ACIG APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

The (Il)legitimacy of Cybersecurity. An Application of Just Securitization Theory to Cybersecurity based on the Principle of Subsidiarity

Johannes Thumfart Research Group Law, Science, Technology and Society (LSTS),Department of Metajuridica, Faculty of Law and Criminology, Vrije Universiteit Brussels, Belgium; International security management at the Faculty of Police and Security, Berlin School of Economics and Law, Germany, ORCID: 0000-0003-4337-2990

Abstract

The application of securitization theory to cybersecurity is useful since it subjects the emotive rhetoric of threat construction to critical scrutiny. Floyd's just securitization theory (JST) constitutes a mixture of securitization theory and just war theory. Unlike traditional securitization theory, it also addresses the normative question of when securitization is legitimate. In this contribution, I critically apply Floyd's JST to cybersecurity and develop my own version of JST based on subsidiarity. Floyd's JST follows a minimalistic and subsidiary approach by emphasizing that securitization is only legitimate if it has a reasonable chance of success in averting threats to the satisfaction of basic human needs. From this restrictive perspective, cyber-securitization is only legitimate if it serves to protect critical infrastructure. Whilst Floyd's JST focuses exclusively on permissibility and needs instead of rights, I argue that there are cases in which states' compliance with human rights obligations requires the guarantee of cybersecurity, most importantly regarding the human right to privacy. My version of JST is also based on the principle of subsidiarity, in the sense that securitization should always include stakeholders directly affected by a threat. To strengthen this kind of subsidiarity, focused on the private sector, I argue for the legitimacy of private active self-defence in cyberspace and emphasize the importance of a 'whole-of-society approach' involving digital literacy and everyday security practices. Moreover, I argue that far-reaching securitization on the nation-state-level should be avoided, particularly the hyper-securitization of the digital public sphere, following unclear notions of 'digital sovereignty'.

Keywords

cybersecurity dilemma, desecuritization, digital sovereignty, securitization, securitization theory, societal security dilemma

Received: 28.09.2022
Accepted: 23.11.2022
Published: 25.11.2022

Cite this article as:
J. Thumfart, "The (Il)legitimacy of Cybersecurity. An Application of Just Securitization Theory to Cybersecurity based on the Principle of Subsidiarity," ACIG, vol. 1, no. 1, 2022, DOI: 10.5604/01.3001.0016.1093

Corresponding author:
Johannes Thumfart, Research Group Law, Science, Technology and Society (LSTS), Department of Metajuridica, Faculty of Law and Criminology, Vrije Universiteit Brussels, Belgium; International security management at the Faculty of Police and Security, Berlin School of Economics and Law, Germany; ORCID: 0000-0003-4337-2990; E-mail: johannes.thumfart@vub.be

1. Introduction

Cybersecurity is a particularly contested branch of security, since it relates to a socio-technical environment that is tightly interwoven with digital civil society and the global free flow of information and services. Correspondingly, cyberspace was historically linked to a cyber-libertarian political culture [1, 2]. From this perspective, it is hardly surprising that the issue of cybersecurity is increasingly discussed within the critical framework of securitization theory [3–6].

Securitization theory was developed by proponents of the Copenhagen School in the 1990s [7]; this theory originally examined 'securitizing speech acts' by which political leaders identify or construct a threat to a 'referent object of security' and promote 'exceptional measures' in order to avert or prevent this threat. This approach relies on the philosophical concept of speech acts that describes utterances which have a high social impact, for example, oaths, declarations of war, and calls to arms [8]. Rather than constituting a neutral methodological turn, the Copenhagen School's shift toward the examination of the role of language in the social construction of security is inherently critical since it is decidedly anti-positivist: its primarily linguistic analyses denaturalize the emotive rhetoric, subconscious fight-or-flight responses, and populist impulses connected with security issues [9, 10].

It is debatable whether securitization theory, which is primarily connected with international conflict and which emphasizes 'extraordinary measures' (including severe forms of coercion), can be applied to cybersecurity at all, which, in turn, is usually connected with everyday problems and focused on civilian technological routine [3]. Regardless of these difficulties, which will be addressed in detail, there are significant benefits from applying it in this manner. Cybersecurity is often related to various degrees of threat inflation, driven by widespread fears regarding rapid technological development on the one hand, and the concrete interests of security experts in the public and private sectors in increasing their wealth and/or power on the other hand, which has been described as the "cyber-industrial complex" [11] or "military-digital complex" [12]. This process has been criticized as "hyper-securitization", in the sense of exaggerated securitization, [3, 6], involving "inflationary and sensationalist danger hyping" [3] and "the rise of militaristic rhetoric around digital threats" [13].

Alongside the misallocation of resources due to such threat inflation, securitization can have undesirable effects on two different levels. First, there is the danger of a 'cybersecurity dilemma': when engaging in cyber-securitization in the sense of creating deterrence by threatening to defend forward, states increase their own security to the detriment of others and thereby destabilize the international system [14]. A similar dilemma arises when states promote their security by submitting civil society to widespread digital surveillance [15]. Second, particularly since cybersecurity is closely related to the digital public sphere, it can lead to the securitization of the digital public sphere [16], which conflicts with the democratic core value of freedom of speech [17]. In consequence, the securitization of cyberspace produces a version of the 'societal security dilemma' [4, 18]: Framing cyber interference as an international security issue shifts the focus away from resolving the domestic social tensions that create vulnerabilities to cyber interference in the first place.

Because these problems require a normative approach toward securitization, they constitute a suitable application of Rita Floyd's Just Securitization Theory (JST) [19–22], a critical offshoot of the Copenhagen School's approach. Floyd criticizes the Copenhagen School approach as "analytically strong" but "normatively weak" [22]. Her own JST is not exclusively focused on social constructivism but has a more empirical dimension and is normatively productive, attempting to answer the normative question of the legitimacy of securitization. Applying JST to cybersecurity will, therefore, allow a distinction to be drawn between legitimate and illegitimate forms of securitization

in cyberspace, with a special focus on the avoidance of hyper-securitization, the cyber security dilemma, and the societal security dilemma. This also includes a normative assessment of different approaches to digital sovereignty [23].

Floyd's JST follows a generally minimalistic and subsidiary approach by emphasizing that the legitimacy of securitization is only given if it stands "a reasonable chance of success" in averting threats to the satisfaction of "basic human needs" [19]. Likewise, she poses the complementary questions of when desecuritization is morally obligatory and how desecuritization should be implemented; 'desecuritization' implies the reversal of securitization, "the shifting of issues out of emergency mode and into the normal bargaining processes of the political sphere" [7].

Table 1. Main differences between Floyd's JST and my JST

	JUST INITIATION	JUST CONDUCT	JUST TERMINATION
FLOYD'S JST	• Focused on basic human needs instead of rights • Focused on permissibility	• Focused on physical threats • Focused on state actors • Contains elements of retributive justice • Considers intentions behind threats	• Securitization and desecuritization are understood as a dichotomy • Focused on sustainable securitization
MY JST TAILORED TO CYBERSECURITY	• Focused on protecting individual rights • Including states' obligation to guarantee security • Emphasizes the knowledge of stakeholders directly affected by a threat	• Considers non-physical threats • Emphasizes stakeholders' everyday security practices • Includes private actors' right to active self-defence • Separates retributive justice from securitization because it requires judicial procedures • Intentions behind threats are irrelevant • No financial or political gains should be connected with securitization	• Securitization and desecuritization are understood as continuous • Hyper-securitization is avoided, and sustainability is guaranteed by subsidiarity

During the discussion of the applicability of Floyd's JST to cybersecurity, I develop my own version of JST (Tab. 1.). First, I extend Floyd's focus, which is restricted to permissibility regarding securitization, to also include nation states' moral and legal obligation to securitize in order to protect human rights relevant to cyberspace, above all the right to privacy. Furthermore, I include private actors and everyday security practices [24] to a greater degree than in Floyd's original JST. Following Hansen and Nissenbaum's definition [6], everyday security practices include the practical knowledge of direct stakeholders and the consideration of the relevance of human behaviour to cybersecurity issues, for example, regarding passwords or phishing mails. The focus on such practices enhances the principle of subsidiarity that is already pre-figured in Floyd's original account. I argue that hyper-securitization can best be avoided by involving the stakeholders most directly affected by a threat in the decision-making processes, and by ensuring that securitization can be enacted autonomously by these stakeholders, provided that they have the necessary legal and technical competencies. In this context, I also emphasize the importance of a right to active self-defence in cyberspace [25]. In general, I argue that the Copenhagen School's dichotomous understanding of securitization and desecuritization, which is also reflected in Floyd's JST, is not applicable to the more continuous dynamics of securitization and desecuritization in cyberspace.

In the second section, I provide a critical discussion of the literature focused on the question of how securitization theory, which stems from the field of international conflict, can be applied to cybersecurity at all, which also involves international conflicts but is mostly focused on technological routine in everyday situations. The subsequent sections follow the structure of JST, which is tripartite in terms of just initiation, just conduct, and just termination. This tripartite nature corresponds to the partition of traditional just war theory in *jus ad bellum* (the right to war), *jus in bello* (rights in war), and *jus post bellum* (rights after war). In the third section, I raise the question of 'just initiation' regarding cybersecurity, which is largely determined by the question of which kind of threat allows for securitization or even morally requires it; in the fourth section, I pose the question of the 'just conduct' in cybersecurity, which involves the development of normative criteria regarding the concrete measures taken during securitization processes; in the fifth section, I pose the third and most difficult question, namely that of desecuritization. These sections are loosely divided into thematic subsections. The whole discussion is followed by a conclusion.

2. Literature Review focusing on the Application of Securitization Theory to Cyberspace and the Principle of Subsidiarity

2.1. The Incompatibilities of Securitization Theory and Cybersecurity

Since JST is a comparably new concept in Security Studies, until now it has only been applied in singular cases [26]. Besides a brief mention of Floyd's research in an article related to cybersecurity [27], JST has not yet been applied to cybersecurity at all. This is the most obvious research gap that this contribution addresses. As will be discussed in detail in Subsection 3.1, applying JST to cybersecurity has the advantage of considering the critical and constructivist approach of the Copenhagen School, whilst adding a normative and productive element to it.

