The Peculiarities of Securitising Cyberspace: A Multi-Actor Analysis of the Construction of Cyber Threats in the US (2003-2016)

Noran Shafik Fouad
University of Sussex, Brighton, UK
n.fouad@sussex.ac.uk

Abstract: The rapid development of information and communication technologies rendered cybersecurity an integral aspect of contemporary security discourses and practices in different fields. Yet, despite the obvious intellectual demands of the field, most academic literature on cybersecurity in international relations and security studies remain policy-oriented and under-theorised. One of the few exceptions are studies utilising the Copenhagen school's securitisation theory to studying discourses and practices of cybersecurity, particularly in the US. Nevertheless, the cyber securitisation literature is still limited in its engagement with the complexity of cybersecurity. One important aspect of this limitation is their focus on official and government's discourses; an approach that is not applicable with a multi-stakeholder, privately-dominated cyberspace. This state-centric approach does not reflect the diversity of cybersecurity discourses by highlighting only the militarised, geopolitical narratives, adopted by some policy makers. Besides, it overlooks the nuances in threat perceptions, not just between the private and the public sectors, but also among different agencies inside the government. Therefore, focusing on the US as a case study, this paper will employ the securitisation theory's sectoral analysis for studying the process of securitisation in the field of cybersecurity, using a multi-actor approach which considers the role of several state and non-state actors in producing and managing cybersecurity discourses, and how complex public-private relationships influence cybersecurity policies and practices. The paper uses the method of discourse analysis in studying cybersecurity discourses of the government, private sector, and media in the US, by examining multiple resources, including official policy documents, congressional hearings, and opinion articles. The analysis covers the period from 2003, when the first cybersecurity strategy was announced, until the end of the Obama administration in 2016. The arguments presented by this paper contribute to the theorisation of the complex conceptual and policy problems of cybersecurity and of cyber securitisation processes through an inductive approach that develops an understanding of the logics and politics of security and risk as contextually-bound and sector-dependent.

Keywords: cybersecurity, cyberspace, securitisation, US cyber policy, discourse analysis

1. Introduction

Since the Morris Worm hit the earliest version of the internet (the ARPANET) in 1988, hostile cyber operations have been growing in number and sophistication; ranging from cyber crimes by non-state actors to state-backed cyber operations. At the same time, the range of 'insecure' objects has been widened to include, not only governments, but also individuals, businesses, and most recently, electoral processes. Despite the obvious intellectual demands of the field, most academic literature on cybersecurity remain policy-oriented and under-theorised. One of the few exceptions, however, are studies utilising the Copenhagen school's securitisation theory to studying discourses and practices of cybersecurity, particularly in the US (Eriksson, 2001; Bendrath, Eriksson and Giacomello, 2007; Dunn Cavelty, 2008a, 2008b; Hansen and Nissenbaum, 2009). The significance of these stems from the securitisation theory's explanatory power for understanding how and why a new realm like cyberspace is being constructed as a security sector, and how cyber practices are legitimised when their 'securityness' is accepted by the relevant audiences.

Nevertheless, the cyber securitisation literature remains very limited in its engagement with the complexity of the cyber realm. This can be seen, for instance, in their focus on official and government's discourses; an approach that is not applicable with the multi-stakeholder nature of cyberspace and one that misses the extent to which non-governmental actors produce and manage relevant threat discourses. This state-centric approach is problematic since it does not reflect the diversity of cybersecurity discourses, and because it only highlights the militarised, geopolitical discourses, adopted by some policy makers, that reinforces cyber territoriality over spatiality in a friend-enemy logic. Furthermore, they deal with states as unitary actors in cyberspace; overlooking the nuances in threat perceptions of intelligence communities and military institutions and cyber commands, executive, and legislative branches. Most importantly, by applying the theory's definition of security that is tied to existential threats and exceptional measures, those studies implicitly assume that meanings and practices of security are fixated along sectors. That is, they do not analyse how just as cyberspace has broadened the security agenda, it may have also transformed those meaning and practices beyond the Copenhagen School's conceptual framework.

