European University Institute
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

WORKING PAPERS

RSCAS 2020/22
Robert Schuman Centre for Advanced Studies
Global Governance Programme-388

Who should be in charge of cyberspace? The European Union, Member States and the Constitution of Structural Power

Moritz Weiss

European University Institute

Robert Schuman Centre for Advanced Studies

Global Governance Programme

Who should be in charge of cyberspace?

The European Union, Member States and the Constitution of Structural Power

Moritz Weiss

EUI Working Paper **RSCAS** 2020/22

ISSN 1028-3625

Published in April 2020 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)
Italy

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Brigid Laffan, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and *ad hoc* initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

For more information: http://eui.eu/rscas

The Global Governance Programme

The Global Governance Programme is one of the flagship programmes of the Robert Schuman Centre. It is a community of outstanding professors and scholars that produces high quality research and engages with the world of practice through policy dialogue. Established and early-career scholars work on issues of global governance within and beyond academia, focusing on four broad and interdisciplinary areas: Global Economics, Europe in the World, Cultural Pluralism and Global Citizenship.

The Programme also aims to contribute to the fostering of present and future generations of policy and decision makers through its executive training programme: the Academy of Global Governance, where theory and 'real world' experience meet and where leading academics, top-level officials, heads of international organisations and senior executives discuss on topical issues relating to global governance.

For more information: http://globalgovernanceprogramme.eui.eu

Abstract

Cyberspace has evolved as a domain of overlapping and essentially contested authorities. This paper seeks to explore the underlying power dynamics between supranational and national actors within the European Union. I argue that, historically, the persistent securitization of cyberspace has constituted structural power positions that privilege member states and grant them the responsibility of formulating policy responses to new challenges. An empirical analysis of more than 500 speech acts collected from public discourse in Germany and the United Kingdom from 1988 to 2017 shows, however, that securitization has not freed governments from normal politics. Calls for exceptional policies have been vague. The conceptual link between securitization and structural power thus allows for a differentiated view as to who should be in charge of cyberspace. These findings contribute to a better understanding of today's cyberpolitics and the historical constitution of structural power within Europe.

Keywords

Cyberspace; authority; securitization; structural power; Germany; United Kingdom.

Introduction

The Internet is not only evolving rapidly from a technological and economic point of view that brings about manifold changes in our daily lives (Nye, 2017), it is also developing into a governance space where authorities overlap and a diverse set of actors compete for power.[1] As its pervasiveness constantly increases to enable the functioning of modern societies (Choucri, 2012: 52), corporate actors, governments and international organizations alike have been struggling over competencies within cyberspace. For instance, a Sino-Russian coalition has for years been attempting to challenge the United States and the transnational legacy institutions that govern the Internet, especially the Internet Assigned Numbers Authority (IANA) (Mueller, 2019). The coalition aims to replace them with sovereign agreements within the United Nations' International Telecommunication Union (ITU) (Flonk et al., 2018; Lindsay, 2015: 37–40). Therefore, not only are great powers contending with each other, but also transnational organizations are competing with international ones. While nation states aim to gain power by territorializing cyberspace, transnational organizations are defending it as a network of networks beyond space and time (Lambach, 2019: 2).

Contested authority claims of this nature are similarly observable within the political system of the European Union (EU). Here, a governance structure is under construction that combines interior, market and security policies (Christou, 2019: 279). For instance, supranational actors such as the European Commission (EC) and the European Parliament (EP) have struggled with EU member states (within the Council) to establish supranational legislation on network and information security (i.e., the NIS directive), which has recently been transposed into national law (European Parliament and Council, 2016). While the EC and EP conceptualize cyberspace as the backbone of economic growth and, therefore, as part of the single market, member states primarily regard it as an opportunity structure that enables diffuse adversaries to threaten them and, as such, as an issue of national security. The legislation process was a prototypical instance of how supranational, national and additionally private actors have been struggling over authority within cyberspace. Ultimately, member states prevailed. This political contest has never been solely driven by technological and functional determinants, however, but was arguably constituted by the existence of diverging beliefs and interests regarding what cyberspace ultimately *is* (Betz and Stevens, 2011; Dunn Cavelty, 2013; Manjikian, 2010).

This paper understands the competition for authority as an – *overt* and *covert* – power struggle. For example, political conflict over the NIS directive was an instance of overt competition, where governments prevailed over supranational actors that sought to gain a more influential position (Leisterer, 2016). By contrast, a structural power context constitutes the enabling and constraining positions that the competitors occupy in the first place (Lukes, 1974). It "produces the very social capacities of structural, or subject, positions in direct relation to one another, and the associated interests, that underlie and dispose action" (Barnett and Duvall, 2005: 53). In this sense, it is covert and may exist without observable conflict, whereas these structural positions, in fact, shape unequal political privileges (see also, Weiss, 2009). Against the backdrop of the vivid debate on overt power struggles (Carrapico and Barrinha, 2017; Newlove-Eriksson et al., 2018), this paper seeks, by contrast, to explore the historically contingent constitution of structural power in order to draw inferences about Europe's main actors' positions within the contemporary contests over ruling cyberspace.

The question thus arises of *how* cyberspace was historically constructed in Europe. This is both theoretically and politically relevant, as these interpretations were arguably not neutral descriptions of a given reality, but 'essentially contested concepts' (Connolly, op. 1993; Betz and Stevens, 2011; Dunn

[1] I would like to acknowledge the generous support by the Robert Schuman Centre for Advanced Studies of the European University Institute, in general, and Ulrich Krotz, in particular. In addition, this research has also benefitted from comments by Felix Biermann, Tim Heinkelmann-Wild, Zita Koehler-Baumann, Markus Jachtenfuchs, Berthold Rittberger, Antonia Schlude and Bernhard Zangl.

Cavelty, 2013). They have shaped a structure of beliefs and interests regarding who should be in charge of cyberspace (Balzacq, 2005): the governments of member states on the one hand or the EU's supranational institutions, such as the EC or the European Union Agency for Network and Information Security (ENISA), on the other.

Building on securitization scholarship, I posit that speech acts that (i) describe cyberspace as posing *existential threats to national security* and (ii) *call for exceptional policies*, constitute a disadvantageous context for supranational institutions (Buzan and Wæver, 2003; Guzzini, 1993; Hansen and Nissenbaum, 2009; Stritzel, 2016). Therefore, this paper argues that securitization suggests structural positions whereby national governments, rather than the EU's supranational institutions, *should* primarily *be* in charge of governing cyberspace and should use exceptional means to do so. In my analysis of more than 500 speech acts collected from public discourse in Germany and the United Kingdom between 1988 and 2017, I develop a *securitization ratio* as well as a *structural power ratio* and respectively identify two patterns.

First, I find evidence that the *securitization of cyberspace* increased in intensity across the period under analysis; that is to say that speech acts repeatedly conceptualized it as a domain that caused threats to and constraints on national security to emerge. The question thus arose: To what extent does the securitization of cyberspace constitute a structural power context in which the state, as a responsible actor, is free to call for exceptional policies?