In contrast to its recent offshoot, JST, securitization theory has been applied to cybersecurity frequently, e.g., [3–6]. The problems with the application of securitization theory to cybersecurity have been most extensively illuminated in Dunn Cavelty's discussion of the research literature [3]. Securitization theory originally developed from a focus on international conflict and understands security primarily as involving the use of force or the threat of force; according to Dunn Cavelty, the theory's genealogy from international conflict determines its focus on exceptional measures, i.e., measures outside of the 'normal' political order of liberal states, including trade-offs between fundamental rights or even the use of force. In contrast to this, cybersecurity is more focused on technological routines, which constitute the everyday situation rather than exceptional measures. She writes:

> When focusing on security that is no longer primarily about threats and battles against an enemy, but is characterized by an inward-looking narrative about vulnerabilities, it becomes necessary to question the perception of security as 'exceptional' and linked to 'extraordinary' means [3].

This observation represents an accurate caveat to this paper's basic attempt to apply JST to the issue of cybersecurity. After all, JST is an offshoot of the Copenhagen School approach and shares its origin in international relations theory. In turn, cybersecurity can involve conflicts between states, but it usually does not, particularly not in the sense of a direct clash between state actors. Non-state actors play an important role in international cybersecurity, as proxies or mercenaries (such as state-sponsored hacker groups) or as agents acting with various degree of independence (for instance, non-state hacker groups) [28].

But even if relevant cases involve a direct confrontation between states, they usually exhibit low intensity and do not pass the critical threshold of the use of force [29–32]. A particularly well-known example of this kind of conflict is the Russian meddling with the digital public spheres of Western countries, which barely exceeds the

spread of propaganda or cyber espionage and will be discussed in detail in section 4. Other phenomena such as cybercrime largely involving private actors only have a small significance to international security in the narrow sense.

2.2. The Compatibilities of Securitization Theory and Cybersecurity

Whilst the incompatibilities of the cybersecurity discourse and the Copenhagen School approach mentioned in the previous subsection are important, one should not overemphasize the degree to which classical securitization theory is exclusively applicable to international conflicts. First, regarding its context, securitization theory stems from the post-Cold War period in the 1990s. This era is characterized by a shift in the security discourse from a relatively simple paradigm of state-centric bipolarity to other, more complex problems, such as humanitarian interventions and terrorism.

When Buzan and Wæver developed securitization theory, they did so with the explicit intention of constructing a pathway between Habermas's discourse-oriented political theory and Schmitt's authoritarian theory of the state, focusing on the state's ability to implement exceptional, even unconstitutional measures in emergency situations [7], [33]. Habermas' discursive legitimatization of democracy does not relate to international conflict [34]; neither does the part of Schmitt's theory that includes his endorsement of the 'state of exception', which rather addresses the 'inner enemy' [35]. In liberal states, this inner enemy could be terrorists. Of course, terrorism is relevant to international security, but its domestic, societal, and cultural aspects demonstrate that securitization theory is familiar with issues that go beyond a paradigm focused on conflicts between states and involves many 'softer' and more complex mechanisms of creating societal security, rather than exceptional measures in the traditional sense [36]. Furthermore, securitization theory has been applied to ethnic conflict [18], HIV/AIDS [37], and human and drug trafficking [38], which all lie beyond the traditional scope of international conflict.

Another aspect of Dunn Cavelty's analysis of the problems with applying classical securitization theory to cybersecurity is the fact that the former is primarily focused on securitizing speech acts, i.e., the rhetorical process of declaring an issue relevant to security. This would imply that securitization theory can hardly be applied to cybersecurity, which is focused on technological procedures rather than on mere rhetoric, and is often not even publicly discussed, a trait that Dunn Cavelty characterizes as "non-discursive practices" [3].

Whilst this terminology is somewhat confusing, since it seems to suggest that there is practice without discourse, it probably has to be understood in the sense that cybersecurity is often exclusively the domain of "technical experts, rather than other political actors" and, therefore, not necessarily publicly discussed [3]. In underlining the non-discursive features of cybersecurity in this sense, Dunn Cavelty follows Hansen and Nissenbaum's seminal critique of "technification that depoliticizes" [6].

However, the Copenhagen School's emphasis on language also needs to be relativized regarding its methodological implications. From a methodological perspective, it must be underlined that traditional securitization theory focuses on *discourses* and *speech acts*, which both go beyond language itself. Traditional securitization theory cited Foucault and Austin as the theorists who coined these concepts [7]. Although the early work of the Copenhagen School indeed focused mostly on language [39], the original Foucauldian understanding of discourses includes theoretical *and* practical features [40]. Likewise, according to Austin, speech acts are defined by their relation to extra-linguistic practices and contexts [8]. The threshold between theory and practice is particularly permeable in the case of cybersecurity, which involves programming languages, algorithms, and workflows that are, by their very nature, situated on the border between theory and practice and can be understood in terms of Austin's speech acts

[41] or in terms of Foucault's discourses [42]. Hence, cybersecurity practices fall within the scope of traditional securitization theory, if *discourses* and *speech acts* are understood acknowledging the full range of these concepts.

In a recent collaborative paper with Egloff, Dunn Cavelty cited the Swiss model of subsidiarity as a possible means of bridging the conceptual conflict between cybersecurity as everyday security practices (often enacted by private stakeholders and neither including 'extraordinary measures' nor public speech acts) and state-level security agendas that tend to 'hyper-securitize', involving public rhetoric [24]. According to this principle, "a central authority should perform only those tasks which cannot be performed effectively at a more immediate or local level" [24]. Following Hansen and Nissenbaum's seminal definition, everyday security practices have to be understood in a double sense: first, they apply the practical knowledge of direct stakeholders to securitization processes; second, they consider the fact that human negligence, for example, regarding passwords or phishing mails, ranks among the most important security threats [6]. In my own account of JST, I will develop this notion of subsidiarity regarding cyber-securitization.

In summary, I argue that the continuities between securitization theory and cybersecurity are more important than their obvious incompatibilities. These continuities are: the definition and speculative construction of threats to a valued object of security, the discourses about and practical production of adequate means to avert these threats (including the attribution of resources), and the corresponding highly emotional (and thus dangerous) fight-or-flight responses. From this perspective, the routine aspects of cybersecurity *and* the exceptional aspects of cybersecurity can be understood within a securitization framework.

3. What is Just Initiation regarding Cybersecurity?

3.1. JST as a remedy against the Copenhagen School's Normative Weakness

Traditional securitization theory is largely critical of securitization since it focuses on putting the naturalization of securitization into question. The classical formula of the Copenhagen School defines the securitizing speech act as a discursive operation by which a securitizing actor (usually the government) justifies exceptional measures to avert an existential threat from a valued referent object of security (e.g., critical infrastructure, sensitive information, the nation, human livelihoods) in front of an audience (usually the public but also expert circles) [7]. Subsequently, the Copenhagen School analysed these securitizing speech acts (also called 'securitization moves') primarily with a focus on the rhetoric of political elites – but, as argued above, the school's methodological focus on discourses and speech acts allows, in principle, for far more practical applications.

The linguistic focus of the Copenhagen School produces a significant degree of moral relativism and incompatibility with the needs of practitioners to gain normative orientation: on the one hand, its methodological constructivism implicitly denies the possibility of security threats that simply "exist 'out there'" [19]; on the other hand, it might be misunderstood as reducing the often brutal measures of securitizing actors to mere rhetorical operations. In Floyd's words: "While analytically strong, the Copenhagen School's theory is normatively weak" [22].

Floyd tackles these weaknesses of the Copenhagen School approach, its moral relativism and lack of practical applicability, by two adjustments to classical securitization theory: first, she focuses on 'security actions' instead of 'securitizing speech acts' or 'securitizing moves', i.e., not merely the rhetoric but actual measures undertaken in acts of securitization. She writes: "Securitization is possible without the securitizing move but not without security action" [43]. Again, comparable to Dunn Cavelty's idea of "*non-discursive practices*" discussed in subsection 2.2, this must raise eyebrows but

is probably meant in a sense that securitization measures are not necessarily publicly addressed or discussed. Whilst it is debatable whether Floyd is accurate to assume that exclusively rhetorical securitization cannot constitute securitization, concrete securitization measures (involving trade-offs between fundamental rights or even the use of force) are obviously to be discussed much more critically than mere rhetoric.

Furthermore, Floyd argues that, due to its de-naturalizing approach focused on social constructivism, the Copenhagen School has, strictly speaking, no concept of objective threats. Moreover, if securitization theory does not distinguish between objective threats and their rhetorical construction, then all securitization moves have the same degree of legitimacy or the same lack of legitimacy. From such a dangerously relativist perspective, the US's attack on Iraq in order to avert the imaginary threat of Weapons of Mass Destruction has the same value as Sweden and Norway joining NATO to avert the real threat of Russian aggression; or, to take an example from cybersecurity, the hysterical securitization due to the unfounded fear of Y2K [4] would have the same value as the necessary securitization regarding WannaCry, which was likely to cause physical damage by attacking hospitals [44]. Floyd writes:

> An exclusive focus on the constructedness of security means (...) that securitization scholars tend to ignore whether or not the threats that inform securitization are real or otherwise. (...) A better strategy is to begin by (...) judging the objective existence of a threat, because unless there is a real threat, securitization is most definitely the wrong political and ethical choice [19].

