JCMS Journal of Common Market Studies UACES
JCMS 2021 pp. 1–17 DOI: 10.1111/jcms.13175

When Trust Fades, Facebook Is No Longer a Friend: Shifting Privatisation Dynamics in the Context of Cybersecurity as a Result of Disinformation, Populism and Political Uncertainty

HELENA CARRAPICO[1] and BENJAMIN FARRAND[2]
[1]Northumbria University, Newcastle-upon-Tyne [2]Newcastle University, Newcastle-upon-Tyne

Abstract

This article discusses how populism and political uncertainty are impacting on one of the main current trends in the Area of Freedom, Security and Justice, namely the privatisation of JHA. Through an exploration of a cybersecurity policy case study, the article proposes to understand how the privatisation of internal security, which has resulted in private actors shaping JHA policies and regulation, is currently being disrupted. Through the use of the theoretical lenses of Regulatory Capitalism, the article argues that this change is directly related to a reduction in trust relations between the State and certain private sector actors, which occurs when priorities in addressing populism and political uncertainty are perceived to diverge.

Keywords: security privatization; area of freedom; security and justice; cybersecurity; political uncertainty

Introduction

Cybersecurity has rapidly risen to the top of the Area of Freedom, Security and Justice's (AFSJ) agenda (Council of the European Union, 2019). The recognition that information security is deeply woven into the fabric of European societies has led European Union (EU) institutions and Member States to focus attention on the way the internal security landscape is being challenged by cybersecurity incidents (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2017, p. 1). Concerns over an expanding panoply of malicious activities, including cyber-crime, State and non-State sponsored cyber-attacks, fake news, and disinformation campaigns, have served as a basis for the development of a EU comprehensive and coherent cyber-security policy, focused on promoting preventative programmes, enhancing law enforcement capabilities, fostering awareness, and developing institutional coordination mechanisms.

For the EU, the key to the effectiveness of this policy field relies on cooperation with private actors, as most critical information infrastructures (CII), such as communication networks related to energy, transport, finance and health, are privately owned. Consequently, the EU has gradually invested in a form of governance for cybersecurity that is heavily based on public–private partnerships. The decision to situate non-traditional actors at the heart of security production raises a number of interesting questions regarding effectiveness and accountability, which the academic literature on security privatization and commercialization has addressed to a great extent (Krahmann, 2010; Abrahamsen and Leander, 2016). The potential for private actors to shape and even take

part in security decision-making has received more limited attention, although research in this area has started to emerge in relation to the AFSJ (Carrapico and Farrand, 2017). An important gap, however, remains in terms of the limits to security privatization trends and the political conditions that could disrupt or even reverse such trends. More specifically, there has been, to the authors' best knowledge, no reflection on the connection between disinformation, populism and political uncertainty, and changing public–private relations in the field of security.

In a context where private companies have become ubiquitous in the operationalization and, in cybersecurity, even design of internal security policies and strategies, this article aims to explore how the rise in populism and the subsequent political uncertainty are impacting on this trend. For the purpose of this article, populism is understood not as a specific ideology, but rather as a form of political communication that has become quite prevalent in a number of European countries, revolving around an anti-elite and emotional discourse, as well as a disregard for traditional politics and processes (Laclau, 2007; Moffitt, 2017; Norris and Inglehart, 2019). The rupture with traditional politics and policies brought about by populist governments creates a high level of uncertainty regarding the continued implementation of domestic policies, the credibility of domestic political architectures, international cooperation, and participation in international organizations (Bronk and Jacoby, 2020). The main argument of the article is that in a context where disinformation has become a very serious concern for the EU, by fostering populism and putting at risk the democratic legitimacy of the current political architecture, there has been a re-assessment of the trust at the basis of public–private cooperation. This is largely the result of some private actors being perceived as being unable or unwilling to address this problem. The article creates a dialogue between three distinct areas of academic literature, which it proposes to contribute to: (1) the privatization of security – by exploring its limits, as well as a policy field rarely covered; (2) the further development of Regulatory Capitalism as a theoretical framework – by reflecting on the role of trust in the development and erosion of public–private relations; and (3) the literature on populism – by considering the impact of populism on a policy field that is yet to be considered by this body of literature.

The article is structured into three sections: the first maps the privatization trends within the AFSJ, indicating that they have become a defining feature of this policy field. This section also proposes that the privatization of Justice and Home Affairs can be best understood through the theoretical lenses of Regulatory Capitalism, a framework that explains the rationale and decision-making behind the positioning of private actors at the heart of policy operationalization and regulatory production. The second section emphasizes the evolution of the private actors present in Network and Information Security (NIS), a sub-field of cybersecurity, focusing in particular on their role as shapers of regulation and regulatory standards. The final section of the article makes the argument that, when trust and the shared sense of responsibility in protecting information security are eroded, private actors, such as social media platforms, can be repositioned outside of decision-making centres. This case study clearly indicates that privatization trends are not unidirectional and that the perception of divergent values can re-orient public–private cooperation in the direction of hierarchical relations.

I. The Privatization/Commercialization of the Area of Freedom, Security and Justice and its Conceptualization through the Lenses of Regulatory Capitalism

When exploring the question of who provides security, a considerable body of literature has developed the idea that security has long ceased to be the monopoly of the State and that businesses have acquired the capacity to protect themselves and to provide security for others (Bryden and Caparini, 2006). This literature points out not only the long history of security businesses supporting and shaping State formation from the Middle Ages to the Nineteenth Century, but also the re-emergence of these actors in the post-Cold War period in the format of Private Military and Security companies (PMSC) (Singer, 2007; Abrahamsen and Leander, 2016). This literature has mainly focused on five elements: (1) highlighting that security privatization has become ubiquitous despite society's general assumption that the Weberian State remains the norm (Abrahamsen and Williams, 2010); (2) theorizing the root causes of privatization in the field of security (Kruck, 2014); (3) refining the concept of privatization, which is understood to mean 'the incidence or process of transferring ownership, control or competences from the public sector (State) to the private sector (business)' (Leander, 2005); (4) exploring the way the security market is organized (Krahmann, 2010), and (5) denouncing the consequences of this process for democratic institutions and for the safety of individuals (Leander, 2010).