Second, the paper's findings with regard to the *structural power ratio* are more ambiguous. While speech acts stressed the primary responsibility of the state to formulate an effective response, they also suggested that threats from cyberspace should be responded to through 'normal' rather than exceptional policies. In other words, the argumentative link between the securitization of cyberspace and the responsibility of the state to address these threats prevailed and shaped the actors' structural positions in the politics of cybersecurity. Nevertheless, the provision of cybersecurity has not produced a state of emergency that frees governments to move beyond standard policy instruments.

The paper seeks to contribute to recent debates on overlapping authorities in global politics and the EU's governance of cyberspace by investigating the *historical prerequisites* of today's political dispute over who should be in charge (Weiss and Jankauskas, 2019; see also, Krotz and Schild, 2013). That allows developing a conceptual bridge between securitization scholarship, on the one hand, and the analysis of structural power, on the other. This link expands scholars' attention beyond the theoretical perspective on how the EU's supranational institutions overtly challenge the power of member states (Blauberger and Weiss, 2013) toward how governments are enabled to exercise structural power over EU institutions (Hansen and Nissenbaum, 2009; Krotz and Maher, 2017; Meijer and Wyss, 2018: 380). More specifically, I will shed light on the fact that authority claims emerge from a historically contingent process that appears, at first glance, free of conflict between competing authorities. Thus, my analysis starts out from the late 1980s, when no authority conflicts in cyberspace existed, and explores whether securitization has gradually constituted today's structural positions with regard to choosing what kind of responses are needed to secure cyberspace. In a sense, the paper is able to trace the *invisible* hand of power (Lukes, 1974; Nicolaïdis et al., 2013; see also, Weiss, 2019, 2020) that, today, constrains supranational institutions' bid for reforms of authority in cyberspace.

The paper is structured as follows. First, I present who is *de facto* in charge of securing cyberspace in general and within the EU in particular. Second, I introduce the structural power perspective, link it to securitization scholarship and thus refocus theoretical interest on the constitutive question: *Who is conceptualized as being in charge of cyberspace?* Third, I present an empirical analysis that starts out from the methodological approach to data collection as well as its operationalization and then moves to the main empirical findings. Finally, the conclusion discusses the main implications for both theorizing the governance of cyberspace and engaging with the real-world politics of cybersecurity.

Who is in charge of securing cyberspace?

Cyberspace is characterized by the interaction of technological determinants with the social world. It is a material structure and, at the same time, an information environment operated and shaped by humans—in other words, it is "a 'virtual' layer of information riding on a physical layer of hardware" (Betz and Stevens, 2011: 37; see also, Mueller, 2019: 10–11). Its material side links it to territorial boundaries and thus to political authority (e.g., laws, property rights), whereas its informational dimension expands beyond territorially defined political organizations (Lambach, 2019: 3). This virtual nature dissolves the distinction between the domestic and the international spheres. Yet, this has not emerged without friction. The rise of cyberspace has prompted intelligence experts to assess cyber threats as more severe than global terrorism (Kello, 2013: 7) and global businesses to rate cyber-attacks as their most important worry (Ross, 2017). The question thus arises as to who is in charge of protecting "institutions against threats, espionage, sabotage, crime and fraud, identify theft, and other destructive e-interactions and e-transactions" (Choucri, 2012: 39). In short, who exercises authority in cyberspace?

Authority is, generally speaking, the likelihood that commands will be obeyed based on a "minimum of voluntary compliance; an interest […] in obedience" (Weber, 1978: 212). More specifically, I focus on the constitution of *political* authority, that is the "authority to make decisions […] for a certain collective" (Zürn, 2018: 51) in territorially or functionally differentiated spaces. This implies that those in charge may impose their will on others. Authority shapes a structure of rulers and ruled within a given domain, in which the former predominantly make the decisions on, for instance, how the latter are to be provided with security. However, the political authority spheres over cyberspace are constantly evolving and inherently complex (Boeke, 2018: 3; Flonk et al., 2018). The boundaries of cyberspace seem far from self-evident. Unlike territory or even functionally differentiated domains, such as the economy, cyberspace is fuzzy and so is the exercise of authority over it (Finnemore and Hollis, 2016; Weiss and Biermann, 2019).

Given this essentially contested nature, formalized power struggles, such as legislating cybersecurity instruments, are not the only matters of relevance (Carrapico and Barrinha, 2017; Christou, 2019), one also needs to explore the so-called *invisible* hand of power (Moe, 2019). The premise is that the historically constituted political context shapes structural positions that privilege some actors' exercise of authority (Guzzini, 1993), while designating other actors to obey and follow the set rules. Before I theorize this constitution of structural power positions, however, I need to introduce the most important stakeholders who *are* currently in charge of protecting cyberspace. Although the state, as the manager of political authority (Genschel and Zangl, 2014), is increasingly committed to making decisions on cybersecurity and has recently enhanced its capacities to do so (Weiss and Jankauskas, 2019), the actor constellation within cyberspace is populated by two further powerful groups(Weiss and Biermann, 2019).

Private actors in general and corporate firms in particular are the protagonists in constructing, operating and partly protecting cyberspace (Choucri, 2012: 40; Healey, 2013; Newlove-Eriksson et al., 2018). For instance, the private sector controls about 90 per cent of the critical infrastructure in the United States (US) (Singer and Friedman, 2014: 15). Transnational organizations likewise have a significant say in cyberspace. In contrast to postal or telecommunications systems, which are predominantly addressed within the ITU, cyberspace is not organized around one specialized (inter-state) organization of the United Nations. Instead, transnational organizations exercise authority with respect to specific functions (Glen, 2014). For instance, the Internet Assigned Numbers Authority (IANA) regulates domain names, IP addressing, and other Internet protocol resources. At the same time, it operates as part of the Internet Corporation for Assigned Names and Numbers (ICANN), which has evolved as an independent non-profit organization that has transitioned its functions to the global multi-stakeholder community.

Within the EU, similarly, supranational actors collaborate with member states' governments to govern cyberspace. The European Parliament and the Council adopted the first supranational legislation

on Network and Information Security (NIS) in 2016 (European Parliament and Council, 2016). Yet, the political process of setting new rules revealed that member states were undoubtedly in the driver's seat with respect to how to provide cybersecurity in Europe. The NIS Directive aims to establish similar standards and policies across the EU and thus to – at least, partly – harmonize divergent approaches to cybersecurity (Boeke, 2018). While it strengthens the advisory role of ENISA, however, it is far from genuinely empowering supranational institutions in this domain. ENISA's budget is only about 11 million Euros per annum, and legislation is primarily about better coordination between *national* authorities. In other words, the supranational agency has not acquired the authority to make decisions; ENISA is merely entitled to *consult* with national authorities on how to converge policies. The rules have thus moved a considerable distance away from the EC's initial proposals published in 2013, which were part of its cybersecurity strategy for the EU (Leisterer, 2016). Member states prevailed in this overt power struggle. As a result, Europe's supranational authority is more than modest in cyberspace (Carrapico and Barrinha, 2017: 1267; Christou, 2019: 285).