Regarding the question of which objective threats to which referent objects make securitization legitimate, Floyd pursues a restrictive and subsidiary approach. According to her, the legitimacy of securitization is only given if it has "a reasonable chance of success" in averting threats to the satisfaction of "basic human needs" [19]. This minimalism is highly ambivalent if applied to the usually non-physical realm of cybersecurity. On the one hand, it is certainly possible to justify the securitization of critical infrastructure from this perspective, e.g., networks related to water, energy, and food supply. On the other hand, this focus on existential human needs may constitute an overly restrictive threshold, considering the non-physical scope of the vast majority of problems related to cybersecurity and the largely private sector-oriented and more quotidian, routine-driven, and civilian nature of cybersecurity, which does not necessarily require such a high threshold as it does not necessarily involve trade-offs between fundamental rights.

But it is worth taking a closer look at Floyd's argument. The advantage of her restrictive focus on concrete human needs as the only legitimate referent objects of security becomes particularly evident if contrasted with other possible referent objects, most importantly, the state. Unlike human beings, the state does not have a moral quality a priori because a state might be a dysfunctional dictatorship committing crimes against humanity. Additionally, particularly from a human rights-centric perspective based on the rule of law, the legitimacy of the state depends on whether it complies with human rights [43, 45].

From the perspective of Floyd's JST, which is not focused on rights but on output legitimacy regarding the satisfaction of basic human needs, this allows the following assessment: whilst Floyd's JST includes the possibility that nondemocratic regimes which guarantee the satisfaction of the basic needs of their citizens can be legitimate referent objects of securitization, this is not the case regarding democratic regimes that cannot guarantee this. One might add that Floyd's JST is too focused on output legitimacy in this regard. Emphasizing human needs instead of human rights might open the door for utilitarian reasoning, trading legitimacy for efficiency. However, Floyd argues that speaking of human needs opens the possibility of including referent objects in JST that do not involve actors and do not have a legislative function, most importantly the ecosystem, which will be discussed in relation to cybersecurity in subsection 3.3 [43].

3.2. JST as a Human-Centric approach to Cybersecurity

If applied to cybersecurity, Floyd's focus on human beings is particularly advantageous in the sense that it constitutes a principle of subsidiarity. It constitutes a "human-centric approach to cybersecurity", as defined by Deibert, to actively counteract a fixation on national security [46]. Frequently, the nebulous and largely rhetorical discourses about 'digital sovereignty' [23] and national cyber security [47] promote 'hyper-securitization' without providing a clear referent object of security. Furthermore, claims to 'digital sovereignty' inherently create what Mueller calls the 'cyberspace jurisdiction paradox' [48]: in the 'post-territorial' environment [46] of digital networks, claims to exercise territorial jurisdiction necessarily transcend borders and have extraterritorial features, such as exemplified by the digital aspects of the 'Brussels Effect' [49] and the 'Beijing Effect' [50]. This means that both the EU and China are exercising forms of extraterritorial jurisdiction in and through cyberspace: the EU in a regulatory sense, China by standard setting but also via globally available Chinese apps such as Alipay, WeChat Pay and TikTok, which share data with the Chinese government [51].

Analogue to these practices of extraterritorial jurisdiction and extraterritorial de facto control, the escalating rhetoric about 'digital sovereignty' [23] creates a 'cybersecurity dilemma' of states striving for an enhancement of their own security by threatening to defend forward, begetting international conflicts. Take for example NATO's doctrine that cyber-attacks can be interpreted as triggering a collective response according to Article 5 of the charter, including kinetic responses [52, 53]. Whilst such doctrines might have a deterrent effect, they can obviously cause destabilization, particularly since attribution is notoriously contested in cyberspace [54]. Moreover, as Dunn Cavelty argues, hyper-securitization not only creates a cybersecurity dilemma on the level of international relations but also regarding the relationship between states and individuals, whose rights are often seriously affected by states' hyper-securitization, such as with mass surveillance [15].

From the perspective of Floyd's JST, discourses regarding national cybersecurity need to be critically examined with respect to whether security claims related to 'sovereignty' actually refer to existential human needs. After all, the notions of 'cyber sovereignty' and 'information sovereignty' emerged in the context of Chinese authoritarianism in the late 1990s [55]. If such claims are not related to the everyday reality of concrete human needs, then their legitimacy seems doubtful. This is particularly the case if they involve restrictions on fundamental rights such as the right to privacy or the right to freedom of information, which includes the right "to receive and impart information and ideas of all kinds, regardless of borders" [56].

In turn, particularly because sovereign states are the ultimate guarantors of human rights, it is possible to conceive of forms of cyber-securitization following the paradigm of sovereignty that aim precisely at protecting these human rights. This is, for example, the case when claims to sovereignty are made to "draw a line" and protect individuals on a state's territory from becoming victims of digital transnational repression, by which authoritarian states reach into the territory of liberal states [57]. This will be discussed further in subsection 3.4.

3.3. JST, Posthuman Security, and the Participation of Civil Society

Floyd's understanding of the ecosystem as a legitimate referent object of securitization, by virtue of its functioning as a guarantee of the satisfaction of existential human needs, can also be applied to cybersecurity. Her approach in this regard can be understood in terms of 'posthuman security'. As has been argued by Mitchell in her essay on this issue [58], such an approach could be relevant to cybersecurity, which involves the protection of networks by focusing on their networked character. This means that complex digital networks require risk awareness in their own right because,

by virtue of their mere complexity and high degree of connectivity, they increase the probability of improbable but dangerous 'black swan' events [59]. Moreover, these events have the potential to affect the whole world, starting with automatized financial markets, for instance, as was the case in the 'flash crash' of 2010 [60]. Hansen and Nissenbaum scrutinized such digital disasters from a critical perspective, yet they did not entirely dismiss their plausibility [6].

In particular, such 'black swan' events, which are impossible to predict, raise complex epistemological questions. Floyd misses the opportunity to apply her human-centric approach to these epistemological problems, which constitutes another application of the principle of subsidiarity in my version of JST. Rather than being merely determined by governmental experts, securitization processes should include the participation of relevant stakeholders to achieve maximum epistemic certainty. The participation of relevant stakeholders is particularly important regarding cyber-securitization. In the cybersecurity sector, states do not necessarily have the upper hand in regard to skills and expertise [61], [62]. In many cases, private companies and civil society actors are better informed about weaknesses, exploits, and possible ways of counteracting them.

Enabling the participation of a wide array of these stakeholders could constitute a powerful aspect of building resilience. For instance, the German Government regularly consults with Europe's largest association of hackers, the Chaos Computer Club [63]. The Swiss government is likewise pursuing an approach focusing on everyday security practices [24]. The EU is pursuing a "whole-of-society approach" [64]. Such bottom-up approaches could also be relevant to international cybersecurity, constructing a private-public network of "distributed cyber deterrence" [25]. The US's Joint Cyber Defence Collaborative involving public-private partnerships is heading in this direction too [65]. If they include all levels of society, not merely an "invisible handshake" between Big Tech and governments [66], such participatory approaches could serve as a corrective force in securitization processes, making sure that fundamental rights and the interests of civil society are acknowledged by nation states, which are, chiefly due to their monopoly on violence, still the most powerful and most important securitization actors.

3.4. States' Obligation to Securitize

Particularly if securitization is connected to civil society, existential human needs, and fundamental rights on the legitimatory and epistemological level, in the way outlined in the previous subsections, it seems incoherent that Floyd's original account of JST focuses exclusively on permissibility, i.e., the question of when securitization is *allowed* [19]. If securitization is constituted in discourses which include the participation of relevant stakeholders, guarantee the satisfaction of existential human needs, and foster the enjoyment of human rights, then the emphasis on nation states' obligation to securitize not only represents a moral imperative but also a legal requirement. In a separate text addressing states' obligation to securitize, Floyd emphasizes different understandings of 'last resort' regarding exceptional measures in emergency situations that could bring about such an obligation [22]. But Floyd discusses this issue exclusively from an effects-based perspective and from a perspective that emphasizes the non-quotidian nature of securitization (the latter will be critically discussed in section 5.)

However, based on a more quotidian understanding of security *and* rights-based approaches, states are obliged to guarantee human rights on their territory, and this obligation clearly extends to cyberspace also. For instance, acts of digital transnational repression, in which authoritarian governments target exiled dissidents abroad, demand security measures since these actions threaten human rights on the host states' territory [67]. And such measures can most effectively be legitimized and communicated using the language of sovereignty, which is, in this sense, a tool for compliance with international obligations [57]. The EU's NIS Directive includes far-reaching obligations of member states to guarantee cybersecurity and to collaborate in this field [68].

Multilateral campaigns, such as the discontinued 'Clean Network Initiative', can be expected to increasingly include contractual obligations in regard to cybersecurity, in order to guarantee the free flow of information within international networks of trusted actors [69]. This constitutes the cybersecurity equivalent of the general economic trend toward so-called 'friend-shoring' [70].

These developing obligations of states in regard to cybersecurity also affect the private sector in an intermediate way, i.e., if legislation requires private actors to provide a certain degree of security, as is stipulated in the EU's NIS Directive. The relative proximity of public actors to the political ends of societies and the respective public debates on the one hand, and the relative remoteness of private actors from such debates on the other hand, contribute to the illusion that cybersecurity by private experts is exempted from political discourse. Such technification and depoliticization [6] is enhanced by excluding private stakeholders from debates regarding the normative foundations of national cybersecurity. In turn, my version of JST, which is focused on subsidiarity, *re-politicizes* cyber-securitization by explicitly including the private sector and emphasizing its obligations within everyday security practices. Following Hansen and Nissenbaum's definition, everyday security practices have two dimensions, involving civil society as an "ambiguous partner and a potential threat": first, they utilize the practical knowledge of direct stakeholders in securitization; second, they consider the fact that human negligence, for example, regarding passwords or phishing mails, ranks among the most important security threats [6].

4. What is Just Conduct regarding Cybersecurity?

4.1. Cybersecurity, Physical Violence, and Intentionality

In the previous section, I have considerably extended the possibilities and responsibilities of states and private actors regarding cyber-securitization in comparison to Floyd's restrictive account of JST. This requires submitting the issue of 'just conduct' to critical scrutiny.

