sales-after-strong-2017-idUSKBN1FW0T1

Ruohonen, J. (2019). An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union. *European Journal for Security Research*, 1-29 (online first view).

Schmidt, V. & Thatcher, M. (2013). *Resilient liberalism in Europe's political economy*. Cambridge University Press.

Serfati, C. (2001). The Adaptability of the French Armaments Industry in an Era of Globalization. *Industry and Innovation,* 8(2), 221-239.

Shonfield, A. (1965). *Modern Capitalism: The Changing Balance of Public and Private Power.* Oxford: Oxford University Press

Stevens, T. (2019). What the Huawei affair means for Anglo-American security cooperation. UK in Changing Europe. May. Retrieved from: https://ukandeu.ac.uk/what-the-huawei-affair-means-for-anglo-american-security-cooperation/

Stevens, T. & O'Brien, K. (2019). Brexit and Cyber Security. *The RUSI Journal*, 164(3), 22-30.

Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs*, 92(5), 1079-1105.

Streeck, W. (2010). E Pluribus Unum? Varieties and commonalities of capitalism. Max-Planck-Institut for Gesellschaftsforschung Discussion Paper 10/12/.

Stupp, C. (2018). French cybersecurity chief warns against 'step back into the past'. *EURACTIV.* Retrieved from: https://www.euractiv.com/section/cybersecurity/news/french-cybersecurity-chief-warns-against-step-back-into-the-past/

Terpan, F., & Saurugger, S. (2020). Soft and hard law in times of crisis: budget monitoring, migration and cybersecurity. *West European Politics*, 1-28.

UK Government (2016). *National Cyber Security Strategy 2016 to 2021*. London: HM Government.

UK Government (2019a). UK Defence & Security Export Statistics for 2018. Department for International Trade, Defence and Security Organization. September. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822133/uk-defence-and-security-export-statistics-for-2018.pdf

UK Government (2019b). EU Cyber Security Certification (EU Exit) Call for Views. Department for Digital, Culture, Media & Sport . December. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/853371/EU_Cyber_Security_Act-_Call_for_Views_1__1_.pdf

Van den Hurk, M., Brogaard, L., Lember, V., Petersen, O. H., & Witz, P. (2015). National varieties of Public–Private Partnerships (PPPs): A comparative analysis of PPP-supporting units in 19 European countries. *Journal of Comparative Policy Analysis: Research and Practice*. 18(1):1-20.

Vergara, I. (2019). Réseaux 5G: la France adopte la "loi Huawei". Le Figaro. July, 24.

Villani, C. (2018). *For a Meaningful Artificial Intelligence: Towards a French and European Strategy*. Mission assigned by the Prime Minister Édouard Philippe A parliamentary mission from 8th September 2017 to 8th March 2018

Weiss, M., & Jankauskas, V. (2019). Securing cyberspace: How states design governance arrangements. *Governance*, *32*(2), 259-275.

Weiss, M. (2020). Varieties of privatization: informal networks, trust and state control of the commanding heights. *Review of International Political Economy*, 1-28 (online first view).

Weiss, L., & Thurbon, E. (2020). Developmental State or Economic Statecraft? Where, Why and How the Difference Matters. *New Political Economy*, 1-18.

White Paper (2008). *The French White Paper on Defence and National Security*. Odile Jacob Publishing Corporation, New York.

White Paper (2013). *White Paper on Defence and National Security*. Paris: Ministry of Defence.