Although this literature has gained considerable importance in the context of Security Studies, namely of international security governance, its engagement with the study of the AFSJ has been considerably more limited. Even though some academic works have focused on internal security, such as private actors contributing to local policing (Button, 2002), as well as managing prisons (Hucklesby and Lister, 2018), network and information infrastructures (Carrapico and Farrand, 2017), and asylum systems (Darling, 2016), these insights have mainly stemmed from Criminology, Sociology, Geography and Migration Studies. As a result, there has been little reflection on the role and impact of private actors in the AFSJ, in particular, from a European integration perspective.[1] And yet, private actors have become central partners in implementing and even shaping Justice and Home Affairs policies.

The mapping of private actor participation in the AFSJ is particularly complex, given the very wide range of sectors these actors are involved in, the activities performed, the degree of contribution, and the different emerging formats of public–private partnerships. This pluralisation in security provision has been characterized by a variety of inputs, with private actors' roles ranging from implementation to advisory and policy-shaping, as well as by a diversification in the nature of the businesses involved, with private actors whose main business is not security-related rapidly increasing their presence (Bures and Carrapico, 2017). These are not only limited to large-scale conglomerates who have taken the decision to invest in the field of security (this is the case, for example, of Sodexo, whose original area was hospitality, of Sopra Steria, an information technology consultancy company currently responsible for UK visas and citizenship application services, and of Palantir, a company specializing in big data analytics, that provides EU

[1]The academic literature on the AFSJ occasionally refers to security privatization, highlighting it as an important trend, but it remains largely under-researched (Bossong and Rhinard, 2016).

agencies with counter terrorism and cybersecurity tools), but also of private actors whose main activity lies elsewhere and which have been enrolled, voluntarily or involuntarily, to contribute to this field. These include finance (Bures, 2016), insurance (Petersen, 2008), transport (Aarstad, 2017), and Internet provision companies (Bossong and Wagner, 2017), among other areas. In the field of civil aviation, for instance, private companies are tasked with contributing towards enhancing security, namely the fight against terrorism and organized crime, by supplying passenger data (Kaunert *et al*., 2012), whereas in the financial sector, they are tasked with monitoring transaction data and reporting on suspicious activity (Bures, 2016). Furthermore, private actors contribute not only to the provision of goods and services, but also to policy and regulation production, by serving as advisers to national and EU institutions and agencies, by commenting on proposed policies and initiatives (as done by industry representatives sitting in the Permanent Stakeholders Group of ENISA, the EU Cybersecurity Agency, and even by co-creating technical security standards, strategies and policies (a practice that has become the norm in the area of Network and Information Security; Carrapico and Barrinha, 2017).

This article proposes contributing to the security privatization literature by highlighting the limits to privatization trends and by analysing the factors that can influence them. By shedding light onto a lesser explored area of security privatization, that of the AFSJ, and in particular the case study of EU cybersecurity policy, it underlines that populism and its consequent political uncertainty have a direct impact on privatization dynamics. More specifically, the increased spread of disinformation in the online environment facilitates the growth of populism and political uncertainty through the challenging of the legitimacy of democratic and political structures. The perceived inability and unwillingness of private sector actors to effectively combat this disinformation in turns results in a changing perception of the role of these actors as part of a regulatory network, resulting in a need to reassess the dynamics of private-public cooperation in cybersecurity provision.

Understanding AFSJ Privatization through Regulatory Capitalism

The authors propose that the privatization trends in the AFSJ can be best understood through the theoretical lenses of Regulatory Capitalism, which focuses on the division of labour between the public and private sectors in regulating, distributing and providing societal services (Braithwaite, 2005; Levi-Faur, 2005). This framework is, above all, interested in asking who is responsible for leading policy (which it calls 'steering') and providing goods and services (which it calls 'rowing') in the context of public services, and uncovering the processes supporting the adjudication of these responsibilities. For the purpose of this article, Regulatory Capitalism will be used as a framework for understanding the rationale and practices supporting the shift in internal security provision from the hands of the State to those of private actors, as well as the consequent emergence of private companies as internal security providers, experts and regulators. Although other theoretical frameworks that consider the role of private actors in the development of policy fields were also explored, these tended to focus on the format of the public–private partnerships, its shaping of policy fields, and the autonomy granted to private actors, which were insufficient to explain the ideational change observed within public–private relations. Regulatory Capitalism, on the other hand, offers a historical view capable of explaining the partial return to more hierarchical public–private relations when the norms

and values usually ascribed to the private sector are perceived to change. In its original version, this theoretical framework has shortcomings in terms of the lack of attention paid to the role of trust in changing public–private dynamics, which the authors hope to contribute to in this article.

Whereas the State's role in creating and maintaining the political, economic and social infrastructure of European societies accelerated after the Second World War, the 1970s saw the introduction of political economic ideas prioritizing the de-regulation of markets and institutional reform through the withdrawal of the State. At the basis of Neoliberal thought was the idea that societal well-being and development would be best achieved through political economic practices associated with free trade, private property rights, individualism, and cuts to public spending and welfare provision (Harvey, 2007). Such practices were attained through increasing reliance on private actors' expertise and capacity, including in areas traditionally controlled by the State, such as energy and communications. State regulation of the economy was presented as being prone to instability given its connection to political interests and electoral results (Moe, 1990). The private sector, on the other hand, was understood as better placed to advance economic development given its level of efficiency and perceived apolitical stance. This powerful discourse would become mainstream throughout the 1980s and 1990s, leading to radical change in the role of private actors. The Regulatory Capitalism framework divides the evolution of the public–private division of labour into three time periods: (1) laissez-faire capitalism (1800s–1930s), (2) welfare capitalism (1940s–1970s), and (3) regulatory capitalism (1980s onwards).