Following the orthodox definition of 'exceptional measures', Floyd argues that securitizing actors are entitled to suspend some human rights in securitization processes [43]. She argues *against* the legitimacy of similar competencies regarding cyber threats, since they usually do not involve physical violence. She writes: "when there is a direct lethal threat, securitization can involve lethal force." However, the removal of hackers "by means of lethal force on the part of the police or some special branch thereof, or even a military strike would be unjust, because they do not pose a direct threat to human life [43]."

Indeed, the cases in which hackers or cyber-attacks brought about direct physical harm are quite rare [71]. An attack involving flickering images used on epileptic victims was one rare incident in which hacking brought about direct physical violence [72]. Other exceptional instances, such as a ransomware attack on the British NHS, might have caused physical harm in a sense that is almost as direct [44]. Considering such exceptional cases that involve violence indirectly or more or less directly, Floyd's JST would certainly allow for securitization.

However, according to Floyd, this is not necessarily the case if the physically violent consequences of a cyber threat were unintended. She writes: "Agents who do not realize that their actions are (...) lethal to other people (are) (...) morally irresponsible for posing the unjust threat [43]." Whilst not entirely dismissing the possibility of legitimate securitization regarding such threats caused – but not intended – by an agent, Floyd emphasizes that such threats do not allow for establishing a "standard formula" of securitization. At first sight, this distinction between "agent-intended threats" and merely "agent-caused threats" seems to make sense. But introducing the category of

intention constructs a nexus between morality and securitization that is highly problematic. By discussing responsibility and intention, Floyd seems to have constructed JST as a punitive instrument related to retributive justice.

However, under the rule of law, punishment can only be enacted following legal procedures, which reach conclusions about how to judge the intentions of suspects that are crucial to determining the degree of guilt. Such proceduralism is particularly important because, due to their non-empirical nature, intentions are inherently difficult to judge. In contrast to this, securitization theory is primarily concerned with averting a threat *pre-emptively and immediately*, and this scope conflicts with such cumbersome proceduralism. Therefore, in the unlikely case that the actions of someone unintentionally pose a lethal threat, it seems to be legitimate to avert this threat by 'extraordinary measures' involving the degree of coercion necessary to avert the threat, regardless of the actor's intentions. From a security perspective focused on the aversion of an immediate threat and the protection of physical integrity, it simply does not matter whether an average person poses a lethal threat by accident, or a brilliantly strategizing terrorist poses a lethal threat intentionally. What changes is merely the fact that a one-time intervention is likely to be much more successful if a particular actor is intentionally posing a threat; and non-intended threats might be reoccurring despite the neutralization of one particular actor.

Moreover, according to Floyd's JST, the decisive criterion regarding the legitimacy of 'exceptional measures' involved in securitization is the degree to which it can be expected that a suspension of human rights (including severe coercion) has "a reasonable chance of success" in averting a threat [43]. In addition to this, she emphasizes proportionality, which is a typical feature of just war theories. This means that the rights violations caused by the degree of coercion used to avert the threat cannot be greater than the rights violations that can be reasonably expected to be caused by the threat. Furthermore, she writes that securitization should, in general, do "the least amount of overall harm possible" [43] Finally, she writes that securitization must be aimed at being reversed by desecuritization at one point and it needs to include measures to "avoid renewed (...) securitization" [43], which means that it should aim for sustainable stability.

4.2. Intelligence Operations and the Securitization of the Digital Public Sphere

Whilst the criteria discussed in the previous subsection are rather uncontroversial, it is far from clear how they would apply to cybersecurity, assuming that a cyber-attack usually does not involve physical violence. Cyber-attacks usually only threaten the right to physical and intellectual property, privacy, and freedom of speech. Thus, Floyd's own account of JST focusing on basic human needs is clearly only applicable here if one understands it in a non-physical manner, involving human rights.

However, Floyd makes an interesting argument that can be used to shed some light on the rationale behind this distinction and which is useful for the application of JST to cybersecurity. She argues that, unlike threats to property, physical threats can be legitimately subjected to securitization processes because they inflict damage that cannot be restituted [43]. Whilst recognizing that Floyd's JST does not include the possibility of being applied to cybersecurity in relation to attacks without physically violent effects (regarding her own explicit assertions discussed in the previous subsection), it is worth asking how extensive a threat to technical infrastructure and complex digital networks would have to be to cause such irreversible damage. Similarly, Hansen and Nissenbaum emphasize the irreversibility of any damage inflicted as a feature that connects the protection of complex networks with the protection of the climate [6], which relates to issues of 'post-human security' discussed in subsection 3.3.

Besides cyber-attacks causing physical violence directly or indirectly, public actors tend to cyber-securitize when core issues of their national security, such as crucial confidential information, are at stake, which certainly may be interpreted as causing irreversible damage. The securitizing actions that have occurred in this context are 'exceptional measures' but not in the sense of involving the use of force. There is a significant degree of uncertainty regarding the adequate kind of response to cyber intelligence operations in this sense. On the one hand, NATO's Tallinn Manual states that "a state may not intervene, including by cyber means, in the internal or external affairs of another state" [53] and NATO does not exclude the possibility to respond kinetically to cyber-attacks [52]; on the other hand, international law tends to be rather permissive in regard to intelligence operations [73].

Attacked states are, therefore, aiming for targeted responses below the level of international conflict. For instance, the attack on the German Bundestag in 2015 brought about EU sanctions against the individuals and bodies involved within the EU's framework for a joint diplomatic response to malicious cyber activities [74]. The EU's so-called 'Cyber Diplomacy Toolbox' avoids national attribution [75]. This can be understood as an attempt to combine securitization with de-escalation. Another example of a response to intelligence operations is the US ban on Huawei, as recently renewed by Biden [76]. This also takes the conflict to the economic sphere without staging it as an international conflict and likewise combines de-escalation with securitization. Such approaches are certainly advisable from the perspective of my own JST framework, which is focused on subsidiarity.

More problematic are threats that surpass the traditional scope of cyber intelligence operations, particularly such threats that can be regarded as illegal interference with a state's self-determination, which can be understood as involving irreversible damage *and* can hardly be separated from a political understanding of international conflict. Self-determination is usually understood as regarding the constitution, i.e. the founding of a state. However, as Ohlin argues, this emphasis stems from an outdated state-centred understanding that ignores the continuous constitutive role of deliberative processes in society [77].

Cases such as the Russian meddling with the US general election, the Brexit referendum in 2016, and the French election campaign in 2017 have demonstrated that, due to their legitimization through deliberative discourses, democracies are particularly vulnerable to such interference as it undermines their own legitimacy. As a reaction to these threats, securitization occurred in the form of severe restrictions on the freedom of speech. For instance, France passed the 'Loi Avia' (2020) against hate speech and 'LoiNo. 2018–1202' against disinformation [78]. Because it touched upon the core of French Republicanism, the law against disinformation was subjected to heated debate, and ultimately its constitutionality was mainly affirmed because it only applies during the three months prior to the elections. In turn, the law against hate speech was so clearly at odds with the liberal paradigm of free speech that it was partly revoked as unconstitutional.

Germany's Network Enforcement Act (NetzDG) from 2017, which served as an inspiration for the French legislation, regulates disinformation and hate speech [78]. In the research literature, the law is regularly criticized for incentivizing the over-blocking of content that is not clearly illegal [79]. Against the intentions of its creators, the law has inspired authoritarian and semi-authoritarian regimes, including Singapore, Russia, the Philippines, and Venezuela, which explicitly mentioned the German NetzDG as model legislation [80]. Interestingly, particularly in the case of the network enforcement act, nation states are not directly involved in securitization in a sense of limiting fundamental rights, but this task is outsourced to private actors that have purely economic motivations to engage in over-deletion. The Germany Director at Human Rights Watch argued that the law "turns private companies into overzealous censors to avoid steep fines" [81].

Another drastic example of the securitization of the digital public sphere is the unprecedented prohibition of the spread of Russian state-sponsored media in the EU in 2022 [82].

Using the framework of JST, the legitimacy of this kind of securitization of the digital public sphere seems highly questionable. Since democratic deliberation is to be 'protected' by these measures, it appears paradoxical that this is done by limiting the legal precondition of public deliberation, which is freedom of speech. Furthermore, securitization of the digital public sphere might work as a short-term remedy against cyber interference, but it is hardly adequate to avert this threat in a sustainable way. Floyd argues that desecuritization (which will be addressed in the next section) is an integral part of JST; according to her, securitization must have the aim of being reversed by desecuritization at one point, and it needs to include measures to aim for sustainable stability and "avoid renewed (...) securitization" [43].

In contrast, although these regulations restricting free speech online were implemented as a reaction to Russia's interference in 2016 and 2017 and the spread of war propaganda in 2022, there are no discussions regarding the reversal of these securitization processes. This is hardly surprising because this kind of securitization of the digital public sphere is evidently not sustainable, since it produces a version of the 'societal security dilemma' [4]: traditionally, this dilemma describes how, for instance in ethnic conflicts, states tend to strengthen their 'own' identity and, paradoxically, precisely this securitization move weakens these states' capacity to integrate minorities that do not identify with the main identity of these states. Therefore, securitization in this sense has a destabilizing effect.

Comparably, informational interference does not create new threats out of the blue, but it rather exploits already existing social fault lines and conflicts. Take for example the US's racial fault lines that were exploited by Russia's support of White Supremacists *and* Black Lives Matter activists alike [83, 84]. Framing this kind of cyber interference as an international security issue shifts the focus away from resolving the domestic social tensions that create vulnerabilities to cyber interference in the first place. Therefore, whilst it satisfies the emotional need to identify a 'foreign' enemy, blaming social problems on 'Russian interference' can be expected to have a destabilizing effect in the long run.

Last but not least, securitizing the digital public sphere in this manner could have unintended ripple effects, since the formulation of prohibitions that cannot really be enforced undermines the credibility of the state (a realistic argument already used by Spinoza to make a point for freedom of speech [85]). For example, the ban on state-sponsored Russian media can be easily circumnavigated using VPNs. Furthermore, hate speech and disinformation will simply migrate to platforms such as Telegram that do not collaborate with the European authorities [86].