Therefore, using the US as a case study, this paper will employ the securitisation theory's sectoral analysis for studying the discursive peculiarities of cybersecurity, using a multi-actor approach which considers the role of state and non-state actors in producing and managing cybersecurity discourses, and how complex public-private relationships influence cybersecurity policies and practices. The analysis covers the period from 2003, when the first cybersecurity strategy was announced in the US, until the end of the Obama administration in 2016. The paper primarily aims at answering the following questions: what issues are constructed as threatening in cybersecurity discourses and practices? To what referent objects? By which actor(s)? And targeting which audience(s)? Whom do such discourses and practices empower and/or exclude? In answering these questions, the paper uses the method of critical discourse analysis (CDA) (Fairclough, 2001, 2003), in which discourses are dealt with as both constitutive and constituted. This method is based on a three-dimensional analysis of discursive events: texts and their linguistic analysis; discursive practices, or the interpretation of processes of text production; and the analysis of social and institutional factors that shape discourses, i.e. discourses as social practice. Tracing the evolution of cybersecurity discourses over the study period, the paper employs CDA's concepts of *interdiscursivity* and *intertextual analysis*, which identifies and evaluates the links between texts, discursive genres, and their relations to external environments. Multiple resources are used in this analysis: 1-) seven cybersecurity-related documents issued by the White House, including cybersecurity strategies, presidential directives, and executive orders; 2-) six documents on cybersecurity by the Department of Defence (DoD), including the cyber defence strategy; 3-) four cybersecurity documents by the Department of Homeland Security (DHS); 5-) fifty four cybersecurity-related congressional hearings in the Committee on Homeland security in the House and the Committee on Homeland Security and Governmental Affairs in the Senate. Such hearings should be indicative of the discourses of MPs, executive officials, security experts, and members of the private sector, who are invited to testify in those hearings; and 6-) one hundred ninety-two editorials and opinion articles that has 'cybersecurity' in the major mentions, in the 'national security and international relations section' in US newspapers and wires, retrieved from the Nexis database. Editorials and opinion articles are presumably more explicit on policies and threat perceptions on the subject matter than news reporting. Given the extent of the textual sources involved, qualitative analysis software (NVivo 12) was used in coding the data.

The paper is divided into three sections. It starts first with an exploration of the logics of threats and vulnerabilities in cybersecurity discourses, and how the need for more cybersecurity is legitimised. It particularly focuses on the securitisation of cyber dependency and increased cyber capabilities, threat attribution and the attack logic, as well as the existentiality vs. urgency paradox. The second section examines the constellation of referent objects in cybersecurity discourses, or the objects constructed as being threatened and in need of protection, as well as the cross-sectoral connections they manifest with military, economic, and political security. The third investigates the cybersecurity ecosystem and the complexities of public-private relationships that shape questions of responsibility, liability, and the controversy over state's role.

2. The logics of threats and vulnerabilities in cybersecurity

> *"As we know, the genie is out of the bottle, just like nuclear weapons. It can be turned against us. We know what our offensive capability is and it is pretty darn impressive. That capability turned against us, I think is what frightens us, and who would have the motivation to do that." - Representative Michael T. Mccaul, congressional hearing (America is Under Cyber Attack: Why Urgent Action Is Needed, 2012, p.45)*

2.1 Securitising cyber dependency: Risk society as a security discourse

In his risk society thesis, Ulrich Beck assumes that we are now living in a 'second modernity', whereby risks can be conceptualised as "a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself" (Beck, 1992, p. 21). This period of 'reflexive modernity' is marked by the dominant force of the unknown, incalculable, and uncontrollable dangers, which are 'de-bounding' spatially, temporally, and socially (Beck, 2002, p. 41). In this advanced modernity, risks are not the result of an undersupply of technology, but rather from its *overproduction*, which eventually affects everyone, even those who produce and profit from risks (Beck, 1992, pp. 19–23).