As can be seen from Table 1, Levi-Faur identifies a first time period of regulatory governance, entitled Laissez-Faire Capitalism, where both the policy implementation (rowing) and policy production/advice (steering) were the responsibility of the private actors. It is followed by the Welfare Capitalism period, characterized by State steering in terms of organizing the economic activity, as well as State rowing regarding the provision of goods and services. Private initiative coexists during this period but is limited to specific areas of activity (Braithwaite, 2005). In this context, the role of private actors is passive, as objects of State regulation, and their relation with the State is clearly hierarchical. From the 1980s onwards, as deregulation strategies begin to spread, the State continues to control the main direction of the economy, although the steering is now shared with independent regulatory agencies, and the private actors gradually become prominent in the provision of goods and services. The relation between the State and the private sector is still hierarchical, but the latter adopts a more active role as it becomes responsible for the adoption of regulation. Levi-Faur and Braithwaite's framework was complemented by Carrapico and Barrinha (2017) who added a fourth time period, entitled

Table 1: The Transformation of Governance and the nature of Regulatory Capitalism (Source: Levi-Faur, 2005)

	Laissez-faire capitalism (1800s–1930s)	*Welfare capitalism (1940s–1970s)*	*Regulatory capitalism (1980s–)*
Steering	Business	State	State and agencies
Rowing	Business	State	Business

Networked Regulatory Capitalism, to reflect the idea that the private sector, in particular in new policy areas, such as Cybersecurity, was no longer just rowing, but was also taking part in the steering (see Table 2).

In this latest period of time, the hierarchical relation between State and private actors gives way to a collaborative relation, more similar to a network, where the private sector is considered to be best placed in terms of expertise and capacity, not only to implement policy and regulation, but also to lead on it in the format of self-regulation, as well as by taking directly part in decision-making processes (advising State bodies and sitting on the board of regulatory agencies). Given their closer proximity to the ground, private actors are perceived as having a more accurate knowledge of societal and market dynamics, placing them in an ideal position to advise policy makers, or even co-decide as to how sectors should be regulated. However, does this mean that privatization trends have become a permanent characteristic of the AFSJ, or is there the potential for their reversal? As the third section of this article will discuss, concerns over populism's increased reach in the online environment have deeply impacted upon trust relations between EU policymakers and certain online service providers, leading to the disruption of security privatization trends in the field of cybersecurity. As a result, there appears to be a move toward 'reclaiming' the steering of cybersecurity policies online as it relates to social media platforms, whereas other private actors such as cybersecurity software providers remain in this steering position. The authors of this article argue that these emerging challenges to privatization should be reflected in the Regulatory Capitalism framework, in the form of 'Selective' Regulatory Capitalism, in which trust relations are highly relevant in determining the level of policy-setting initiative that different private actors are afforded; rather than a 'steering and rowing' position being ubiquitous online, it is variable, dependent upon perceptions of shared values and levels of trust (see Table 3).

II. Private Actors in Network and Information Security: From Rowing to Steering

Cybersecurity is highly complex, with threats not restricted to a single type, a single sphere of activity or a geographical location. Instead, the threats are multitudinous, with no respect for physical borders or distinctions between public or private actors. Cybersecurity threats can target both the public and private sector and they can be perpetrated for reasons of personal profit, political protest, or to attain state-based interests. Given the highly distributed nature of cybersecurity threats, the risks are not easily managed, particularly by individual companies or states. Cooperation is therefore essential in order to ensure effective protection from cyber-attacks. In this section, the authors will discuss why private actors in the online environment have been afforded

Table 2: Source: Adaptation of Levi-Faur (2005) and Braithwaite (2005)

	Laissez-faire capitalism (1800s–1930s)	*Welfare capitalism (1940s–1970s)*	*Regulatory capitalism (1980s–)*	*Networked regulatory capitalism (2000s–)*
Steering	Business	State	State and agencies	State, agencies, business
Rowing	Business	State	Business	Business

Table 3: The Limits of Privatization – Trust and Selective Regulatory Capitalism

	Laissez-faire capitalism (1800s–1930s)	*Welfare capitalism (1940s–1970s)*	*Regulatory capitalism (1980s–)*	*Networked regulatory capitalism*	*Selective regulatory capitalism*
Steering	Business	State	State and agencies	State, agencies, business	State, agencies, (business)
Rowing	Business	State	Business	Business	Business
Levels of trust	N/A	Low	Medium	High	Variable

this responsibility, focusing on three elements: (1) the role of private sector expertise, (2) control over infrastructure as a means of ensuring resilience, and (3) the position of trust which they hold.

Where the first element is concerned, cybersecurity exemplifies a move to networked regulatory capitalism, in which business is not only responsible for the 'rowing' involved in regulation, but also for 'steering', by shaping policy in dialogue with the state and regulatory agencies (2017, pp. 249–51).[2] This corresponds not only to a reshaping of governance in line with the move to the regulatory State (where the State only provides the regulatory framework), but also with a changing understanding of who is best placed to engage in regulating areas of high technical complexity where the state does not hold direct control over infrastructure (Carrapico and Barrinha, 2017). This is acknowledged by the EU in the Cybersecurity Strategy, which states that since the 'large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cybersecurity is crucial' (2013, p. 6). Understood in terms of security ecology, the rationale for the inclusion of private sector actors in both policy formation as well as security provision is based on a perception of shared risk as the result of this interdependence that incentivises cooperation (Ballou *et al*., 2016; Christensen and Petersen, 2017).