In sum, there are overlapping spheres of authority in cyberspace and some uncertainty among various actors about who is in charge. While private or semi-private actors beyond national jurisdictions have gained power there, national governments have persistently enhanced their capacities and imposed new regulations to re-establish their authoritative position (Boeke, 2018; Healey, 2013). "States assert their authority over cyberspace by translating familiar territorial logics to this 'undiscovered country'" (Lambach, 2019: 2). By contrast, classical international organizations – whether the ITU or the EU – have hardly evolved as the vanguard of governing bodies in cyberspace. The question thus arises of how states' structural privileges were constituted in the first place?

Structural power, securitization and who should be in charge of securing cyberspace?

Power relationships are at work when A causes B to do, prefer, or believe something that B otherwise would not (Dahl, 1957; Lukes, 1974). Beyond this general notion, "power is a shaper of behavior and outcomes in ways that run much deeper than the study of visible political struggles can reveal" (Moe, 2019: 5; see also, Weiss, 2009). This characterizes political life as such, but it becomes even more prevalent in constellations where neither the boundaries of the domain nor the authority-holders are firmly established (Weiss and Dalferth, 2009).

Against this backdrop, I seek to better understand the historically contingent constitution of the political context in which struggles over authority in cyberspace have recently unfolded in Europe. I therefore suggest that A is not necessarily an actor, but can also be conceptualized as a structure that systematically creates patterns of incentives and constraints. For instance, the structure of capital–labor relations constitutes positions with unequal opportunities, privileges and capacities (Gill and Law, 1989).

Such a notion of structural power refers to the indirect institutional, unintended and impersonal creation of effects by A that cause to B to act in a particular way (Guzzini, 1993: 451–467). Power is at play even when there is no observable conflict. The specific strength of structural power varies from influencing incentives and opportunities to shaping the interests or even identities of other actors. Most significantly, these power relationships shape structural positions that "allocate differential capacities, and typically differential advantages" (Barnett and Duvall, 2005: 53); in other words, the structural power context. When, for instance, national security is at stake, governmental executives rather than parliaments or international organizations have advantages in addressing these policy challenges. Yet, this is not simply necessitated by functional needs, but results from historical trajectories. The workings of structural power can be illustrated by another example from European integration.

Today, defense procurement within the EU is increasingly evolving as an instance of public procurement in accordance with the principles of the single market (Weiss, 2014). However, arms acquisition has historically been a prerogative of sovereign states, which were free to set the rules within

this domain according to their own beliefs and interests. The structural positions were clear. Governments were the rulers; the European Commission was excluded. Since there was no observable conflict between governments and the EU's supranational institutions, this political context was taken for granted and could thus be regarded as free from power considerations. Yet was it? When the European Court of Justice (ECJ) accidentally took up defense procurement in a completely detached judgment on value-added tax reductions, it suggested a very narrow interpretation of the exemption clause in cases of national security. This was a straightforward challenge to member states' authority inasmuch as it called upon and empowered the European Commission to act as the guardian of the treaties (Blauberger and Weiss, 2013).

However, in sharp contrast to the combined wisdom of political science theorizing, the European Commission did *not* take advantage of this opportunity. Instead, it sought to prevent the Court from ruling with respect to this sovereign prerogative. It argued that the sued member state had never raised the exemption clause in the pre-litigation phase and thus the Court was not entitled to interpret it (Case 414/97, No. 18). In other words, the structural positions in the domain of defense procurement were taken for granted to such an extent that the disadvantaged European Commission even defended the privileges of its competitor, the member states. Up until this point, there was no observable power struggle between national and supranational actors; yet, power was permanently at play and invisibly shaped the positions of who *should be* in charge (Weiss and Blauberger, 2016).

Three inferences can be drawn from this brief illustration. First, the fact that overt conflict is hardly observable does not imply that power is not at play. While the European Commission had a self-interest in strengthening its competences, it anticipated member states' responses and thus abstained from making use of judicial support. Second, the boundaries of a domain – be it cyberspace or defense procurement – are not self-evident. As long as political actors treated defense procurement as an instance of national security, the sovereign prerogative was not challenged and thus reproduced itself. When the European Commission redefined the boundaries of defense procurement in the course of the late 2000s, the same policy field increasingly became an instance of economic governance and unlawful state aid. Third, the reference to national security is not a neutral description of a given reality, but entails structural positions of member states on the one hand, and of the supranational institutions on the other. If a functional task – arms acquisition or protecting cyberspace – is conceptualized as primarily economic and thus a market issue, the EU's supranational institutions have a say. By contrast, governments provide national security, and thus the EU is excluded.

Given the relevance of structural power to studying overlapping spheres of authority, as illustrated in this instance the question arises of how it is constituted in general, and how it has evolved for the task of securing cyberspace in particular. I build on the premise that

> "[r]outine actions can constitute rituals of power that suggest the realm of the possible. They construct (and deconstruct) the horizon of the thinkable and feasible […]. Social interactions mobilize rules for agenda setting that privilege specific agents, that is, the agent's actual power in a bargain is fostered by the system's governance" (Guzzini, 1993: 474).

When I apply this notion of structural power to governing cyberspace in Europe, the working presumption would be: Member states' governments might have prevailed in the bargaining over legislating for the protection of cyberspace by virtue of historically constituted governance structures and routinized interactions that defined what kind of new rules were conceivable. For instance, a pattern of routinized interactions in the governance of cyberspace was that the more challenges were conceptualized as a threat to national security, the more states established hierarchical control. By contrast, the more governments conceptualized challenges as societal vulnerabilities or even positive opportunities, the less hierarchical control and the more indirect modes of governance were employed (Weiss and Jankauskas, 2019). I therefore theorize that the routinized conceptualization of cyberspace has historically constituted the structural power context (see also, Mueller, 2019: 4). References to security threats constrain supranational EU institutions and put them at a disadvantage by privileging individual member states as adequate respondents.

Hence, I build on securitization scholarship to approach the historically contingent constitution of Europe's structural power context in cyberspace. Securitization is understood as a successful speech act "through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object [i.e., the state], and to enable a call for urgent and exceptional measures to deal with the threat" (Buzan and Wæver, 2003: 491). Survival and political urgency are consequently at stake. This state of emergency allows normal politics, such as legislation and regulation according to the formal rules of the game, to be bracketed. Instead, governments build up emergency capacities and are free to choose policies that they deem adequate without creating political resistance. This puts them in a very powerful position (Sjöstedt, 2012: 145–146; Stritzel, 2016: 360). Securitization, furthermore, not only empowers state executives, it weakens authority claims from other actors, such as private companies or international organizations. This applies, in particular, to instances that are characterized by overlapping spheres of authority (Weiss and Dalferth, 2009). By contrast, de-securitization, that is, describing a challenge as an economic problem, empowers those actors that are in charge of market regulation, such as, for instance, the European Commission.

As a result, I am able to spell out a baseline model that allows the constitution of Europe's structural power context in cyberspace to be studied. My starting point is a situation in which public discourse securitizes a specific policy field (step 1). This securitization constitutes structural power positions within this policy field (step 2). Consequently, power relations constitute actors other than sovereign governments in a disadvantaged position with respect to making authority claims for this policy field (step 3). Figure 1 provides an overview of the baseline model that will be applied to the empirical analysis below.