Beck's risk society thesis can be seen as a security discourse per se, rather than just an approach to study the objective reality of cyber risks. It can be argued that risk society is a dominant discourse adopted by the majority of actors in constructing cyber threats. In this discourse, cyber dependency is securitised and portrayed as exponential, inevitable, and inherently threatening. Securitising cyber dependency is based on a belief in a revolutionary *present*: one in which ICTs are revolutionising modern life in 'unprecedented' ways, creating a 'new reality'. This revolutionary present is constructed as a threat as such using two logics. The first legitimises the call for more cybersecurity by highlighting how crucial cyber technologies are for "prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies" (The White House, 2011, p. 3). Accordingly, an insecure cyberspace means "the gains from computer integration can be wiped out or reversed" (Goldsmith and Hathaway, 2010). The second logic is centred on the increasing vulnerabilities produced by this dependency. It assumes that cyber technologies are growing more complex, and with complexity comes more insecurities and greater risks, because "Complexity is something we can't change" (Overview of the Cyber Problem, 2003, p. 11).

Thus, the need for security is legitimised by the importance of overcoming dependency-induced threats or to benefit from the fruits of the ICTs and the 'digital revolution'. Both logics produce multiple assertions in constructing the cyber threat: 1-) increasing cyber dependency and complexity are unavoidable, making the future more threatening than the present; 2-) cyber technology is inherently vulnerable, and thus impossible to fully secure; 3-) calls for 'more security' becomes self-justifying, given the understanding that the more cyber dependent the state is, the more inevitably threatened it becomes.

2.2 Geography and threat sources: from technical to political attribution

Since the first cybersecurity strategy was announced in 2003, attribution was not clearly used in cybersecurity discourses, and threats from states and non-state actors were presented on equal footing. Terms like 'our adversaries', 'attackers', 'malicious actors', and 'America's enemies' were used without a clear identification of particular actor(s). However, this situation has been changing gradually ever since to one in which attribution sometimes form the core of the cyber threat perception, with a strong emphasis on nation-states as a threat source, namely Russia, China, Iran, and North Korea. Much of this emphasis on threat attribution is driven from some territorial understanding of cyberspace and the sense of ownership that is found in many political discourses. Phrases like 'America's cyberspace', 'cyber borders', and an emphasis on the threat of the 'foreign' and the 'external' are important examples.

Here, we can differentiate between two types of attribution: *attack* attribution and *threat* attribution. The first is concerned with attacks that have already taken place, while the second is related to the ones that have not, and thus seeks to establish links between future threats/hazards and a particular source. Discourses that attribute the cyber threat to a certain source transfer conventional threat perception to cybersecurity. If the cyber threat is mainly associated with the aforementioned countries that are generally perceived as antagonistic to the US, and if their cyber capabilities are portrayed as exponentially increasing, then the US is automatically threatened. Consequently, the construction of futuristic threat scenarios becomes easier with little needed justification, because threat attribution with traditional enemies is invoked as a *facilitating condition* for securitisation. Although the published reports on attack attribution by the private sector exceed those of the government (Rid and Buchanan, 2015, p. 28), it is the government and some think tanks that focus more on this *threat* attribution. But other than categorisation purposes, what does attribution contribute to the cyber threat construction and why should it be problematised?