From a perspective focused on sustainable and subsidiary securitization, it would be more effective to stick to the EU's 'whole-of-society' approach and create sustainable resilience by promoting digital "media literacy as a key civic virtue" [64] Furthermore, the class divide contributes to the unquestioned acceptance of the claims of fake news [87]. Insofar as hostile cyber interference is exploiting social and other domestic fault lines, it would be more sustainable to tackle these vulnerabilities than to re-frame them as a result of foreign interference.

4.3. Private Companies as Norm Entrepreneurs and Securitizing Actors

Regarding private companies, it is debatable to what extent they can legitimately become securitizing actors. Evidently, private actors cannot engage in trade-offs between fundamental rights. When it comes to 'extraordinary measures' undertaken

in securitization, all that private actors can do is allocate extraordinary resources to an issue or accept more friction in their services and processes due to security measures. This also means that companies will usually tend to engage less in cybersecurity if there are no direct financial concerns related to this (e.g. by protecting a company's trade secrets or customer data) or if they are not required by states to engage in cybersecurity or nudged by consumer demand to create products that offer a high degree of security.

Larger companies (such as Microsoft) are an exception to this rule: they seek cooperation with legislators and act as 'norm entrepreneurs' in matters related to cybersecurity, i.e., they engage in promoting societal, legal, and political norms regarding cybersecurity [88, 89]. Also, though the platforms involved in enforcing the securitization of the digital public sphere are not necessarily intending this, it serves to enhance their power, particularly regarding the over-deletion of content [90]. This points to an aspect of just war theory that Floyd failed to address in her JST. Classical just war theory argues that no financial or political gains should be connected with just war [91]. Likewise, no financial or political gains should be connected with just securitization. This restriction, which is important to prevent just wars from being abused as justification for conquest or the acquisition of booty, is particularly important in relation to the involvement of private actors in securitization.

Companies large enough to afford compliance with complex cybersecurity regulations have a significant interest in promoting complex legislation since it can be a tool to push smaller players out of the market. To give some examples that do not directly relate to cybersecurity: in the field of data protection, the GDPR was hurting small and medium-sized enterprises (SMEs) more than bigger companies [92]. As a result of the learning derived from this asymmetrical effect, the new Digital Markets Act and the Digital Services Act (which likewise do not directly relate to cybersecurity) are exclusively regulating the activities of 'gatekeepers' and 'very large online platforms '(VLOPs) [93, 94]. Similar asymmetrical effects can be expected in regard to extended cybersecurity regulations if these do not exclusively target the bigger players. Therefore, the respective regulations should consider company size, and focus on subsidiarity in the sense that regulations should not overburden SMEs, thereby engendering market concentration. The EU's NIS Directive explicitly excludes small and micro enterprises for this reason [68].

Furthermore, the securitization of the digital public sphere by the restriction of freedom of speech gives large digital platforms a problematic degree of political power – even more problematic than the power that usually comes along with securitization, since private companies are not subject to the same legitimatory requirements as states [62]. Lehdonvirta argues that large digital platforms have transformed into 'Cloud Empires' because they guarantee and enforce social order and security on their virtual premises [95]. In summary, in contrast to the involvement of civil society stakeholders discussed in section 3, particularly the inclusion of Big Tech in the hyper-securitization of the digital public sphere is highly problematic since it can be associated with financial profits and gains in political power.

4.4. In favour of Self-Defence in Cyberspace

The issue of private self-defence in cyberspace is discussed in the literature [25, 62, 96]. Although this issue is situated below the threshold of physical violence, it is certainly a good example of securitization processes according to JST since it involves 'exceptional measures': the exemption from prosecution for acts that would normally be subject to this if they did not serve to avert a threat. In physical environments, a proportionate degree of physical resistance is justified if it serves to avert even non-violent acts of wrongdoing, for example, to deter threats to property, and if the act of resistance in question constitutes an adequate means of averting that threat, most notably in a pre-emptive sense. This is expressed in the stand-your-ground laws that are particularly far-reaching in the US [96].

These laws have been widely debated because they are connected with lethal violence and should be discussed critically [97]. Nevertheless, they express a fundamental principle of liberal legal and political philosophy: that individuals have the right to actively defend themselves if no other remedy is available, following Grotius's notion of 'private just war', which I applied to justify self-defence in cyberspace in another article [25]. Most notably, laws regarding self-defence are rather focused on the aversion of the threat than on proportionality in the sense of retributive justice. Even in heavily gun-controlled Germany, it is possible to resort to physical defence against crimes that do not directly affect the body, for instance, theft [98].

In 2017 and 2019, the bipartisan 'Active Cyber Defence Certainty Act' proposal, known as the 'hack back' bill, was discussed in the US Congress [99]. It would have applied the principle of self-defence to cyberspace [100] by allowing private companies to engage in active self-defence against attackers. Interestingly, the bill applied the same distinction between irreversible and reversible damage on which Floyd bases the whole idea that securitization is permissible in the case of an existential threat. Directly complementary to Floyd's legitimization of 'exceptional measures' in cases in which threats cause irreversible damage, the 'hack back bill' restricts private legitimate self-defence to such cases in which this active self-defence "does not result in the destruction of data or result in an impairment of the essential operating functionality of the attacker's computer system" [99].

Of course, the so-called 'hack-back bill' has been widely criticized for enabling vigilantism [101]. However, it is not altogether apparent why the general right to self-defence should be virtually non-existent in cyberspace. Following the analogy to self-defence in offline environments, which can be aggressive as long as it clearly serves to avert a threat or constitutes a swift reaction to an attack, it is not even clear why these measures should be restricted to "defensive measures", as argued by Pattison [62]. It seems to be sufficient that they are occurring swiftly and are effective in averting or preventing a threat.

Whilst it may seem paradoxical, a greater degree of autonomous securitization on the subsidiary level of private actors might contribute to de-escalation and desecuritization, since it allows for a certain degree of cyber-securitization to occur on the level of immediate stakeholders without escalating to the national level. In this regard, securitization executed in a largely autonomous sense by private actors would be directly opposed to the highly problematic form of hyper-securitization involving an entanglement between Big Tech and governments as discussed earlier. Furthermore, particularly regarding cybercrime with an international dimension, for instance, cross-border economic espionage, keeping the whole conflict below the international level could contribute to de-escalation inasmuch as this subsidiary strategy has, at least, the potential to keep international actors out of relatively petty conflicts and to guarantee a certain degree of deterrence at the same time.

5. What is Just Termination regarding Cybersecurity?

5.1. Cybersecurity beyond the flawed distinction between 'Normal' and 'Exceptional'

Just termination is certainly one of the most interesting features of Floyd's JST. Just termination refers to desecuritization following the Copenhagen School approach, i.e., the reversal of securitization, "the shifting of issues out of emergency mode and into the normal bargaining processes of the political sphere" [7]. Most importantly, she sticks to her overall restrictive trajectory by emphasizing that whilst she denies the obligation to securitize (see section 3), she underlines that there is an obligation to de-securitize:

> Just desecuritization is about what desecuritizing actors are required to do, not about what such actors are permitted to [43].

Whereas Floyd is aware of the problems with the Copenhagen School's definition in this regard, her rationale remains that the desecuritized situation represents the 'normal' situation, in which civil liberties and fundamental rights are in full effect, whereas the securitized situation represents the situation in which these rights and liberties are partly suspended through 'exceptional measures'.

From an intercultural perspective, the Copenhagen School's definition is highly flawed, since it implicitly assumes that well-functioning liberal societies with a history of colonialist exploitation (in the style of Denmark in the 1990s) represent the 'normal' state of affairs (which they never did globally) [102]. Furthermore, this terminological-conceptual setup produces two significant problems. First, it does not apply to authoritarian regimes such as China, where the 'normal' situation is heavily securitized; second, it fails to consider the obvious fact that civil liberties and human rights do not represent a 'normal' state of affairs but are the product of the state's monopoly on violence, which could be understood as a form of continuous, low-intensity, day-to-day securitization (as argued in section 3).

Following the Copenhagen School's understanding of securitization, based on the dichotomy between the 'normal' and the 'exceptional', Floyd writes that "desecuritization of just securitization must occur when the initial and related new objective existential threats have been neutralized" [43]. This makes a good deal of sense, despite the problematic assumptions behind the dichotomy between securitization and desecuritization. Particularly since they involve trade-offs between fundamental rights, securitization measures need to be proportionate and then revoked once their necessity becomes less evident.

This understanding of securitization as an exceptional form of disruption also applies, in certain aspects, to cybersecurity. For instance, security concerns have been cited to legitimize exceptions to the WTO's free trade regime regarding the banning of Chinese 5G suppliers such as Huawei [103, 104]. Since these measures are exceptions, their justification based on national security concerns suggests that they should be reversed once the Chinese government ceases to constitute a threat. Generally speaking, desecuritization is crucial regarding digital technologies because they rely on a baseline situation characterized by the free flow of information and services.

However, precisely for this reason, the dichotomy between securitization and desecuritization is problematic regarding cybersecurity. As discussed in sections 2 and 3, cybersecurity is mostly connected to everyday technological routines, rather than to 'exceptional measures'. Alongside this, due to the iterative nature of technological procedures, cybersecurity is not enacted momentarily and then reversed but is usually thought of as constituting a lasting feature that is inherently positive, as long as it guarantees the protection of human rights, such as the right to privacy. Rather than constituting an exceptional opposite to the free flow of information and services, cybersecurity must be combinable with openness, ideally with the greatest degree of openness. Cybersecurity, in the ideal typical sense (this means there are many exceptions to this), requires permanent securitization under the condition of permanent desecuritization.