Figure 1: The constitution of a structural power context in cyberspace

Step 1	→	**Step 2**	→	**Step 3**
Securitization of a specific policy field in public discourse.		Structural power positions are constituted.		Power relations constitute non-state actors in a disadvantaged position with regard to the exercise of political authority over a specific policy field.
Securitization of cyberspace in public discourse.		*Member states should be in charge of cybersecurity.*		*Power relations constitute the EU in a disadvantaged position with regard to the exercise of political authority over cyberspace.*

Speaking about cyberspace in Germany and the UK (1988–2017)

I have argued above that the securitization of an issue-area shapes its political authority constellation and thus policy-making, or the allocation of values by collectively binding decisions. To identify whether cyberspace has historically been securitized, I conduct a qualitative content analysis or, more specifically, a speech act analysis (see also, Weiss and Weiss, 2005). The data necessary to carry out such a speech act analysis was collected from newspapers and parliamentary sources. In the following I will outline the core decisions I took during data collection as well as analysis and present the findings of the analysis.

Data collection

The selection of specific EU member states

In order to assess to what extent the discourse on cyberspace has been securitized in EU member states, I based my speech act analysis on newspaper articles and parliamentary minutes from two European member states, Germany and the United Kingdom (UK). This supplements existing studies that have focused on securitization at the EU level (e.g. Christou, 2019). The two countries are adequate cases to analyze the securitization of cyberspace discourse in the EU because they can be assumed to represent typical instances of the two extremes of a continuum. The UK's approach has arguably been most similar to that of the United States inasmuch as it has stressed the national security nature of cyberspace (Sexton, 2016). By contrast, Germany has put the emphasis more strongly on the protection of privacy in cyberspace and thus advocated for less state interference for the purpose of national security (Schallbruch and Skierka, 2018). While the ideal would be to consider all member states, the selection of the UK and Germany at least protects against creating an obvious bias for or against securitization from the outset.

The selection of specific speech acts

The next step of the analysis needs to spell out the criteria governing which specific speech acts were selected. The premise is that in "most cases a security scholar will […] be confronted with a process of articulations creating sequentially a threat text which turns sequentially into a securitization" (Stritzel, 2016: 377). Hence the temporal challenge was to provide for the possibility that cyberspace might have been already securitized at the outset, whenever it was talked about it. Without considering the greater salience of cybersecurity in recent years, a random selection would have most likely led to a dramatic increase in securitization from 1988 to 2017. Rather than collecting cyber-related speech acts in general, I thus decided for the first part of my timeframe of analysis to focus only on documents that addressed a specific cyber incident.[2] This selection procedure from the outset strengthened the probability that securitization began relatively early and was constant over time. In other words, I biased my selection towards continuity so that a potential finding of change would provide more credibility and thus argumentative leverage.

The speech act analysis is based on two types of source. First, I collected newspaper articles, since the media arguably plays "an instrumental role in securitization, it constructs an 'us' and 'them', tells us what the conflict is about and what can be done to stop it" (Watson, 2009: 21). The media serves three purposes in the securitization process: It makes securitizing claims of its own; it communicates securitizing claims made by other actors; and it exposes securitizing claims to contesting views (Weiss and Weiss, 2005). By using the cyber incident names as search terms, I collected 252 newspaper articles from British and German newspapers published between 1988 and 2017 through the online search engine Lexis Nexis and the archives of relevant newspapers. To limit the number of articles to be

[2] Here, I have built on the cyber historiography of Healey (2013), who lists ten crucial cyber incidents that took place between 1986 and 2010.

analyzed, for every cyber incident I selected ten articles only. The selection criterion was to establish variation across countries and newspaper quality. Hence, I chose 104 newspaper articles published in a variety of journals in Germany (e.g., *Fokus*, *Der Spiegel*, *Süddeutsche Zeitung*, *Frankfurter Allgemeine Zeitung*, *Die Zeit*, *Die Welt*) and in the UK (e.g., *The Guardian*, *The Daily Telegraph*).

The second type of source was parliamentary debates in Germany and the UK between 1988 and 2017. While the media discourse contributes to constituting a structural power context, political actors remain vested with a particular authority to make securitizing moves. Thus, I accessed parliamentary outputs (esp. parliamentary questions, legislation and debates) and searched the online archives of the German and British Parliaments using the terms *cyber*, *virus*, *computer* and *hacker*. Again, I selected 101 of these 203 documents with the objective of having, at least one parliamentary source from each of the two member states for every year of the analysis. In total, I analyzed 68 parliamentary documents from Germany and 33 from the UK (1988–2017).

Operationalization of securitization

Once a document was selected for analysis, I identified single speech acts within it. A particular document might contain several speech acts and one speech act might comprise more than one sentence. A speech act, for my purposes, was an utterance that addressed the topic *computer* or the topic *cyberspace*. Securitization referred to the process whereby an issue became a security issue, not necessarily because a real existential threat existed but because the issue was presented as a threat of that kind (Sjöstedt, 2012; Watson, 2009: 41).

More specifically, I suggested that securitizing cyberspace involved the coding of speech acts by two indicators. First, speakers either perceive cyberspace to be primarily a security domain – or they do not. Second, speakers focus on the (negative) security-related constraints of cyberspace that affect societies – or they do not. For each of these two categories I developed a *securitization ratio* that assessed whether, in any given year between 1988 and 2017, speech acts securitized cyberspace relative to the total number of speech acts or did the opposite. The main rationale behind developing a ratio rather than measuring the frequency of securitizing speech acts was to create a more differentiated picture of the public discourse on cyberspace. I not only considered securitization but also related it to non-securitization.

$$\textit{Securitization ratio} = \frac{\text{Number of securitizing speech acts} - \text{Number of non-securitizing speech acts}}{\text{Total number of speech acts}}$$

The *securitization ratio* consequently varies between 1 and -1. If the *securitization ratio* lies above 0 in a given year, I estimate the discourse to be securitized in that year. If the *securitization ratio* lies below 0, I estimate the discourse not to be securitized in that year. I assume that the discourse is fully securitized in a given year, if the *securitization ratio* lies above 0 for both categories.[3]

Operationalization of the structural power context

The paper's objective is not only to assess whether cyberspace is securitized, but also whether these speech acts constitute the state in an advantageous structural position that frees it from the rules of normal politics. Therefore, I developed another *ratio* to assess how the structural power context is constituted in the discourse on cyberspace. Again, two indicators help us to derive these positions from

[3] Speech acts that do not refer to the respective category at all are not taken into consideration.

speech acts. First, I explore whether speakers refer to the state, rather than private actors or international organizations, as the actor capable of addressing challenges in cyberspace. Second, I investigate whether speakers stress the exceptional nature of the challenge, making it one that requires the use of forceful instruments, namely, capacity-building in the realms of the military, intelligence and law enforcement. In such a situation, normal policies, such as legislation and regulation, appear inadequate to deal with the state of emergency.