Expertise, capacity and necessity, therefore, lie at the centre of the privatized provision of cybersecurity in the AFSJ, where state/policy-maker understanding of threats and capacity to respond to them is comparatively low when compared to that of the private sector, but the strategic importance of the sectors affected are comparatively high. For the State, a successful attack on CII in the privatized energy sector, for example, could result in loss of electricity for all or part of a country, with significant risks for health and safety. For the private sector operator of that energy company, there is the risk to reputation for having ineffective protection of its infrastructure. For both, there is the economic impact, both through GDP/productivity losses during the period of outage, as well as the loss of profits for the energy supplier. Therefore, cooperation in ensuring resilience facilitates preservation of reputation and guaranteeing of essential services. Mutual benefit comes in the form of the private actors having a say in the standards of resilience by which they are bound, whereas for the EU, not only does this help to improve the effectiveness of EU cybersecurity policies, but also facilitates 'Europeanization through

[2]The complete overview of the first three stages of cybersecurity policy are not discussed here, but can be found in their entirety in Carrapico and Barrinha (2017).

standardization', in which all private operators of NIS in the EU work to the same standards and practices (Cantero Gamito, 2018). This standardisation of cybersecurity approaches in the EU is one that centres on the notion of 'resilience' (Carrapico and Barrinha, 2017). This resilience is central to the role of private sector actors in developing cybersecurity policies as well as enacting them, due to their control over the ecosystem that is at the centre of the EU's cybersecurity agenda.

For Christou, resilience in cyberspace comprises complex interactions between public and private actors, as well as between law, politics and technology as part of a networked system of regulation (2015, p. 24). In this respect, in the field of cybersecurity, security governance is best characterized as 'security as resilience' (Kavalski, 2009, p. 532), in which 'security does not refer to the absence of danger but rather the ability of a system […] to reorganize to rebound from a potentially catastrophic event' (Dunn Cavelty, 2013, p. 6). The EU shares this understanding of cybersecurity as resilience, as evidenced by its 2013 Strategy, in which cyber-resilience was identified as the first strategic priority of the EU in safeguarding the online environment (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013, p. 4). The characterization of resilience as requiring the cooperation of both the public and private sector is underscored, focused both on the relationships between actors and the nature of the infrastructure.

The standards developed through public–private partnership between cybersecurity experts and national agencies, diffused through ENISA, and then operationalized by service providers in order to ensure resilience are the means by which these asymmetries in cybersecurity are combated. This entails significant relations of trust, the third element of analysis in this section. As a result of public–private partnering in cybersecurity, 'thousands of companies have entered into special trust relationships with the state' (Klimburg, 2011, p. 52). This requires the government to be able to trust the private actors facilitating its cybersecurity policies as much as it requires the private actors to trust the government (Klimburg, 2011, p. 55). Trust is essential as it allows for actors to make decisions about cooperation in situations of vulnerability or uncertainty (Larson, 1997, p. 19). It works as an effective basis for agreements or cooperation, without a continual need for oversight, verification and renegotiation, which would be the case where there is little trust, or active mistrust (Uslaner, 2018, p. 2).

In the context of cybersecurity, we can consider trust to be particularized, which Hoffman describes it as being a form of fiduciary trust not based on parties' assessment of self-interest, but on the perception of the character or values of the other party (2002). This trust is 'predicated upon a belief that others have a particular character, that they are inherently trustworthy' (Rathbun, 2009, p. 355), based in collective identity and shared values – in the context of cybersecurity, this would be a mutual trust that each party is working in the collective interest of ensuring security based on principles of Western liberal democracy, freedom of expression, guaranteeing privacy and avoiding situations of undue state control. Through the pooling of knowledge and expertise, solutions to cybersecurity problems can be reached that are generally considered neutral and apolitical (Christensen and Petersen, 2017, p. 1449), fitting effectively with evidence-based policy approaches and furthering trust between public and private sectors. The explicit and conscious inclusion of private sector actors both in policymaking as well as operationalizing cybersecurity is indicative of their status as 'in-group' members, in

which particularized trust is invested. However, in times of perceived crisis, trust has the potential to break down, as one or both parties may be perceived as acting in ways that betray that trust, or no longer share certain values upon which the trust relationship is based (Ruzicka and Keating, 2015, p. 17). The final section of this article explores what happens when a breakdown in trust (including both strategic and particularized) occurs in the field of cybersecurity, using social media platforms as a case study that may be indicative of public–private relations in the AFSJ more generally.

III. The Impact of Disinformation and Uncertainty on the Role of Cybersecurity Private Actors: From Networked to Selective Regulatory Capitalism?

As discussed above, trust is an essential characteristic of the Regulatory Capitalism framework. In the context of security, this is not only trust in the effectiveness of the actor as a policy actor, but in that actor sharing certain values or interests. Where trust fades, it is likely that we see a restructuring of the governance relationship, with the result that the 'networked' regulatory capitalism model becomes a 'selective' model, in which the level of both autonomy and policy-setting power is determined by the levels of trust in the private actor. In times of increased uncertainty and political turbulence, and particularly where the logics of privatization are being more closely scrutinized, significant failings may result in revisiting the extent and ambit of privatization of security activities.

In this respect, 2016 represents something of a political shift in the dynamics of public–private cooperation in the field of cybersecurity, centred around the apparent unwillingness and limited capacity of social media platforms to tackle the spread of disinformation using their systems. In between the election of Donald Trump, the results of the UK referendum on EU membership, and the rise of non-mainstream and 'populist' parties and politicians throughout the world, a sense of the destabilization of 'politics as usual' has impacted upon a range of policy sectors, including that of the AFSJ. In April 2016, the EU began warning of 'hybrid threats', which combined the 'unconventional' use of military, economic and technological methods of achieving state and non-state aims, which could include 'massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors' (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016, p. 2). Russia had been expanding its networks of offline *and* online disinformation since 2004, which initially focused upon the spread of disinformation within Russia in its first phase and then Russia's immediate neighbourhood in the second phase. However, as an issue on the EU's political agenda, disinformation appears largely as a response to Russia's expansion of its disinformation campaigns to the rest of Europe, as well as the US, in 2014 (Treverton *et al*., 2018, p. 69). The European Council, together with the Commission serving as a key driver of the EU's disinformation policies, indicated in the context of the Ukrainian annexation and Russia's information warfare over the issue that it:

> stressed the need to challenge Russia's ongoing disinformation campaigns and invited the High Representative, in cooperation with Member States and EU institutions, to prepare by June an action plan on strategic communication (European Council, 2015, p. 4).