Firstly, this aspect of the cyber threat construction takes for granted the need for attribution in cyber defence. In conventional defence strategies, knowing the attack source and their capabilities before defensive or offensive responses is a must. However, cybersecurity is characterised by a high level of asymmetries that render this attribution-specific defence strategies obsolete (Rivera and Hare, 2014, p. 104). Secondly, the cyber threat/hazard attribution overlooks the uncertainties intrinsic to attack-attribution in cybersecurity. For instance, packets used in attacks can be changed before reaching the target and their original addresses can be erased by bots. Thus, 'to whose benefit' is not a credible strategy in attribution, because attacks can be implanted by a third-party. And even when they are traced to a certain country, it can be a separate political organisation or individual working for their own interests (Libicki, 2009). Thirdly, defining cyber capabilities is often more a matter of speculation than knowledge. Unlike military arms, cyber offensive tools are not observable, cannot be quantified, and in most cases, they cannot be recognised before an attack actually takes place, because in cyberspace, "offensive capacity correlates with defensive vulnerability" (Schutte, 2012, p. 8). Fourthly, in recent years, the line between offensive and defensive cyber operations is being blurred. Government officials acknowledge that many 'friendly' nations maintain an existence on the U.S. networks for information collection. Then who draws the line between the offensive and the defensive? This reinforces the idea about the cyber threat attribution as a political rather than a technical act, particularly in what the state decides to publish.

2.3 The nature of the cyber threat: between existentiality and urgency

Unlike other security sectors, cybersecurity threats are always perceived in the form of *attacks*, or hostile, purposeful, and deliberate actions by an enemy/adversary against the referent object(s). While this attack logic can still be used occasionally in all sectors, it is the *dominant* one in cybersecurity. All cyber operations, even the 'defensive', involve the use of malware by an actor to gain unauthorised access into the target's system. A vulnerability in a system is not threatening per se if not exploited, and this exploitation requires an adversary's or another party's involvement. Although the resemblances with the military sector here are high, one more aspect makes cybersecurity more distinctive: the question of existentiality. According to the securitisation theory, the defining feature of security is the idea of existentiality; i.e. security is concerned with the *survival* of a certain referent object(s), which justifies the calls for urgent responses.

In cybersecurity, despite the existence of existential discourses, the existentiality assumption is not as straightforward as it is in other sectors for multiple reasons. Firstly, the majority of cyber attacks that are seen as the most serious in history were neither objectively existential from a technical viewpoint, nor portrayed as such by the concerned actors. Stealing military, commercial, or personal information can hardly affect the survival of the state, the private sector, or any individual. Similarly, denying customers/citizens access to certain services through denial of service attacks (DOS) does not pose an existential threat to anyone. This does not mean that cyber threats cannot be hyped, exaggerated, or presented in urgent terms, since all those qualities are not essentially linked to existentiality. Secondly, the indirect nature of the majority of cyber attacks and the non-physicality of their consequences, although does not undermine their seriousness and urgency, acts as an *impeding* rather than a facilitating condition to the existentiality assumption. The empirical analysis also proves that existentiality is not the only reason for threats to register in the cybersecurity debate and that it is not a precondition for perceived *urgency*. Generally, cybersecurity is marked by different understandings of *disruptive* and *destructive* implications of cyber threats, and all invoke a certain level of urgency. The majority of discourses emphasise these 'disruptive' implications, including huge financial losses that can slow down the economy, loss of productivity and global competitiveness, customers' loss of confidence in the information infrastructure, etc. Though not portrayed in 'survival' terms, these disruptive implications are still perceived as immanent, urgent, and as serious threats to national security.

3. The constellation of referent objects in cybersecurity: cross-sectoral connections

A referent object of security is the object being threatened and the one that security policies aim to protect or secure. In the securitisation theory's framework, the identification of something as a referent object is always linked to a legitimate claim to existentiality (Buzan, Wæver and Wilde, 1998, pp. 103–104). Nevertheless, applying the same logic on cybersecurity disregards a wide range of important referent objects that lacks this survival quality due to the distinctive nature of cyber threats. Generally, the identification of an exclusive set of referent objects in cybersecurity is not an easy task, because such objects are subject to competing discourses and conflicting interests of multiple actors. As argued by Hansen, cybersecurity is better analysed through the "*competing* articulations of *constellations* of referent objects" (Hansen and Nissenbaum, 2009, p. 1163). And since the traditional public-private and individual-collective divide is blurred in cybersecurity, it is common to find strong links among them all in the same discourse, of which the following statement is an example: "Our national security, public safety, economic competitiveness, and personal privacy are at risk" (Emerging Cyber Threats to the United States, 2016, p11).