In parallel to the *securitization ratio*, I developed a *structural power ratio* and assessed whether, in every given year between 1988 and 2017, the collected speech acts constituted the state as the responsible actor that was free to choose among policy options. With respect to the first indicator, the perception of who was the adequate problem-solving actor, the *structural power ratio* relates the overall number of speech acts that prescribe the state to the overall number of speech acts that prescribe private actors or international organizations as being the primary problem-solving actors. It then divides the result by the overall number of speech acts that address the question of who is in charge of solving cyber-related issues. With respect to the second indicator, the *structural power ratio* relates the overall number of speech acts that recommend the build-up of extraordinary (e.g., military) capacities to the overall number of speech acts that prescribe normal policies (e.g., regulation, coordination) and divides the result by the overall number of speech acts that make explicit policy recommendations.

$$\textit{Structural power ratio} = \frac{\text{Number of speech acts constituting the state as responsible actor} - \text{Number of speech acts that do not constitute the state as responsible actor}}{\text{Total number of speech acts}}$$

The *structural power ratio* consequently varies between 1 and -1. If the *structural power ratio* is above 0 in a given year, I estimate the discourse constitutes the state as most powerful actor in that year. If the *structural power ratio* lies below 0, I assume that the discourse does not constitute the state as the most powerful actor in that year. I assume that the discourse fully constitutes the state as the responsible and free actor in a given year, if the *structural power ratio* lies above 0 for both categories.[4]

Data analysis

From securitization toward a structural power context?

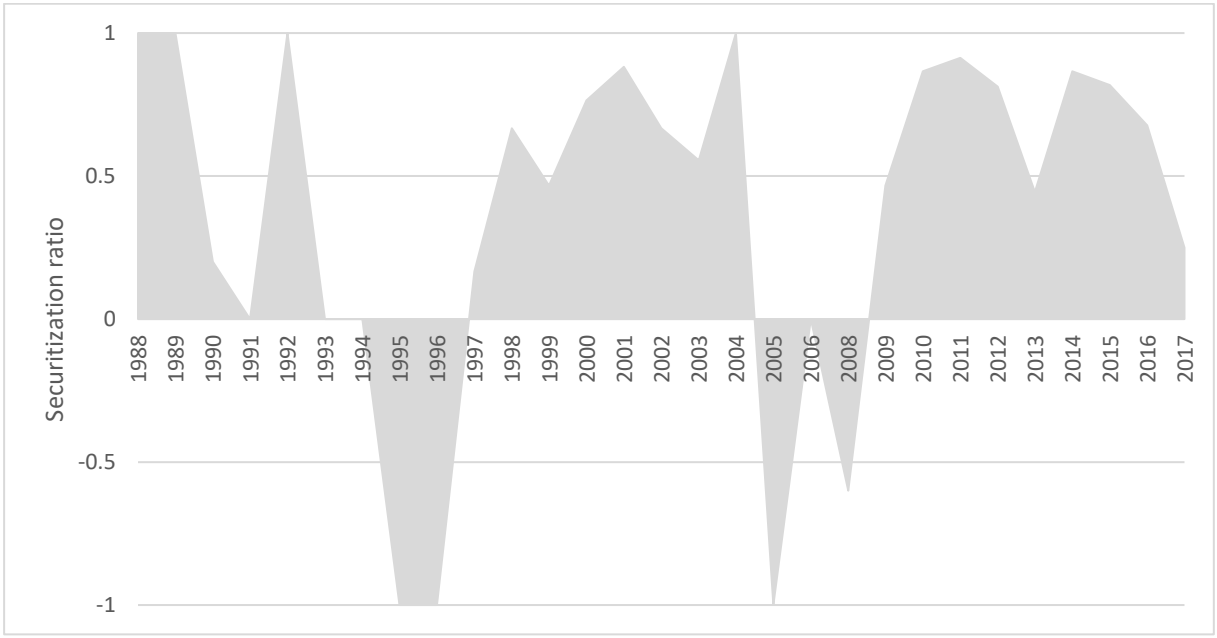
The findings of the empirical analysis suggest that discourses in Germany and the UK have consistently securitized cyberspace, at least since the end of the 2000s. This securitization has constituted structural power positions that favor member states over supranational institutions. Yet, while speakers have indeed identified the state as the key actor in charge of cyberspace and thus implicitly excluded the EU (or private actors), they primarily propose 'normal' policies rather than that governments should move towards 'exceptional' policies.[5]

[4] Speech acts that do not refer to the respective category at all are not taken into consideration.

[5] It is important to note that the findings will be presented from a pan-European perspective rather than establishing variation between the UK and Germany. This is based on the sampling and selection of these two member states because they are arguably located at the poles of a scale running from the most- to the least-likely candidate for the securitization of cyberspace.

Securitization: Is cyberspace a threatening security domain? According to my analysis, speech acts on cyberspace have securitized this domain since the end of the 2000s, as the *securitization ratio* consistently lies above 0. Cyberspace is regularly portrayed as a domain that gives rise to threats to both Germany's and the UK's national security. Data show that speakers generally perceived the nature of cyberspace as such (Figure 2), as well as the nature of constraints (Figure 3), as being predominantly related to national security during this period. In this instance, I speak of full securitization.

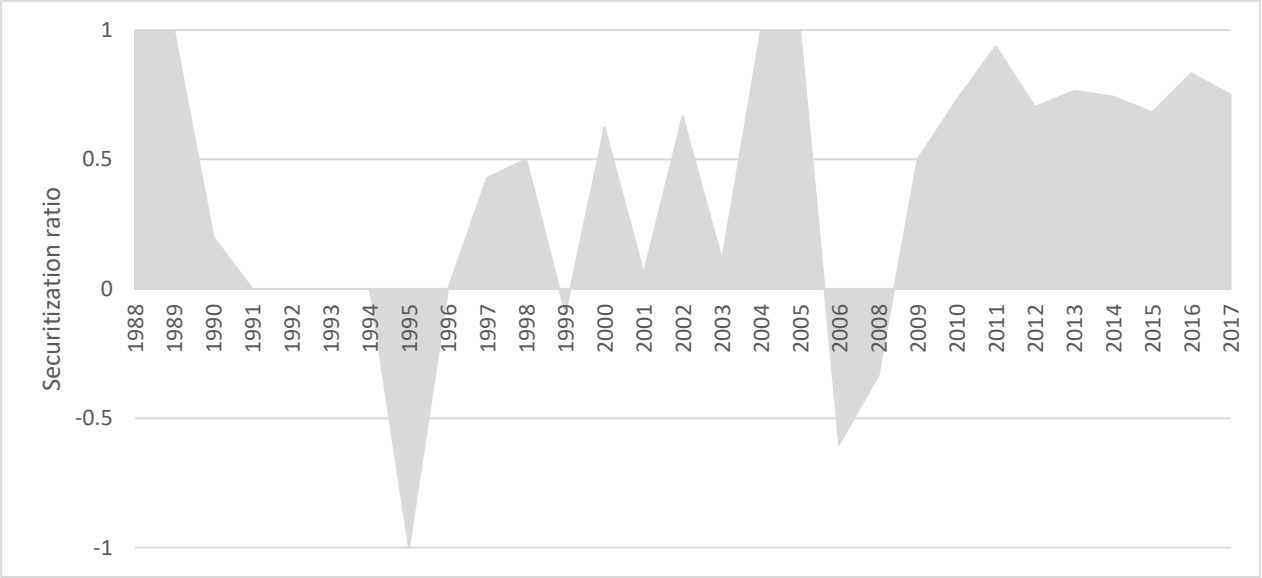
Figure 2: Securitization ratio regarding the perceived nature of cyberspace, 1988-2017



Note: N = 453. Positive values indicate that cyberspace is predominantly perceived to be security-related, thus indicating securitization. Negative values indicate that cyberspace is predominantly perceived to be non-security-related (i.e., economy- or democracy-related), thus indicating non-securitization. A zero value indicates either that the discourse is perfectly balanced between securitization and non-securitization or that there is no speech act at all referring to the nature of cyberspace in that particular year (this applies to the years 1991, 1993 and 1994).