The necessity of tackling disinformation, according to the Joint Framework communication that resulted, was that it constitutes a form of hybrid threat that 'aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties' (2016, p. 3). Disinformation in the context of contemporary politics, and indeed, the EU's concerns, is intended to sew division and distrust (Marwick and Lewis, 2018), undermining democratic institutions through assaults on their legitimacy (Morgan, 2018), destabilizing their politics and providing opportunities for 'anti-system' and populist actors to influence policy or even win elections (Hopkin, 2020). Examples of the EU's concerns include political disinformation regarding the actions of the EU and its institutions (High Representative of the European Union for Foreign Affairs and Security Policy and the European Commission, 2018), and the spread of anti-vaccine and now COVID-19 conspiracy theories that negatively impact efforts to contain the disease (Europol, 2020). The importance of social media in disseminating disinformation lies in its large user-base, its immediacy and reach, and the low-cost nature of information distribution (Marwick and Lewis, 2018).

While the Joint Framework was silent on the role of online intermediaries, the Commission separately expressed some concerns with the growing power of these bodies, particularly those such as Facebook, regarding their dominant market position, attitudes towards privacy, and indeed, engagement in content moderation (see European Commission, 2016). By the end of 2016, however, the EU was strongly aware of these intermediaries' role as a key dissemination point for online disinformation, which it considered as the basis of populist 'anti-politics' threatening the cohesion of the Union. In 2017, the European Parliament published a report stating that whereas the default position for online intermediaries was one of immunity from liability under the E-Commerce Directive, that immunity needed to be revisited in light of the need for 'online platforms to provide users with tools to denounce fake news in such a way that other users can be informed that the veracity of the content has been contested' (European Parliament, 2017, p. 11). Online providers have argued that they are a mere conduit for information with no general obligation to monitor the use of their systems under Article 15 of the Directive, and as such do not exercise editorial control. The significant power possessed by social media platforms, combined with an unwillingness to remove content disseminated through their systems, have led to calls to close a supposed loophole in the previously mentioned E-Commerce Directive, which is currently being assessed in the context of Commission President von der Leyen's 'Shaping Europe's Digital Future' agenda (European Commission, 2020a). Central to this assessment is whether the principles of immunity for liability need to be reformed, instead obliging social media platforms in particular to be active in the oversight of their services on the basis of an imposed 'duty of care' (Síthigh, 2020), as well as a loss of trust in the shared values of some social media platforms.

The dissemination of disinformation online is linked to the issue of network and information security, insofar as it concerns the integrity of information contained within a network system. Often NIS is thought of in terms of the external attacks on a system itself, with the emphasis of policies being on the prevention of successful attacks such as DDoS, and the resilience of these systems in the event that they are taken offline. However, less attention has been paid to the attacks on information occurring *within* those systems that do not impact upon the functioning of the system itself. By way of example,

if an external attack on a banking system in order to gain access to bank records to digitally add money to an account was successful, this would be considered in terms of NIS. However, if an authorized Facebook user spreads anti-vaccination information, this does not impact on the integrity of the communications software but has significant real-world implications for human security. As the NIS Directive states in Article 2, NIS incorporates 'any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems'. In this respect, the dissemination of disinformation through information systems such as social media can be considered as being a form of cybersecurity threat (Riikonen, 2019). Particularly given the concern that disinformation online impacts upon the good functioning of political and social structures (see for example Duffy, 2018; O'Connor and Weatherall, 2019), information manipulation of this type has been argued as being a potential attack on CII (Li *et al*., 2018). While this paper does not propose that social media platforms themselves should be considered a form of CII, an argument that goes beyond the remit of this article, it is made instead to emphasize the importance of social media platforms for the communication of ideas, information, and indeed disinformation, that has significant security implications, in fields such as immigration, the integrity of electoral politics and human health.

Social media platforms, however, do not appear to demonstrate the same level of prioritization in the combating of online disinformation using their systems. Siddiquee suggests that a combination of trust and sense of shared responsibility is fundamental in successful public–private partnerships (2011, p. 143), and there is a growing sense on the part the EU that social media platform providers do not share that sense of responsibility.[3] After the release of the High Level Group report on Fake News and Online Disinformation (2018), the Commission published a Communication stating that 'disinformation erodes trust in institutions and in digital and traditional media, and harms our democracies by hampering the ability of citizens to take informed decisions' (European Commission, 2018a, p. 1), criticising social media platforms for having 'so far failed to act proportionately, falling short of the challenge posed by disinformation and the manipulative use of platforms' infrastructures' (European Commission, 2018a, p. 2). In order to encourage these platforms to tackle the spread, the Commission published a voluntary Code of Practice agreed with Facebook, Twitter and Google, based on principles of transparency, diversity of information, credibility of information, and inclusivity (European Commission, 2018b). However, in an interim assessment made by the Commission in February 2019, it was stated that the social media platforms were falling far short of the expectations set by the Code of Practice (European Commission, 2019). These concerns were reiterated in October 2019, when the Commissioner for the Security Union, Julian King, stated that it was no longer sufficient for social media platforms to 'mark their own homework […] we're going to have to have a step-change in the amount of

[3]It is undoubtedly the case that the spread of disinformation in the context of French elections and in Germany concerning Merkel's policies on refugees have served as drivers for action in those state and reinforced the positions of the European Council and Commission on disinformation, and that there is significant divergence between Member States on the nature and seriousness of the 'disinformation problem'. However, as the main focus of this article is on the relations between policymakers at the EU level and private actors operating in the online environment, these dynamics will not be explored further here.

outside scrutiny that platforms are willing to tolerate' (Heikkilä, 2019). The Commission and High Representative of the Union for Foreign Affairs and Security made it clear that they were not satisfied with the effectiveness of the measures being taken, and the result of a study to be completed in 2020 (but has not yet been released at the time of writing) could result in 'further initiatives, including of a regulatory nature' (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2019, p. 5).