The relationship between cybersecurity and other security sectors can be first examined in the case of critical national infrastructure (CNIs). CNIs are defined as the "public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defence industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping" (The White House, 2003). They are usually granted more importance than individual or corporate cybersecurity: "The risks to that infrastructure are greater than the sum of the risks to the individual companies" (Overview of the Cyber Problem, 2003, p13). These infrastructures represent a unique case of the intersection between private and national security, since 85% of them are owned and run by the private sector. Additionally, they represent a constellation of referent objects per se, given their perceived connections to the 'state's security', 'economy', 'way of life', 'lifestyle', 'military operations', 'personal communications', 'public health', etc.

In addition to CNIs, particular intersection with economic security can be seen in portraying 'economic competitiveness', 'business opportunities', 'innovation', 'customers' confidence' as referent objects of cybersecurity, especially against threats of cyber espionage and intellectual property rights theft. Again, here, the public and private are intertwined; it is not just firms that are perceived as threatened, but also the American global 'competitive advantage' and 'economic leadership'. The military as a referent object is also one important component of many cybersecurity discourses, particularly by the executive branch. This was intensified after cyberspace has been declared by the state as a domain of warfare in 2010, just like land, air, sea and space (The White House, 2010; U.S. Department of Defense, 2010). Here, the survival of the armed forces is not necessarily presented as directly threatened as in the military sector, rather it is the survivability of military operations and communications, the military's defence and emergency capabilities, and its ability to utilise cyberspace as a force-multiplier that are perceived as referent objects.

Another very controversial referent object is 'privacy and civil liberties', which usually puts the individual in the centre of cybersecurity discourses. There are two ways in which privacy and civil liberties are constructed as referent objects. The first category of discourses focuses on how privacy is threatened by cyber attacks like identity theft and espionage. The second category questions the negative implications of cybersecurity policies on privacy and civil liberties and criticises the binary of 'security vs. privacy' that is sometimes used to legitimise government practices such as imposed backdoors and surveillance. These criticisms particularly deepened following Edward Snowden's revelation about the NSA's spying practices. As argued in an editorial: "Personal freedom or public safety? In our current environment, it seems one is increasingly taking a back seat to the other" (*The Lowell Sun*, 2015). For instance, voices are divided between a complete support for increased encryption on the basis that it positively affects innovation, the economy, and human rights, and those who oppose it arguing that it can impede law-enforcement processes and facilitate terrorists' communications. It has to be noted here that it is not just the government that tries to legitimise its opposition for increased encryption and its calls for backdoors by prioritising security over privacy. Other voices sometimes also argue that "We cannot achieve privacy without cyber security" (Cyber Security-2009, 2009, p29), and that giving agencies like the NSA more information that affects privacy is "a small price to pay for national, public health and energy security" (Brunner, 2015). These latter discourses implicitly assume that state's security is more important than individual's security, and misses the fact that deliberately weakening encryption may affect the overall security of the system on the long-run, given its links with intellectual property rights and financial transactions (Brantly, 2016).