The findings prior to 2009 are more nuanced. In some years, speech acts securitized cyberspace (e.g., 1988–1990), in others they did not (e.g., 1995, 2008). There were also years in which the discourse was fairly evenly balanced between securitizing and non-securitizing claims (e.g., 2006). Given the purposefully chosen bias in favor of continuity, resulting from the selection of cyber incidents in the first period of analysis, the findings suggest that the securitization of cyberspace is a relatively permanent phenomenon with a trend towards growth. This becomes even clearer when the second indicator is considered (Figure 3).

Figure 3: Securitization ratio regarding the nature of cyberspace constraints, 1988–2017

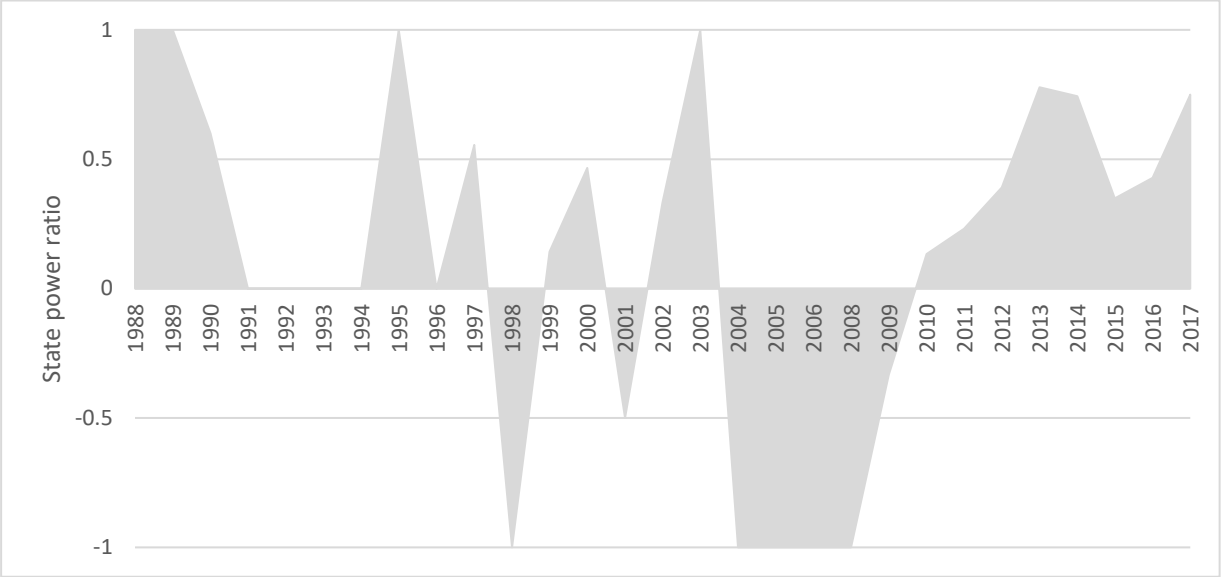


Note: N = 388. Positive values indicate that the constraints are predominantly perceived to be security-related, thus indicating securitization. Negative values indicate that constraints are predominantly perceived to be non-security-related (i.e., related to the economy or democracy), thus indicating non-securitization. A null value indicates either that the discourse was perfectly balanced between securitization and non-securitization or that there was no speech act at all referring to cyberspace constraints in that given year (as was the case for the years 1991, 1992, 1993, 1994 and 1996).

In a similar vein, when the focus of the analysis shifts toward specifying the constraints unfolding from cyberspace, national security is frequently portrayed to be at stake and, therefore, securitization is also found to have been prevalent. The two indicators for the *securitizing ratio* do not always go hand in hand, however, prior to 2009. For example, the nature of cyberspace is consistently portrayed as being security-related between 1997 and 2004, but the perceived constraints tend to fluctuate between securitization and non-securitization during the same period. Nonetheless, to sum up, both the overall results and the temporal trend point in a uniform direction: permanent and generally increasing securitization of cyberspace.

Structural power and who should be in charge of securing Europe's cyberspace? While my analysis has so far revealed that speech acts in the UK and Germany have securitized cyberspace as from 2009 at the latest, the constitution of the structural power context is more ambiguous. On the one hand, speech act analysis shows that since 2010 speakers have consistently attributed the responsibility for solving cyberspace challenges to the state (Figure 4). The government is in charge to provide security in cyberspace. In the two preceding decades, however, the findings are less clear-cut. Sometimes the problem-solving responsibility was predominantly attributed to the state (e.g., 1988–1990); and sometimes more often to international organizations or private actors (e.g., 2004–2009).

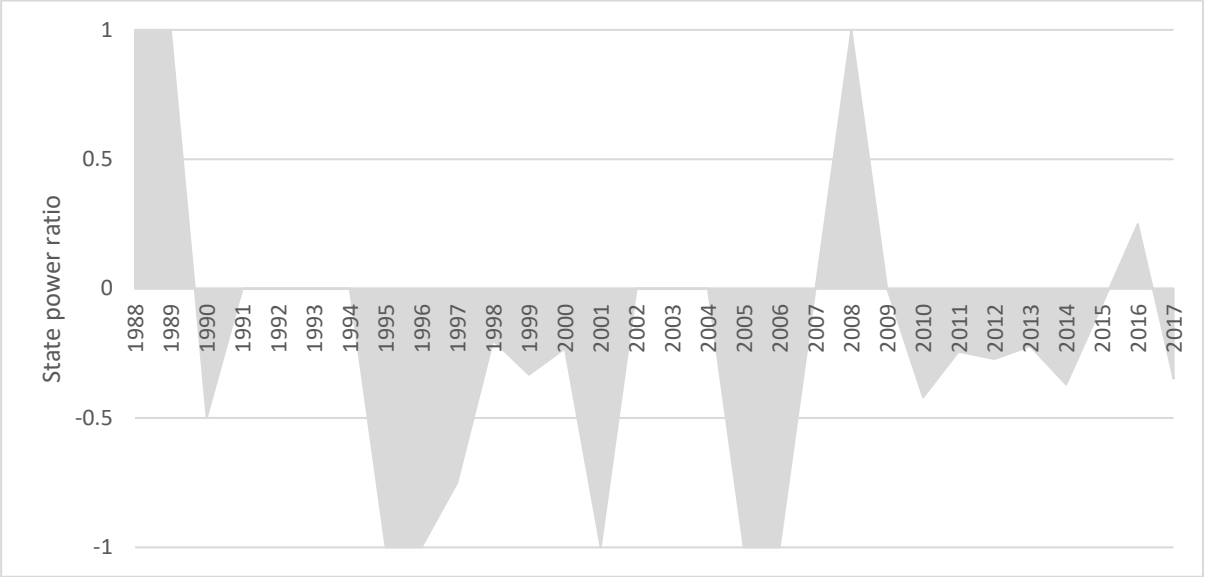
Figure 4: Structural power ratio with regard to the state's responsibility for responding to the negative repercussions of cyberspace, 1988–2017