These measures suggest a changing relationship between state actors and social media platforms in this particular area of cybersecurity, based on falling levels of trust, both in regulatory effectiveness as well as shared values. Refusals of representatives of Facebook in particular to attend hearings, as well as relaxing its restrictions on paid advertising and exempting statements from politicians from its fact-checking operations (Boyle, 2019) indicate that a combination of a libertarian position on freedom of expression, combined with financial interests diverging from European security interests, no longer make it a reliable partner in tackling disinformation. At the centre of this deepening distrust is a perception amongst actors in the EU that many of the US-based social media platforms do not share the EU's values where it comes to freedom of expression. Zuckerberg has stated in European Parliament hearings that Facebook should not regulate what is true or not, representing a philosophical ideal that all political speech should be permitted with a plurality of views being represented (Lischka, 2019), indicative of an understanding of expression more in line with a US regulatory approach under the 1st Amendment to the Constitution. This approach to speech is not perceived as conforming to EU principles of expression, in which speech that is considered to be actively harmful, such as hate speech or glorification of terrorism is explicitly illegal and should be actively regulated (Ross, 2019). Whereas a more self-regulatory, 'light-touch' approach to governance with private actors engaged within a regulatory network appears coherent with the US approach, a more top-down, command-based form of regulation, in which the state and agencies take on a 'steering' position, with a legally-enforced 'rowing' position for social media providers would seem more appropriate where there are low levels of trust in that private sector actor. The perception of a lack of shared sense of norms and values, resulting in greater oversight, would represent a return to a more hierarchical form of Regulatory Capitalism, that can be directly juxtaposed with the increased role for other cybersecurity providers. In the 2019 Cybersecurity Act implemented by the EU, an expanded mandate for ENISA and combined certification and best-practice powers granted to private cybersecurity providers (Regulation 2019/881, 2019) indicate that while we are not seeing a complete reversal of the Networked form of Regulatory Capitalism in the cybersecurity field, but a more judicious, selective form of Regulatory Capitalism dependent upon levels of trust; where trust in providers to possess effective regulatory practices and shared values is high, an active steering and rowing-approach is maintained. However, where trust falters, as in the capacity and willingness of social media platforms to tackle hybrid cybersecurity threats such as disinformation, a more command based 'rowing-only' approach appears to be preferred. Those that preserve the integrity of the 'network' in cybersecurity still maintain a privileged position, whereas those seen to fail in preserving the integrity of the 'information' in cybersecurity may face increased regulatory oversight. This can further be seen in the Commission's initiatives in the field of cybersecurity pursued as a result of the increased dependency on NIS,

particularly due to changed work and social behaviours as a result of COVID-19 – whereas those private actors engaged in cybersecurity provision tools and software focused on the integrity of networks and resilience from attack are encouraged to cooperate with EU and national authorities in expanding CII protection and developing standards for the resilience of test and trace systems (Commission Recommendation 2020/518, 2020; European Commission, 2020b), social media platforms are highlighted as being a key source of insecurity, contributing to political uncertainty and instability through their role in spreading disinformation concerning COVID-19's origins, effects and the response of the EU and its Member States (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020). To put it another way, where those private actors are perceived to share a mutual interest in the resilience of networks and systems from attacks such as DDoS and unauthorized access to data, then those actors are selected to actively engage in steering and rowing cybersecurity policies. In comparison actors perceived to diverge on interests, values and norms are not trusted partners to be active shapers of policy, such as in the combating of online disinformation, but instead as less trusted entities tasked with providing oversight based on the requirements imposed by EU institutions serving to steer the ship.

Conclusion

The purpose of this article was to discuss the way populism and political uncertainty are impacting on the privatization dynamics in this policy field. Using the case study of Network and Information Security, a sub-area of Cybersecurity, the article argued that we are currently witnessing a change in trust relations as the result of perceived shortcomings in the way that private sector social-media platforms are responding to the security threats posed by disinformation being shared on their networks. As a result, the European Commission is less inclined to leave these platforms to self-regulate, with the likelihood of increased oversight and potentially legislative initiatives. In comparison, the new EU Cybersecurity Act allows for a proactive role for security-providing software companies in certification of cybersecurity products. What this demonstrates is a move toward a form of Selective Regulatory Capitalism, where the ability of the private sector to 'steer' cybersecurity governance is dependent on the level of trust in those private sector actors. Where trust is high, whether due to an understanding of mutual interests, or due to a shared sense of community and values, then private sector actors are welcomed into the policy-making sphere. Where trust is low, and the interests of those actors being in conflict with those of policymakers, or where they are perceived to not share the same ideals, governance is more likely to be hierarchical in nature. What this suggests for the AFSJ more generally is that privatization in the field of security is not necessarily a one-way trend of increased private sector involvement, but likely to be subject to variations based on the political context and sense of stability and predictability of public–private cooperation.

Acknowledgments

The authors would like to thank Aridna Ripoll Servent, as well as the two anonymous reviewers for their insightful and thoughtful comments to an earlier draft of this article.

Correspondence:
Helena Carrapico
Department of Social Sciences, Lipman Building
Northumbria University
Newcastle-upon-Tyne NE1 8ST
email: helena.farrand-carrapico@northumbria.ac.uk

References

Aarstad, Å.K. (2017) 'Maritime Security and Transformations in Global Governance'. *Crime, Law and Social Change*, Vol. 67, pp. 313–31. https://doi.org/10.1007/s10611-016-9656-0

Abrahamsen, R. and Leander, A. (2016) 'Introduction'. In Abrahamsen, R. and Leander, A. (eds) *Routledge Hanbook of Private Security Studies* (Routledge Handbook Series) (New York: Routledge), pp. 1–8.