4. Security actors in the cyber ecosystem: From the co-production of cyber technology to the co-production of cybersecurity

> *"Every computer company you bring into this room will tell you that liabilities will be bad for their industry. Of course they're going to tell you that; it's in their best interests not to be responsible for their own actions. The Department of Homeland Security will tell you that they need money for this and that massive government security program. Of course they're going to tell you that; it's in their best interests to get as large a budget as they can. The FBI is going to tell you that extreme penalties are necessary for the current crop of teenage cyberterrorists; they're trying to make the problem seem more dire than it really is to improve their own image. If you're going to help improve the security of our nation, you're going to have to look past everyone's individual self-interests toward the best interests of everyone." - Bruce Schneier, Counterpane Internet Security, Inc., congressional hearing (Overview of the cyber problem, 2003, p15).*

Classifying cybersecurity actors is not an easy task. The traditional divisions between 'public' and 'private' actors cannot grasp the complexity of the cyber ecosystem and the conflict of interests it is characterised by. This public-private classification gives a false image of a non-existent coherence among the various actors in each category. For instance, on the government side, it is not possible to combine the presidency, DHS, DoD, and the NSA all in one category, since each has their own interests, powers and responsibilities, and technical capabilities in cybersecurity. On the private sector side, a wider division of labour exists among software and hardware vendors, owners and operators of national infrastructures, internet service providers (ISPs), companies running search engines and social media platforms, security firms that provide consultation or insurance services, and all the rest of private sector corporations and entities whose security is essential to the state.

This multiplicity of actors challenges the Copenhagen school's conceptualisation of what constitutes a *securitising actor*. The theory defined the securitising actor as the one who *speaks security* or declares a referent object as existentially threatened by a speech act, which could be any individual or group, not necessarily the state. This is different from 'functional actors', who influence decisions taken to handle a threat without trying to securitise it themselves (Buzan, Wæver and Wilde, 1998, p. 40). Yet, the theory did not go further to consider those entitled with *acting security* or taking the decisions that security speech acts seek to influence. It can be argued that by being silent on who has the power not just to *speak* security but to *act* security, the securitisation theory retains a state-centric perception of security environments. Anyone can *securitise,* but it is the state that makes *security* happen. However, the situation is completely different in cybersecurity. Not only are the private actors significant securitising actors and referent objects of their own, they are in most cases the ones who act security and take the most critical decisions that affect the cybersecurity of the whole nation.

In the cybersecurity debate, there is always a controversy over assigning responsibilities for achieving cybersecurity and determining liabilities for cyber insecurity. Generally, most discourses emphasise the idea of 'collective responsibility', that no one entity can control or achieve cybersecurity without cooperation from all stakeholders, including individual users. Moreover, the government sometimes refer to the private sector as the more capable actor in leading cybersecurity than the government, and that it should form 'the first line of defence' (The Department of Defense, 2015, p. 5).

Accordingly, opinions are divided on whether the government should leave the market forces deicide, or should it have a more regulatory role. Proponents of the second view always warn against giving the government the power to micro-manage cybersecurity, which can cripple innovation, slow threat response processes, and harm the economy. The kind of intervention endorsed from this point of view is one that commercialises cybersecurity and support the indirect role of the government in influencing the market as a security customer. However, on the other side, other discourses note the mismatch between national security and commercial security interests: "The challenge is market forces are not designed to respond to national security threats. You cannot make a market case for the Cold War" (Securing America's Future: The Cybersecurity Act of 2012*,* 2012, p44). The interventions that these arguments call for include: incorporating code integrity clauses in contracts to hold vendors accountable; increasing government's funds for cybersecurity research; forcing businesses to declare when they are subject to cyber intrusions; improving information-sharing with the private sector; among others.

Alas, the most controversial political debate regarding the role of government in cybersecurity is related to the DoD and the NSA. Since its establishment in 2002, the DHS was given the main role of leading the national cybersecurity program following the release of the National Cybersecurity Strategy in 2003 and the establishment of its National Cybersecurity sub-division. Given its civilian nature, there has been no debate on whether it should be involved in cybersecurity or not. The majority of criticism directed towards the agency is usually regarding its effectiveness in securing the .gov infrastructures and cooperating with the private sector. On the other side, the DoD has considered the need to actively operate in cyberspace since 2006, when it regarded cyberspace as an essential component of its military operations. This was followed in 2010 by an official declaration of cyberspace as an 'operational domain' of warfare, and the establishment of the US Cyber Command. Similarly, for many years the NSA has been trying to stretch its prerogatives in cybersecurity policy by emphasising the similarities between military and civilian cybersecurity processes. In fact, this discourse is not just sponsored by the NSA, but also by some security firms and think tanks. According to them, the NSA has more technical acumen to lead national cybersecurity, particularly given what they perceive as a failure of the DHS. Nevertheless, more voices have been criticising this argument and warning from the dangers of militarising cyberspace. They argue that the NSA's role is the main hurdle in information-sharing with the private sector, because everyone fears that the shared information might end up in the NSA's bulk data collection program.