5.2. Subsidiarity as structural Desecuritization

Precisely because of these non-dichotomous aspects discussed in the previous subsection, it is important to concentrate on desecuritization in relation to cybersecurity also. If there is no distinction between securitization and desecuritization, then anything goes. As already mentioned in section 4, the permanent character of cyber-securitization creates particular incentives for abuse. It can create lasting structures and a steady stream of revenue, which constitutes a strong incentive to engage in threat inflation and hyper-securitization within the "cyber-industrial complex" [11] or the "military-digital complex" [12]. The continuous securitization of the digital public sphere

discussed in section 4 might be an example of the problematic and ambivalent outcome of this kind of securitization. In some cases, such as regarding the enticement to violence or slander, it may be understood as a protection of human rights; in other cases, that is when over-deletion occurs, it simply constitutes a restriction of the freedom of speech by which the state and corporations mutually enhance their powers and limit civil liberties.

Whilst acknowledging the importance of the temporal aspect of securitization and de-securitization, inasmuch as it provides a criterion to judge *the aims* of securitization and the degree to which it provides sustainable stability, a simple binary between the 'normal' de-securitized situation and the 'exceptional' securitized situation does not do justice to the complexity of the cybersecurity landscape, which involves a great diversity of actors, temporalities, and trajectories and must consider securitization and desecuritization in the same instance.

As discussed in sections 3 and 4, this complex situation can be, at least partially, resolved by a version of JST based on the principle of subsidiarity, which does not generally favour de-securitization but is more inclined to pursuing a form of structural de-securitization: whilst acknowledging the necessarily lasting character of low-intensity securitization on an everyday level, particularly if it guarantees human rights, such an approach avoids hyper-securitization by relating securitization to the stakeholders most directly affected and granting them far-reaching possibilities to participate actively and autonomously in securitization.

The risk of hyper-securitization may also exist in the private sector but due to the high costs related to security, besides Big Tech's 'Cloud Empires', market mechanisms generally counteract hyper-securitization. Usually, private companies offer products with different levels of security, tailored to the need of individual customers and legal requirements. Turning securitization into a conscious consumer choice in this way is perhaps the best and most realistic road toward de-securitization since it moves securitization from the domain of the exceptional, instinctive, collective, and emotional to the domain of mundane and rational choices by mature individuals and their everyday security practices [24].

In contrast to this, as argued earlier, hyper-securitization primarily occurs within the framework of an "invisible handshake" [66] involving governments and Big Tech, which, in turn, should be observed critically, particularly regarding the acquisition of economic and political power through securitization.

6. Conclusion

In this contribution, I discussed the application of Floyd's JST to cybersecurity. As a reaction to the incompatibilities of JST and cybersecurity, I developed JST further to be more compatible with this specific sociotechnical environment, which is characterized by the great importance of the private sector and the civilian nature of the digital public sphere. In general, I have strengthened human rights and the idea of subsidiarity, according to which executive measures should ideally be enacted by the lowest organizational level. The germ of my arguments can be found in Floyd's original JST, which restricts the legitimacy of securitization to such cases in which securitization can be reasonably expected to be successful in averting threats to the satisfaction of existential human needs.

Two of my adjustments to Floyd's original JST (fig. 1) are particularly crucial in relation to cybersecurity: first, nation states' role in cybersecurity cannot be adequately understood by assuming that they are only *permitted* to securitize, as this constitutes the focus of Floyd's original JST. Rather, since states are required to guarantee the human right to privacy, they do have *legal and moral obligations* to guarantee cybersecurity on a day-to-day basis. Regarding everyday security practices, opposing the Copenhagen

School's questionable construction of a dichotomy between the 'exceptional' and the 'normal' situation, it is rather the maintenance of the 'normal' situation under the rule of law that requires quotidian low-intensity securitization involving the state's monopoly on violence. In this context, violence is rather to be understood as an implicit threat behind the state's regulatory function, than as something that is acted out in 'exceptional measures'. Indirectly, nation states' obligation to guarantee human rights in cyberspace also shapes the obligations of the private sector regarding cybersecurity. Moreover, the dichotomy between securitization and desecuritization is hardly applicable to cybersecurity since, in this context, securitization should occur under desecuritized conditions, guaranteeing an uninterrupted but secure global flow of information and services.

This non-dichotomous relationship between securitization and desecuritization is tackled by the principle of subsidiarity, which can be understood as a structural form of desecuritization. This principle does justice to the central role of private actors regarding cybersecurity, which are often more competent in the identification of threats and the construction of adequate securitization and defence mechanisms than states are. The subsidiarity principle, as the central aspect of my account of JST developed in this paper, has a permissive and a restrictive aspect. On the one hand, it leads to the demand that stakeholders directly affected by a threat should have the opportunity to participate in decision-making processes regarding cyber-securitization; furthermore, these stakeholders should also be given the legal means to engage in active self-defence, as this is common in offline environments with stand-your-ground laws and similar rules in many liberal jurisdictions.

On the other hand, this focus on subsidiarity directly tackles the issue of threat inflation and hyper-securitization: hyper-securitization causes a 'cybersecurity dilemma' that poses a threat to international security if states choose to deter by threatening to defend forward and respond with kinetic means to cyber-attacks, or if they attempt to strengthen national security by submitting citizens to surveillance. Moreover, hyper-securitization produces a variant of the 'societal security dilemma' by shifting the focus away from sustainably resolving domestic social conflicts and attributing them to 'foreign' interference instead. As a general rule, such hyper-securitization in cyberspace is not likely to be caused by private actors alone but by public-private partnerships in the framework of the "invisible handshake" [66], including the "cyber-industrial complex" [11] or the "military-digital complex" [12].

This paper opens up a broad horizon for further research. Floyd's focus on 'human needs' could be discussed in more detail regarding its ethical foundations, particularly with respect to the upsides and downsides of effects-based, i.e. utilitarian, approaches and intention-based, i.e. deontological or rights-based, approaches. My discussion suggests that Floyd mixes these approaches in a problematic manner. This inserts elements of retributive justice into her JST that appear incompatible with her understanding of securitization as involving 'exceptional measures'. The whole issue of retributive justice regarding cybersecurity should be investigated further, including but not restricted to the difficult problem of how to relate judicial and moral categories focused on physical violence to cyberspace at all.

My approach to strengthening the liberal principle of subsidiarity in JST is certainly not without alternatives. Floyd's monograph on JST [43] and particularly her more open discussion of possible approaches to JST as "a meta-theoretical framework" [22] [20] will certainly produce many opportunities to address the details of possible applications of JST to cybersecurity. I believe that my focus on the principle of subsidiarity has resolved the basic problems of this application reasonably well, which consists of the incompatibility of day-to-day technological routines and the drastic securitization discourses of states as discussed in section 2. Nevertheless, I am fully aware of the fact that my endorsement of private active self-defence in cyberspace may appear highly

problematic. But it seems the burden of proof falls on the side of those who argue that the right to self-defence, which is fundamental to liberal societies, should not apply in cyberspace, since this would constitute a form of 'cyberspace exceptionalism' [105]. Similar to Floyd's assessment of her own JST, my application of JST to cyberspace represents just "one possible variant of such a theory" [22].

Funding

Johannes Thumfart received funding from Gerda Henkel Stiftung's special programme Security Society and the State and the European Union Horizon 2020 research programme under MSCA COFUND grant agreement 101034352 with co-funding from the VUB-Industrial Research Fund.

Acknowledgements

I would like to thank the two reviewers for their thoughtful comments that greatly improved the paper.

REFERENCES

[1] J. P. Barlow. (2016, Jan. 20). *A declaration of the independence of cyberspace*, Electronic Frontier Foundation. [Online]. Available: https://www.eff.org/de/cyberspace-independence. [Accessed: July 1, 2021].

[2] R. Barbrook, A. Cameron, "The Californian ideology," *Science as Culture*, vol. 6, no. 1, pp. 44–72, 1996, doi: 10.1080/09505439609526455.

[3] M. Dunn Cavelty, "Cybersecurity between hypersecuritization and technological routine," in *Routledge handbook of international cybersecurity*, E. Tikk, M. Kerttunen, Eds. New York: Routledge, Taylor & Francis Group, 2020, pp. 11–21.

[4] J. Burton, C. Lain, "Desecuritising cybersecurity: towards a societal approach," *Journal of Cyber Policy*, vol. 5, no. 3, pp. 449–470, 2020, doi: 10.1080/23738871.2020.1856903.

[5] M. Lacy, D. Prince, "Securitization and the global politics of cybersecurity," *Global Discourse*, vol. 8, no. 1, pp. 100–115, 2018, doi: 10.1080/23269995.2017.1415082.

[6] L. Hansen, H. Nissenbaum, "Digital disaster, cyber security, and the Copenhagen school," *International Studies Quarterly*, vol. 53, no. 4, pp. 1155–1175, 2009.

[7] B. Buzan, O. Wæver, J. de Wilde, *Security: A new framework for analysis*. Boulder, Colo: Lynne Rienner Pub, 1998.

[8] J. L. Austin, *How to do things with words*. Oxford: Clarendon Press, 1962.

[9] C. Kinnvall, J. Mitzen, "Anxiety, fear, and ontological security in world politics: Thinking with and beyond Giddens," *International Theory*, vol. 12, no. 2, pp. 240–256, 2020, doi: 10.1017/S175297192000010X.

[10] R. McDermott, "Some emotional considerations in cyber conflict," *Journal of Cyber Policy*, vol. 4, no. 3, pp. 309–325, 2019, doi: 10.1080/23738871.2019.1701692.

[11] J. Brito, T. Watkins. (2012, Apr. 10). *Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy*, Mercatus Center. [Online]. Available: https://www.mercatus.org/publications/technology-and-innovation/loving-cyber-bomb-dangers-threat-inflation-cybersecurity. [Accessed: July 2, 2021].

[12] R. W. McChesney, *Digital disconnect: How capitalism is turning the Internet against democracy*. New York: The New Press, 2013.

[13] V. Bernal, "The cultural construction of cybersecurity: Digital threats and dangerous rhetoric," *Anthropological Quarterly*, vol. 94, no. 4, pp. 611–638, 2021, doi: 10.1353/anq.2021.0037.