Note: N = 309. Positive values indicate that the perception of the state as problem-solving actor prevailed. Negative values indicate that the perception of private actors and international organizations as problem-solving actors prevailed. A zero value indicates either that the discourse was perfectly balanced between constituting and not constituting the state as the responsible actor or that there were no speech acts referring to cyberspace constraints in that year (the latter applies to the years 1991, 1992, 1993 and 1994).

On the other hand, my analysis shows that the securitization of cyberspace and the increasing emphasis on the state as the actor responsible for addressing this challenge does not establish a state of emergency and, consequently, does not move the adequate policy responses outside 'normal' politics. Instead, the security-related challenges from cyberspace are to be tackled by standard policy instruments. Investigating policy recommendations made by speakers (Figure 5), I find that the build-up of military or intelligence resources is not the predominant policy prescription. Instead, cyberspace has to be secured by information-sharing, coordination and, in particular, regulation. These policy instruments prevailed among speakers except for short periods (1988–1989, 2008 and 2016).

Figure 5: Structural power ratio with respect to adequate policy responses to cyberspace constraints, 1988–2017



Note: N = 309. Positive values indicate that the demand for 'exceptional' measures (i.e., capacity-building) prevailed. Conversely, negative values indicate that the demand for 'normal' policies (i.e., information provision, regulation and coordination) prevailed. A zero value indicates either that the discourse was perfectly balanced or that there was no speech act prescribing policy responses in that year (as was the case for the years 1991 and 1994).

In sum, the findings of my analysis suggest that public discourse on cyberspace – in the form of a myriad of speech acts – was securitized. When talking about cyberspace, speakers predominantly stressed its security implications. Diffuse existential threats to the state were repeatedly referred to. However, the discourse did not consistently constitute the state as the predominant power with freedom to do whatever it deemed necessary. While speakers stressed the competence and authority of state institutions to develop effective counter-policies and referred to international organizations, such as the EU, only sporadically, the suggested adequate responses hardly moved beyond 'normal politics'. The state is responsible for securing cyberspace – yes; the state may move its policies beyond the confines of the rule of law and normal politics – no (Table 1).

Table 1: The main findings of the analysis

Dimension	**Indicators**	**Empirical findings**
Securitization	*Focus on cyberspace as security issue*	Yes
	Focus on security constraints from cyberspace	Yes
Constitution of the structural power context	*Focus on the state as central actor*	Yes
	Focus on 'exceptional' policies as response to cyberspace challenges	No

Conclusion

Cyberspace transcends territorial boundaries. It is populated by a variety of actors from diverse backgrounds and with divergent interests. Who should be in charge of it? Private actors, nation states, or international organizations? While the EU has recently legislated on network and information security, member states have prevailed insofar as they have set these rules according to their national interests. ENISA has not evolved as the new powerhouse. Today, national rather than European authorities are in charge of securing cyberspace. Since this was far from the only possible outcome (Leisterer, 2016), this paper has explored the historical constitution of who *should be* in charge of cyberspace in Europe.

I have argued that speech acts that (i) perceive cyberspace as a domain that poses *existential threats to security* and thus (ii) call for *exceptional policies* to counter those threats, constitute a disadvantageous context for supranational institutions. Instead they privilege sovereign governments. In other words, I have established a conceptual bridge between securitization scholarship, on the one hand, and structural power analysis, on the other. The paper has consequently developed both a *securitization* and a *structural power ratio* and applied them to the empirical evidence of more than 500 speech acts that were recorded in the UK and Germany between 1988 and 2017. The patterns identified are mixed. While cyberspace has historically been securitized, not only in the recent past, and this has clearly positioned national governments as being in charge of policy responses, the call for exceptional policies has been rather weak. Instead, the speech acts have overwhelmingly advocated for normal policies, such as regulations, information-sharing and improved coordination.

These findings contribute to debates on both the governance of cyberspace in Europe (e.g. Carrapico and Barrinha, 2017; Christou, 2019; Hansen and Nissenbaum, 2009) and the constitution of structural power more broadly (Barnett and Duvall, 2005; Guzzini, 1993; Weiss and Weiss, 2005). First, the paper has expanded the applicability of securitization approaches to the study of European integration as it has modified these theoretical tools and applied them beyond the EU's governance of migration and terrorism (Huysmans, 2002; Watson, 2009). Given the ambivalence of overlapping authorities in cyberspace (Dunn Cavelty, 2013; Flonk et al., 2018), it is of the utmost importance to understand the underlying normative logics of today's politics of cybersecurity.

Second, the historical prerequisites for – national or supranational – governance within this policy field in Europe have not yet entered the research arena. Despite its importance to Europeans' daily lives, the EU's recent bid for authority in the legislation process surrounding the NIS directive has largely gone unnoticed. The paper reveals the historical prerequisites for overt conflict by investigating the covert securitization of cyberspace and sheds light on the power positions of both supranational and national legislators. While the paper does not explain the political outcome itself, it provides a better understanding of the decision-making context and how it enabled the outcome (see also, Krotz, 2007; Meijer and Wyss, 2018).

Finally, the paper advances securitization scholarship by combining it with structural power analysis (see also, Nicolaïdis et al., 2013). This not only specifies the link between speech acts and their power implications, it also allows for a differentiated view. While securitization clearly empowers national governments to be in charge of a domain, it does not automatically free them from the constraints of normal politics. The state of emergency does not automatically follow. This allows for future theory-building on the conditions of constrained vs. full securitization and the normative implications that will be involved.

References

Balzacq T (2005) The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations* 11(2): 171–201.

Barnett MN and Duvall R (2005) Power in International Politics. *International Organization* 59(1): 39–75.

Betz DJ and Stevens T (2011) *Cyberspace and the state: Toward a strategy for cyber-power*. Abingdon: Routledge.

Blauberger M and Weiss M (2013) 'If you can't beat me, join me!': How the Commission pushed and pulled member states into legislating defence procurement. *Journal of European Public Policy* 20(8): 1120–1138.

Boeke S (2018) National cyber crisis management: Different European approaches. *Governance* 31(3): 449–464.

Buzan B and Wæver O (2003) *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press.

Carrapico H and Barrinha A (2017) The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies* 55(6): 1254–1272.

Choucri N (2012) *Cyberpolitics in International Relations*. Massachusetts Institute of Technology: The MIT Press.