On the question of liabilities for cyber insecurity, disagreements are even deeper. We can distinguish between three discourses in this regard. The first always blames 'America's adversaries' or 'enemies', that are usually 'external' or 'foreign', as argued earlier. It focuses absolutely on blaming the attacker, with implicit assumptions that complete security is impossible. The second focuses on the end-users or customers in a neo-liberal discourse, viewing them as responsible for their insecurities due to their inability to deal with the uncertainties of a risk society. End-users are thus criticised for not updating their systems regularly and configuring them properly. The third discourse focuses on the role of the industry, particularly software vendors. Here, the idea of blaming end-users is criticised, as argued by a think tank representative in a congressional hearing: "cyber crime is the only crime I know of where we blame the victim" (Emerging Cyber Threats to the United States, 2016, p12). Software vendors and private corporations transfer the risk to customers, who suffer the consequences with little or no cost on the side of vendors. Therefore, one solution that is being advocated by a wide-spectrum of actors is imposing liability on the industry, whether software producers or network operators. However, vendors usually use the complexity argument and the idea of the impossibility of vulnerability-free software to get exempted from any sort of liability. Additionally, many vendors argue that imposing liabilities will damage the industry and increase the software cost on customers.

5. Conclusion

This paper used the idea of sectoralisation as presented by the Copenhagen' school securitisation theory to study the peculiarities of cybersecurity discursive construction. It did so by analysing cybersecurity discourses of the government, the private sector, think tanks, and the media over the period from 2003 until 2016 in the US. In discussing the logics of threats and vulnerabilities in constructing the cyber threat, the paper showed how cyber dependency is securitised in a way that legitimises the emphasis on a threatening future, the need for more security, and a certain level of risk acceptance. Threat attribution is also one important characteristic of the cyber threat construction, in which the political may override the technical. Discourses that attribute the cyber threat to Russia, China, Iran, and North Korea have been growing over the years, using the antagonistic relationship between those countries and the U.S. as a facilitating condition for cyber securitisation. Such discourses present the cyber threat as urgent and immanent, but not necessarily always *existential*.

On the referent object of cybersecurity, the paper examined the cross-sectoral connections between cybersecurity and other sectors, particularly the economic, political and military. Again, although critical national infrastructure constitutes the main referent object in the majority of discourses, other objects that lack the existential quality specified by the securitisation theory register in the cyber securitisation discourses. Finally, the paper discussed the multi-stakeholder nature of cybersecurity and how this security is being co-produced by a wide range of actors representing different, and in some cases contradicting, interests. By analysing aspects of power, responsibilities, and liabilities, the paper explored the main controversies in cybersecurity debates over state's role and intervention, the liabilities of the industry, and the responsibilities of end-users. It can be argued that there is no *one* discourse on cybersecurity or cyber threats, and it is a simplification to assume that there is even one discourse that represent each securitising actor, be it the government or the private sector. This diversity explains why the securitisation theory's assumptions and logics can apply on only some but not all discourses of cybersecurity.

Acknowledgments

I would like to thank my PhD supervisors, Prof. Stefan Elbe and Dr. Stefanie Ortmann, for their feedback on the chapter based on which this paper was written.

Funding: This paper was written as part of my PhD research, which is funded by the University of Sussex's Chancellor International Research Scholarship.