[14] M. C. Libicki, "Is there a cybersecurity dilemma?," *The Cyber Defense Review*, vol. 1, no. 1, pp. 129–140, 2016.

[15] M. Dunn Cavelty, "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities," *Science and Engineering Ethics*, vol. 20, no. 3, pp. 701–715, 2014, doi: 10.1007/s11948-014-9551-y.

[16] B. C. Taylor, "Defending the state from digital deceit: The reflexive securitization of deepfake," *Critical Studies in Media Communication*, vol. 38, no. 1, pp. 1–17, 2021, doi: 10.1080/15295036.2020.1833058.

[17] N. Kshetri, *The quest to cyber superiority: Cybersecurity regulations, frameworks, and strategies of major economies*. New York: Springer, 2016.

[18] P. Roe, *Ethnic violence and the societal security dilemma*. London, New York: Routledge, 2005.

[19] R. Floyd, *The morality of security: A theory of just securitization*. New York: Cambridge University Press, 2019.

[20] R. Floyd, "The promise of theories of just securitization," in *Ethical security studies: A new research agenda*, J. Nyman, A. Burke, Eds. Abingdon, Oxon, New York: Routledge, 2016, pp. 75–88.

[21] R. Floyd, "Can securitization theory be used in normative analysis? Towards a just securitization theory," *Security Dialogue*, vol. 42, no. 4–5, pp. 427–439, 2011, doi: 10.1177/0967010611418712.

[22] R. Floyd, "States, last resort, and the obligation to securitize," *Polity*, vol. 51, no. 2, pp. 378–394, 2019, doi: 10.1086/701886.

[23] J. Thumfart, "The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the Covid-crisis 2020/21 as catalytic event," in *Enforcing rights in a changing world*, D. Hallinan, R. Leenes, P. de Hert, Eds. London: Hart Publishing, 2021, pp. 1–44.

[24] M. Dunn Cavelty, F. J. Egloff, "Hyper-securitization, everyday security practice and technification: Cyber-security logics in Switzerland," *Swiss Political Science Review*, vol. 27, no. 1, pp. 139–149, 2021, doi: 10.1111/spsr.12433.

[25] J. Thumfart, "Public and private just wars: Distributed cyber deterrence based on Vitoria and Grotius," *Internet Policy Review*, 2020, doi: 10.14763/2020.3.1500.

[26] G. Dimari, N. Papadakis, "The securitization of the Covid-19 pandemic in Greece: A just or unjust securitization?," *Quality & Quantity*, 2022, doi: 10.1007/s11135-022-01341-9.

[27] A. C. Dwyer, C. Stevens, L. P. Muller, M. D. Cavelty, L. Coles-Kemp, P. Thornton, "What can a critical cybersecurity do?," *International Political Sociology*, vol. 16, no. 3, p. olac013, 2022, doi: 10.1093/ips/olac013.

[28] T. Maurer, *Cyber mercenaries: The state, hackers, and power*. Cambridge, New York, Port Melbourne, New Delhi, Singapore: Cambridge University Press, 2018.

[29] E. Lilli, "Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence," *Contemporary Security Policy*, vol. 42, no. 2, pp. 163–188, 2021, doi: 10.1080/13523260.2021.1882812.

[30] S. Haataja, *Cyber attacks and international law on the use of force: The turn to information ethics*. Abingdon, Oxon, New York: Routledge, 2019.

[31] C. J. Finlay, "Just war, cyber war, and the concept of violence," *Philosophy & Technology*, vol. 31, no. 3, pp. 357–377, 2018, doi: 10.1007/s13347-017-0299-6.

[32] F. J. Egloff, J. Shires, "Offensive cyber capabilities and state violence: Three logics of integration," *Journal of Global Security Studies*, vol. 7, no. 1, p. ogab028, 2021, doi: 10.1093/jogss/ogab028.

[33] C. Schmitt, *Political theology: Four chapters on the concept of sovereignty*. Chicago: University of Chicago Press, 2005.

[34] J. Habermas, *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*. Cambridge: MIT press, 1992.

[35] C. Schmitt, "The concept of the political," in *The concept of the political*, G. Schwab, Ed. Chicago: University of Chicago Press, 2007, pp. 19–79.

[36] J. P. Burgess, N. Mouhleb. (2007). *A presentation of the state of societal security in Norway*, PRIO International Peace Research Institute, Oslo. [Online]. Available: https://www.prio.org/publications/7197. [Accessed: July 2, 2021].

[37] S. Elbe, "Should HIV/AIDS be securitized? The ethical dilemmas of linking HIV/AIDS and security," *International Studies Quarterly*, vol. 50, no. 1, pp. 119–144, 2006, doi: 10.1111/j.1468-2478.2006.00395.x.

[38] N. J. Jackson, "International organizations, security dichotomies and the trafficking of persons and narcotics," in "Post-soviet central Asia: A critique of the securitization framework," *Security Dialogue*, vol. 37, no. 3, pp. 299–317, 2006.

[39] F. Robinson, "Feminist care ethics and everyday insecurities," in *Ethical security studies: A new research agenda*, J. Nyman, A. Burke, Eds. Abingdon, Oxon, New York: Routledge, 2016, pp. 116–130.

[40] M. Foucault, *The archaeology of knowledge*. New York: Vintage Books, 2010.

[41] L. Tien, "Publishing software as a speech act," *Berkeley Technology Law Journal*, vol. 15, no. 2, pp. 629–712, 2000.

[42] A. R. Galloway, *Protocol: How control exists after decentralization*. Cambridge, Mass: MIT Press, 2004.

[43] R. Floyd, *The morality of security: A theory of just securitization*. New York: Cambridge University Press, 2019.

[44] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, P. Aylin, "A retrospective impact analysis of the WannaCry cyberattack on the NHS," *npj Digital Medicine*, vol. 2, no. 1, p. 98, 2019, doi: 10.1038/s41746-019-0161-6.

[45] J. Waldron, "The rule of international law," *Harvard Journal of Law and Public Policy*, vol. 30, no. 1, pp. 15–30, 2006.

[46] R. J. Deibert, "Toward a human-centric approach to cybersecurity," *Ethics & International Affairs*, vol. 32, no. 4, pp. 411–424, 2018, doi: 10.1017/S0892679418000618.

[47] N. Möllers, "Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state," *Science, Technology, & Human Values*, vol. 46, no. 1, pp. 112–138, 2021, doi: 10.1177/0162243920904436.

[48] M. Mueller, *Will the Internet fragment? Sovereignty, globalization and cyberspace*. Cambridge, United Kingdom, Malden: Polity Press, 2017.

[49] A. Bradford. (2020). *The Brussels effect: How the European Union rules the world*, Oxford University Press. [Online]. Available: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190088583.001.0001/oso-9780190088583. [Accessed: Feb. 13, 2022].

[50] M. S. Erie, T. Streinz. (2021). "The Beijing effect: China's digital silk road as transnational data governance," *New York University Journal of International Law and Politics*, vol. 54, no. 1. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810256. [Accessed: Feb. 13, 2022].

[51] A. Kokas, *Trafficking data: How China is winning the battle for digital sovereignty*. New York: Oxford University Press, 2022, doi: 10.1093/oso/9780197620502.001.0001.

[52] M. Prucková, *Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO*, NATO Cooperative Cyber Defence Centre of Excellence. [Online]. Available: https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/. [Accessed: Nov. 2, 2022].

[53] M. N. Schmitt, NATO Cooperative Cyber Defence Centre of Excellence, Eds., *Tallinn manual 2.0 on the international law applicable to cyber operations*, 2nd ed. Cambridge, United Kingdom, New York, USA: Cambridge University Press, 2017.

[54] F. J. Egloff, "Contested public attributions of cyber incidents and the role of academia," *Contemporary Security Policy*, vol. 41, no. 1, pp. 55–81, 2020, doi: 10.1080/13523260.2019.1677324.

[55] W. Cong, J. Thumfart, "A Chinese precursor to the digital sovereignty debate: Digital anti-colonialism and authoritarianism from the Post–Cold War Era to the Tunis Agenda," *Global Studies Quarterly*, vol. 2, no. 4, 2022, doi: https://doi.org/10.1093/isagsq/ksac059.

[56] U. Nations. (1948, Dec. 10). *Universal Declaration of Human Rights*. [Online]. Available: https://www.un.org/en/about-us/universal-declaration-of-human-rights. [Accessed: Nov. 14, 2022].

[57] M. Michaelsen, J. Thumfart, "Drawing a line: Digital transnational repression against political exiles and host state sovereignty," *European Journal of International Security*, pp. 1–21, 2022, doi: 10.1017/eis.2022.27.

[58] A. Mitchell, "Posthuman security / ethics," in *Ethical security studies: A new research agenda*, J. Nyman, A. Burke, Eds. Abingdon, Oxon, New York: Routledge, 2016, pp. 60–72.

[59] A. Avery. (2020). *Cybersecurity Scenario Modeling: Imagining the Black Swans for Digital Infrastructures Risk Management*. [Online]. Available: https://aisel.aisnet.org/sais2020/5. [Accessed: Nov. 14, 2021].

[60] I.-C. Tsai, "Flash crash and policy uncertainty," *Journal of International Financial Markets, Institutions and Money*, vol. 57, pp. 248–260, 2018, doi: 10.1016/j.intfin.2018.09.002.

[61] K. Bannelier, T. Christakis. (2017). *Cyber-Attacks – prevention-reactions: The role of states and private actors*, Les Cahiers de la Revue Défense Nationale, Paris. [Online]. Available: https://ssrn.com/abstract=2941988. [Accessed: Nov. 14, 2021].

[62] J. Pattison, "From defence to offence: The ethics of private cybersecurity," *European Journal of International Security*, vol. 5, no. 2, pp. 233–254, 2020, doi: 10.1017/eis.2020.6.