Abrahamsen, R. and Williams, M.C. (2010) *Security Beyond the State: Private Security in International Politics* (New York: Cambridge University Press).

Ballou, T., Allen, J. and Francis, K. (2016) 'U.S. Energy Sector Cybersecurity: Hands-off Approach or Effective Partnership?' *Journal of Information Warfare*, Vol. 15, pp. 44–59.

Bossong, R. and Rhinard, M. (eds) (2016) *Theorizing Internal Security in the European Union* (Oxford: Oxford University Press).

Bossong, R. and Wagner, B. (2017) 'A Typology of Cybersecurity and Public–Private Partnerships in the Context of the EU'. *Crime, Law and Social Change*, Vol. 67, pp. 265–88. https://doi.org/10.1007/s10611-016-9653-3

Boyle, B. A. (2019) 'Opinion: Facebook Just Gave Up the Fight against Fake News' [WWW Document]. *Los Angeles Times*. Available at: «https://www.latimes.com/opinion/story/2019-10-03/facebook-enables-fake-news» (accessed 2.13.20).

Braithwaite, J. B. (2005) 'Neoliberalism or Regulatory Capitalism'. Regnet Occasional Paper No. 5.

Bronk, R. and Jacoby, W. (2020) 'The Epistemics of Populism and the Politics of Uncertainty'. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3539587

Bryden, A. and Caparini, M. (eds) (2006) *Private Actors and Security Governance* (Munich: LIT Verlag).

Bures, O. (2016) 'Ten Years of the EU's Fight against Terrorist Financing: A Critical Assessment'. In Argomaniz, J., Bures, O. and Kaunert, C. (eds) *EU Counter-Terrorism and Intelligence – A Critical Assessment* (New York: Routledge), pp. 17–42.

Bures, O. and Carrapico, H. (eds) (2017) *Security Privatization: How Non-security-related Private Businesses Shape Security Governance* (Cham: Springer).

Button, M. (2002) *Private Policing* (London: Routledge).

Cantero Gamito, M. (2018) 'Europeanization through Standardization: ICT and Telecommunications'. *Yearbook of European Law*, Vol. 37, pp. 395–423. https://doi.org/10.1093/yel/yey018

Carrapico, H. and Barrinha, A. (2017) 'The EU as a Coherent (Cyber)Security Actor?' *Journal of Common Market Studies*, Vol. 55, pp. 1254–72. https://doi.org/10.1111/jcms.12575

Carrapico, H. and Farrand, B. (2017) '"Dialogue, Partnership and Empowerment for Network and Information Security": The Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers'. *Crime, Law and Social Change*, Vol. 67, pp. 245–63.

Christensen, K.K. and Petersen, K.L. (2017) 'Public–Private Partnerships on Cyber Security: A Practice of Loyalty'. *International Affairs*, Vol. 93, pp. 1435–52. https://doi.org/10.1093/ia/iix189

Christou, G. (2015) *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (New York: AIAA).

Commission Recommendation 2020/518 (2020) 'On a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis, In Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data'.
Council of the European Union (2019) 'Future Direction of EU Internal Security – Outcome of Discussions. Presidency Report'. No. 14297/19. 22 November. Brussels.
Darling, J. (2016) 'Privatising Asylum: Neoliberalisation, Depoliticisation and the Governance of Forced Migration'. *Transactions of the Institute of British Geographers*, Vol. 41, pp. 230–43. https://doi.org/10.1111/tran.12118
Duffy, B. (2018) *The Perils of Perception: Why We're Wrong About Nearly Everything* (London: Atlantic Books).
Dunn Cavelty, M. (2013) 'A Resilient Europe for an Open, Safe and Secure Cyberspace' (No. 23). Swedish Institute of International Affairs.
European Commission (2016) 'Online Platforms and the Digital Single Market: Opportunities and Challenges for Europe' (No. COM(2016) 288).
European Commission (2018a) 'Tackling Online Disinformation: A European Approach' (No. COM(2018) 236).
European Commission (2018b) EU Code of Practice on Online Disinformation.
European Commission (2019) Statement on the Code of Practice against Disinformation: Commission Asks Online Platforms To Provide More Details on Progress Made [WWW Document]. Eur. Comm. Available at «https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_1379» (accessed 2.13.20).
European Commission (2020a). 'Shaping Europe's Digital Future'.
European Commission (2020b) 'Europe's Moment: Repair and Prepare for the Next Generation' (No. COM(2020) 456 final).
European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2016) 'Joint Framework on Countering Hybrid Threats' (No. JOIN(2016) 18).
European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2017) 'Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU'. JOIN(2017) 450 final. 13th September.
European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2019) Report on the implementation of the Action Plan Against Disinformation (No. JOIN(2019) 12).
European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2020) Communication on the Global EU response to COVID-19 (No. JOIN(2020) 11 final).
European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (No. JOIN(2013) 1). Brussels.
European Council (2015) Council Conclusions (No. EUCO 11/15, CO EUR 1, CONCL 1).
European Parliament (2017) Report on Online Platforms and the Digital Single Market (No. 2016/2276(INI)).
Europol (2020) 'Catching the Virus: Cybercrime, Disinformation and the COVID-19 Pandemic'.
Harvey, D. (2007) *A Brief History of Neoliberalism* (New York: Oxford University Press).
Heikkilä, M. (2019) 'EU Warns Big Tech Platforms To Do More against Disinformation'. *POLITICO*.
High Representative of the European Union for Foreign Affairs and Security Policy & the European Commission (2018) Action Plan against Disinformation (No. JOIN(2018) 36 final).