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

Connolly WE (op. 1993) *The terms of political discourse*. Princeton (N.J.): Princeton University Press.

Dahl RA (1957) The Concept of Power. *Systems Research Behavioral Science* 2(3): 201–215.

Dunn Cavelty M (2013) From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review* 15(1): 105–122.

European Parliament and Council (2016) *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: NIS Directive*, Brussels: July 6, 2016.

Finnemore M and Hollis DB (2016) Constructing Norms for Global Cybersecurity. *American Journal of International Law* 110(3): 425–479.

Flonk D, Jachtenfuchs M and Obendiek A (2018) *Authority conflicts in internet governance: From free to sovereign internet? Paper presented at ECPR General Conference*, Hamburg.

Genschel P and Zangl B (2014) State Transformations in OECD Countries. *Annual Review of Political Science* 17(1): 337–354.

Gill SR and Law D (1989) Global Hegemony and the Structural Power of Capital. *International Studies Quarterly* 33(4): 475–499.

Glen CM (2014) Internet Governance: Territorializing Cyberspace? *Politics & Policy* 42(5): 635–657.

Guzzini S (1993) Structural power: The limits of neorealist power analysis. *International Organization* 47(3): 443–478.

Hansen L and Nissenbaum H (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53(4): 1155–1175.

Healey J (2013) *A Fierce domain: Conflict in cyberspace, 1986 to 2012*. Washington, D.C.: Cyber Conflict Studies Association.

Huysmans J (2002) The European Union and the Securitization of Migration. *JCMS: Journal of Common Market Studies* 38(5): 751–777.

Kello L (2013) The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security* 38(2): 7–40.

Krotz U (2007) Parapublic Underpinnings of International Relations: The Franco-German Construction of Europeanization of a Particular Kind. *European Journal of International Relations* 13(3): 385–417.

Krotz U and Maher R (2017) Europe in an age of transition. *Global Affairs* 3(3): 193–210.

Krotz U and Schild J (2013) *Shaping Europe: France, Germany, and embedded bilateralism from the Elysée Treaty to twenty-first century politics*. Oxford: Oxford University Press.

Lambach D (2019) The Territorialization of Cyberspace. *International Studies Review* OnlineFirst. (https://doi-org.eres.qnl.qa/10.1093/isr/viz022).

Leisterer H (2016) New EU cyber security legislation: a Q & A with Andreas Schwab. *Internet Policy Review* (accessed 13 August 2018).

Lindsay JR (2015) The Impact of China on Cybersecurity: Fiction and Friction. *International Security* 39(3): 7–47.

Lukes S (1974) *Power: A Radical View*. London u.a.: Macmillan.

Manjikian MM (2010) From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly* 54(2): 381–401.

Meijer H and Wyss M (2018) Upside down: Reframing European Defence Studies. *Cooperation and Conflict* 54(3): 378–406.

Moe TM (2019) *The politics of institutional reform: Katrina, education, and the second face of power*. Cambridge, United Kingdom: Cambridge University Press.

Mueller ML (2019) Against Sovereignty in Cyberspace. *International Studies Review* 41(4): 206.

Newlove-Eriksson L, Giacomello G and Eriksson J (2018) The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security. *The International Spectator* 53(2): 124–140.

Nicolaïdis K, Whitman RG and Diez T (2013) Normative power as hegemony. *Cooperation and Conflict* 48(2): 194–210.

Nye JS (2017) Deterrence and Dissuasion in Cyberspace. *International Security* 41(3): 44–71.

Ross T (2017) *Threat of Cyber Attack Is Biggest Fear for Businesses*. Available at: https://www.bloomberg.com/politics/articles/2017-02-21/threat-of-cyber-attack-is-biggest-fear-for-businesses-survey (accessed 3 June 2017).

Schallbruch M and Skierka I (2018) *Cybersecurity in Germany*. Cham: Springer International Publishing.

Sexton M (2016) U.K. cybersecurity strategy and active cyber defence – issues and risks. *Journal of Cyber Policy* 1(2): 222–242.

Singer PW and Friedman A (2014) *Cybersecurity and cyberwar: What everyone needs to know*. Oxford: Oxford University Press.

Sjöstedt R (2012) Ideas, identities and internalization: Explaining securitizing moves. *Cooperation and Conflict* 48(1): 143–164.

Stritzel H (2016) Towards a Theory of Securitization: Copenhagen and Beyond. *European Journal of International Relations* 13(3): 357–383.

Watson SD (2009) *The Securitization of Humanitarian Migration*. Routledge.

Weber M (1978) *Economy and Society*. Berkeley: University of California Press.

Weiss M (2009) Power and signals: Explaining the German approach to European security. *Journal of International Relations and Development* 12(3): 317–348.

Weiss M (2014) Integrating the Acquisition of Leviathan's Swords? The Emerging Regulation of Defense Procurement Within the EU. In: Genschel P and Jachtenfuchs M (eds) *Beyond the regulatory polity? The European integration of core state powers*. Oxford: Oxford Univ. Press, pp. 27–45.

Weiss M (2019) From Wealth to Power? The Failure of Layered Reforms in India's Defense Sector. *Journal of Global Security Studies* 4(4): 560–578.

Weiss M (2020) Varieties of privatization: Informal networks, trust and state control of the commanding heights. *Review of International Political Economy*. OnlineFirst (https://doi.org/10.1080/09692290.2020.1726791).

Weiss M and Biermann F (2019) Varieties of Cybersecurity? The Institutional Foundations of Protecting Critical Infrastructures. *Science Peace Security '19. Proceedings of the Interdisciplinary Conference on Technical Peace and Security Research*, Darmstadt (https://tuprints.ulb.tu-darmstadt.de/9164/2/2019_SciencePeaceSecurity_Proceedings-TUprints.pdf#page=50).

Weiss M and Blauberger M (2016) Judicialized Law-Making and Opportunistic Enforcement: Explaining the EU's Challenge of National Defence Offsets. *JCMS: Journal of Common Market Studies* 54(2): 444–462.

Weiss M and Dalferth S (2009) Security Re-Divided: The Distinctiveness of Policy-Making in ESDP and JHA. *Cooperation and Conflict* 44(3): 268–287.

Weiss M and Jankauskas V (2019) Securing Cyberspace: How States Design Governance Arrangement. *Governance* 32(2): 259–275.

Weiss M and Weiss H-J (2005) Indexing. A General Approach for Explaining Political Biases in War Coverage. *Annual Conference of the International Communication Association (ICA)*, New York.

Zürn M (2018) *A theory of global governance: Authority, legitimacy, and contestation*. Oxford, United Kingdom: Oxford University Press.

Author contacts:

Moritz Weiss
Jean Monnet Fellow (2019/2020)
Robert Schuman Centre for Advanced Studies
European University Institute
Villa Raimondi
Via Boccaccio 121
50133 Firenze

Email: Moritz.Weiss@eui.eu
(ORCID iD: https://orcid.org/0000-0001-9311-6480)


With the support of the Erasmus+ Programme of the European Union

The European Commission supports the EUI through the European Union budget. This publication reflects the views only of the author(s), and the Commission cannot be held responsible for any use which may be made of the information contained therein.