[63] P. Beuth, J. Breithut. (2021, Sep. 12). *40 Jahre CCC: Chaos macht Politik*, Der Spiegel. [Online]. Available: https://www.spiegel.de/netzwelt/netzpolitik/40-jahre-ccc-chaos-macht-politik-a-655ecc5b-d135-4ae5-846e-535d340448c3. [Accessed: Aug. 30, 2022].

[64] M. Wigell, H. Mikkola, T. Juntunen. (2021). *Best practises in the whole of society approach in countering hybrid threats*. [Online]. Available: https://www.europarl.europa.eu/committees/de/best-practises-in-the-whole-of-society-a/product-details/20210531CAN61132. [Accessed: July 1, 2021].

[65] Cybersecurity & Infrastructure Security Agency, *Joint cyber defense collaborative*. [Online]. Available: https://www.cisa.gov/jcdc. [Accessed: Aug. 30, 2022].

[66] M. D. Birnhack, N. Elkin-Koren, "The invisible handshake: The reemergence of the state in the Digital Environment," *SSRN Electronic Journal*, 2003, doi: 10.2139/ssrn.381020.

[67] M. Michaelsen. (2020). *The digital transnational repression toolkit, and its silencing effects*, Freedom House. [Online]. Available: https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects. [Accessed: May 29, 2021].

[68] European Union. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. [Accessed: Nov. 4, 2022].

[69] The Clean Network. (2017–2021). *United States Department of State*. [Online]. Available: https://2017-2021.state.gov/the-clean-network/. [Accessed: Sep. 2, 2022].

[70] G. Maihold. (2022). *A new geopolitics of supply chains: The rise of friend-shoring*, Stiftung Wissenschaft und Politik. [Online]. Available: https://www.swp-berlin.org/10.18449/2022C45/. [Accessed: Oct. 26, 2022].

[71] F. J. Egloff, J. Shires, "The better angels of our digital nature? Offensive cyber capabilities and state violence," *European Journal of International Security*, pp. 1–20, 2021, doi: 10.1017/eis.2021.20.

[72] CBS News. (2008, May 8). *Epilepsy site hacked with seizure images*. [Online]. Available: https://www.cbsnews.com/news/epilepsy-site-hacked-with-seizure-images/. [Accessed: May 17, 2022].

[73] A. Deeks, "Confronting and adapting: intelligence agencies and international law," *Virginia Law Review*, vol. 102, no. 3, pp. 599–685, 2016.

[74] European Council, *Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack*. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/. [Accessed: Nov. 6, 2022].

[75] F. Dumortier, V. Papakonstantinou, P. de Hert. (2020, Sep. 28). *EU sanctions against cyber-attacks and defense rights: Wanna Cry?*, European Law Blog. [Online]. Available: https://europeanlawblog.eu/2020/09/28/eu-sanctions-against-cyber-attacks-imposed-and-defense-rights-wanna-cry/. [Accessed: July 20, 2022].

[76] BBC News. (2021, Nov. 12). *US President Joe Biden tightens restrictions on Huawei and ZTE*. [Online]. Available: https://www.bbc.com/news/technology-59262329. [Accessed: Nov. 5, 2022].

[77] J. D. Ohlin. (2017). *Did Russian cyber interference in the 2016 election violate international law?*, Texas Law Review, vol. 95, no. 7 [Online]. Available: https://texaslawreview.org/russian-cyber-interference-2016-election-violate-international-law/. [Accessed: June 30, 2022].

[78] D. Steiger, "Protecting democratic elections against online influencevia 'fake news' - and hate speech – the french Loi Avia and Loi No. 2018–1202, the GermanNetwork enforcement act and the EU's Digital Services actin light of the right to freedom of expression," in *Theory and practice of the European Convention on Human Rights*, S. Schiedermair, A. Schwarz, D. Steiger, Eds. Baden-Baden: Nomos, 2022, pp. 165–214.

[79] L. Marc, *Das NetzDG in der praktischen Anwendung: Eine Teilevaluation des Netzwerk-durchsetzungsgesetzes*. Carl Grossmann, 2021. doi: 10.24921/2021.94115953.

[80] J. Mchangama, J. Fiss. (2019). *The digital Berlin Wall: How Germany (accidentally) created a prototype for global online censorship*, Justitia, Copenhagen. [Online]. Available: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf. [Accessed: Nov. 5, 2022].

[81] Human Rights Watch. (2018, Feb. 14). *Germany: Flawed social media law*. [Online]. Available: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law. [Accessed: Sep. 8, 2022].

[82] B. Baade. (2022, Mar. 8). *The EU's 'Ban' of RT and Sputnik*, Verfassungsblog. [Online]. Available: https://verfassungsblog.de/the-eus-ban-of-rt-and-sputnik/. [Accessed: Apr. 6, 2022].

[83] S. Bradshaw, R. DiResta, C. Miller, "Playing both sides: Russian state-backed media coverage of the #blacklivesmatter movement," *The International Journal of Press/Politics*, 2022, doi: 10.1177/19401612221082052.

[84] T. Snyder, *The road to unfreedom: Russia, Europe, America*. New York: Tim Duggan Books, 2018.

[85] B. de Spinoza, *Theological-political treatise*. Cambridge, New York: Cambridge University Press, 2007.

[86] S. Krempl. (2022, Mar. 24). *NetzDG-Streit mit Telegram: Deutsche Justiz wendet Zustellungstrick an*, heise online. [Online]. Available: https://www.heise.de/news/NetzDG-Streit-mit-Telegram-Deutsche-Justiz-wendet-Zustellungstrick-an-6624629.html. [Accessed: Sep. 8, 2022].

[87] D. A. Scheufele, N. M. Krause, "Science audiences, misinformation, and fake news," *Proceedings of the National Academy of Sciences*, vol. 116, no. 16, pp. 7662–7669, 2019, doi: 10.1073/pnas.1805871115.

[88] L. M. Hurel, L. C. Lobato, "Unpacking cyber norms: private companies as norm entrepreneurs," *Journal of Cyber Policy*, vol. 3, no. 1, pp. 61–76, 2018, doi: 10.1080/23738871.2018.1467942.

[89] C. M. Glen, "Norm entrepreneurship in global cybersecurity," *Politics & Policy*, vol. 49, no. 5, pp. 1121–1145, 2021, doi: 10.1111/polp.12430.

[90] R. Caplan, "The Artisan and the Decision Factory: The organizational dynamics of private speech governance," in *Digital technology and democratic theory*, L. Bernholz, H. Landemore, R. Reich, Eds. Chicago: University of Chicago Press, 2020, pp. 167–190.

[91] J. Thumfart, "Francisco de Vitoria and the Nomos of the Code: The Digital Commons and Natural Law, digital communication as a human right, just cyber-warfare," in *At the origins of modernity*, vol. 10, J. M. Beneyto, J. Corti Varela, Eds. Cham: Springer International Publishing, 2017, pp. 197–217.

[92] D. Barnard-Wills, L. Cochrane, K. Matturi, F. Marchetti. (2019). *Report on the SME experience of the GDPR*, Trilateral Research, Budapest - Brussels - Waterford, STAR II Deliverable D2.2. [Online]. Available: https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf. [Accessed: Nov. 5, 2022].

[93] European Parliament. (2022, Mar. 24). *Deal on digital markets act: Ensuring fair competition and more choice for users*. [Online]. Available: https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users. [Accessed: Apr. 14, 2022].

[94] European Parliament. (2020). *Digital Services Act – questions and answers*. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348. [Accessed: Apr. 14, 2022].

[95] V. Lehdonvirta, *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. Cambridge, Massachusetts: The MIT Press, 2022.

[96] H. Gandhi, "Active cyber defense certainty: A digital self-defense in the modern age," *Oklahoma City University Law Review*, vol. 43, pp. 101–131, 2019.

[97] C. McClellan, E. Tekin, "Stand your ground laws, homicides, and injuries," *Journal of Human Resources*, vol. 52, no. 3, pp. 621–653, 2017, doi: 10.3368/jhr.52.3.0613-5723R2.

[98] J. Bülte, "Zur Verhältnismäßigkeit der Notwehr und Art. 103 Abs. 2 GG als Schranken-Schranke," *Neue Kriminalpolitik*, vol. 28, no. 2, pp. 172–192, 2016.

[99] T. Graves. (2019, June 28). *Text - H.R.3270 - 116th Congress (2019–2020): Active Cyber Defense Certainty Act*. [Online]. Available: https://www.congress.gov/bill/116th-congress/house-bill/3270/text. [Accessed: July 1, 2021].

[100] M. Noone. (2018, Feb. 2). *Self-defense goes cyber: Congress considers a bill permitting victims of cyberattacks to 'hack back'*, University of Baltimore Law Review. [Online]. Available: https://ubaltlawreview.com/2018/02/02/self-defense-goes-cyber-congress-considers-a-bill-permitting-victims-of-cyberattacks-to-hack-back/. [Accessed: Sep. 4, 2022].

[101] M. Giles. (2019). *Five reasons 'hacking back' is a recipe for cybersecurity chaos*, MIT Technology Review. [Online]. Available: https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/. [Accessed: Sep. 10, 2022]

[102] A. Howell, M. Richter-Montpetit, "Is securitization theory racist? Civilizationism, methodological whiteness, and antiblack thought in the Copenhagen school," *Security Dialogue*, vol. 51, no. 1, pp. 3–22, 2020, doi: 10.1177/0967010619862921.

[103] S.-y. Peng, "Cybersecurity threats and the WTO national security exceptions," *Journal of International Economic Law*, vol. 18, no. 2, pp. 449–478, 2015, doi: 10.1093/jiel/jgv025.

[104] S. Nebehay. (2020, June 11). *China hits back at U.S. telecom supply chain order at WTO*, Reuters. [Online]. Available: https://www.reuters.com/article/us-usa-trade-china-wto-idUSKBN23I32V. [Accessed: Nov. 2, 2022].

[105] J. Cohen. (2007). *Cyberspace as/and space*, Georgetown Law Faculty Publications and Other Works. [Online]. Available: https://scholarship.law.georgetown.edu/facpub/807. [Accessed: Nov. 2, 2022].