Hoffman, A.M. (2002) 'A Conceptualization of Trust in International Relations'. *European Journal of International Relations*, Vol. 8, pp. 375–401. https://doi.org/10.1177/1354066102008003003

Hopkin, J. (2020) *Anti-System Politics: The Crisis of Market Liberalism in Rich Democracies* (New York: Oxford University Press).

Hucklesby, A. and Lister, S. (eds) (2018) *The Private Sector and Criminal Justice* (London: Palgrave Macmillan).

Kaunert, C., Léonard, S. and MacKenzie, A. (2012) 'The Social Construction of an EU Interest in Counter-terrorism: US Influence and Internal Struggles in the Cases of PNR and SWIFT'. *European Security*, Vol. 21, pp. 474–96. https://doi.org/10.1080/09662839.2012.688812

Kavalski, E. (2009) 'Timescapes of Security: Clocks, Clouds, and the Complexity of Security Governance'. *World Futures*, Vol. 65, pp. 527–51. https://doi.org/10.1080/02604020903276834

Klimburg, A. (2011) 'Mobilising Cyber Power'. *Survival*, Vol. 53, pp. 41–60. https://doi.org/10.1080/00396338.2011.555595

Krahmann, E. (2010) *States, Citizens and the Privatisation of Security* (Cambridge: Cambridge University Press).

Kruck, A. (2014) 'Theorising the Use of Private Military and Security Companies: A Synthetic Perspective'. *Journal of International Relations and Development*, Vol. 17, pp. 112–41. https://doi.org/10.1057/jird.2013.4

Laclau, E. (2007) *On Populist Reason* (London: Verso).

Larson, D.W. (1997) *Anatomy of Mistrust: U.S.–Soviet Relations during the Cold War* (Ithaca, NY: Cornell University Press).

Leander, A. (2005) 'The Power to Construct International Security: On the Significance of Private Military Companies'. *Millennium*, Vol. 33, pp. 803–26.

Leander, A. (2010) 'The Paradoxical Impunity of Private Military Companies: Authority and the Limits to Legal Accountability'. *Security Dialogue*, Vol. 41, pp. 467–90.

Levi-Faur, D. (2005) 'The Rise of Regulatory Capitalism: The Global Diffusion of a New Order''. *Annals of the American Academy of Political and Social Science*, Vol. 598, pp. 12–32. https://doi.org/10.1177/0002716204272590

Li, T., Fei, F. and Yanqing, H. (2018) 'Governing Social Media Platforms as Critical Information Infratructures'. In *Beyond the Boundaries: Challenges for Business, Policy and Society.* Presented at the the 22nd Biennial Conference of the International Telecommunications Society, Seoul, pp. 1–21.

Lischka, J.A. (2019) 'Strategic Communication as Discursive Institutional Work: A Critical Discourse Analysis of Mark Zuckerberg's Legitimacy Talk at the European Parliament''. *International Journal of Strategic Communication*, Vol. 13, pp. 197–213. https://doi.org/10.1080/1553118X.2019.1613661

Marwick, A. and Lewis, R. (2018) *Media Manipulation and Disinformation Online* (New York: Data & Society Research Institute).

Moe, T.M. (1990) 'Political Institutions: The Neglected Side of the Story'. *Journal of Law, Economics, and Organization*, Vol. 6, pp. 213–53.

Moffitt, B. (2017) *The Global Rise of Populism: Performance, Political Style, and Representation* (Stanford: Stanford University Press).

Morgan, S. (2018) 'Fake News, Disinformation, Manipulation and Online Tactics to Undermine Democracy'. *Journal of Cyber Policy*, Vol. 3, pp. 39–43. https://doi.org/10.1080/23738871.2018.1462395

Norris, P. and Inglehart, R. (2019) *Cultural Backlash: Trump, Brexit, and Authoritarian Populism* (New York: Cambridge University Press).

O'Connor, C. and Weatherall, J.O. (2019) *The Misinformation Age: How False Beliefs Spread* (New Haven, CT: Yale University Press).
Petersen, K.L. (2008) 'Terrorism: When Risk Meets Security''. *Alternatives*, Vol. 33, pp. 173–90. https://doi.org/10.1177/030437540803300204
Rathbun, B.C. (2009) 'It Takes All Types: Social Psychology, Trust, and the International Relations Paradigm in our Minds''. *International Theory*, Vol. 1, pp. 345–80. https://doi.org/10.1017/S1752971909990121
Regulation 2019/881 (2019) On ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification.
Riikonen, A. (2019) 'Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China'. *Strategic Studies Quarterly*, Vol. 13, pp. 122–45.
Ross, A. (2019) 'Values and Issues'. In Ross, A. (ed.) *Finding Political Identities: Young People in a Changing Europe* (Palgrave Politics of Identity and Citizenship Series) (Cham: Springer), pp. 45–95.
Ruzicka, J. and Keating, V.C. (2015) 'Going Global: Trust Research and International Relations'. *Journal of Trust Research*, Vol. 5, pp. 8–26. https://doi.org/10.1080/21515581.2015.1009082
Siddiquee, N.A. (2011) 'Rhetoric and Reality of Public–Private Partnerships: Learning Points from the Australian Experience'. *Asian Journal of Political Science*, Vol. 19, pp. 129–48. https://doi.org/10.1080/02185377.2011.600163
Singer, P.W. (2007) *Corporate Warriors: The Rise of the Privatized Military Industry* (Updated edition) (Ithaca, NY: Cornell University Press).
Síthigh, D.M. (2020) 'The Road to Responsibilities: New Attitudes towards Internet Intermediaries'. *Information & Communications Technology Law*, Vol. 29, pp. 1–21. https://doi.org/10.1080/13600834.2020.1677369
Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K. and McCue, M. (2018). 'Addressing Hybrid Threats. Center for Asymmetric Threat Studies; The European Centre of Excellence for Countering Hybrid Threats'. Swedish Defence University.
Uslaner, E.M. (ed.) (2018) *The Oxford Handbook of Social and Political Trust* (New York: Oxford University Press).