References

America Is Under Cyber Attack: Why Urgent Action Is Needed, Hearing before the Subcommittee on Oversight, Investigations, and Management, of the Committee on Homeland Security (Serial No. 112-85), U.S. House of Representatives, 112th Cong. (2000).

Beck, U. (1992) Risk Society: Towards a New Modernity. London ; Newbury Park, Calif: SAGE Publications Ltd.

Beck, U. (2002) 'The Terrorist Threat: World Risk Society Revisited', Theory, Culture & Society, 19(4), pp. 39–55. doi: 10.1177/0263276402019004003.

Bendrath, R., Eriksson, J. and Giacomello, G. (2007) 'From "Cyberterrorism" to "Cyberwar", Back and Forth: How the United States Securitized Cyberspace', in Eriksson, J. and Giacomello, G. (eds) International Relations and Security in the Digital Age, pp. 57–82.

Brantly, A. (2016) 'A Holistic Approach to the Encryption Debate', in Herr, T. and Harrison, R. M. (eds) Cyber Insecurity: Navigating the Perils of the Next Information Age. Rowman & Littlefield, pp. 191–204.

Brunner, J. (2015) 'Sharing Is Caring: Obama's New Cyber Security Executive Order', The State Press: Arizona State University, 19 February. Available at: https://www.nexis.com/ (Accessed: 14 February 2018).

Buzan, B., Wæver, O. and Wilde, J. de (1998) Security: A New Framework for Analysis. Boulder, Colo: Lynne Rienner Publishers.

Dunn Cavelty, M. (2008a) Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. London: Routledge (CSS studies in security and international relations).

Dunn Cavelty, M. (2008b) ‘Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate’, Journal of Information Technology & Politics, 4(1), pp. 19–36. doi: 10.1300/J516v04n01_03.

Eriksson, J. (2001) ‘Cyberplagues, IT, and Security: Threat Politics in the Information Age’, Journal of Contingencies and Crisis Management, 9(4), pp. 200–210. doi: 10.1111/1468-5973.00171.

Fairclough, N. (2001) Language and Power. 2 edition. Harlow, Eng. ; New York: Routledge.

Fairclough, N. (2003) Analysing Discourse: Textual Analysis for Social Research. London ; New York: Routledge.

Goldsmith, J. and Hathaway, M. (2010) ‘Cybersecurity Changes We Need’, The Washington Post, 29 May. Available at: https://www.nexis.com/ (Accessed: 14 February 2018).

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

Libicki, M. C. (2009) Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND.

Rid, T. and Buchanan, B. (2015) ‘Attributing Cyber Attacks’, Journal of Strategic Studies, 38(1–2), pp. 4–37. doi: 10.1080/01402390.2014.977382.

Rivera, J. and Hare, F. (2014) ‘The deployment of attribution agnostic cyberdefense constructs and internally based cyberthreat countermeasures’, in 2014 6th International Conference On Cyber Conflict (CyCon 2014). 2014 6th International Conference On Cyber Conflict (CyCon 2014), pp. 99–116. doi: 10.1109/CYCON.2014.6916398.

Schutte, S. (2012) ‘Cooperation Beats Deterrence in Cyberwar’, Peace Economics, Peace Science and Public Policy, 18(3). doi: 10.1515/peps-2012-0006.

The Department of Defense (2015) ‘The Department of Defense Cyber Strategy’. Available at: http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf (Accessed: 23 March 2017).

The Lowell Sun (2015) ‘Cyber Security at What Privacy Price?’, 25 February. Available at: https://www.nexis.com (Accessed: 14 February 2018).

The White House (2003) ‘The National Strategy to Secure Cyberspace’. United States Government. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (Accessed: 22 March 2017).

The White House (2010) ‘National Security Strategy of the United States’. United States Government. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (Accessed: 2 April 2017).

The White House (2011) ‘International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World’. United States Government. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Accessed: 22 March 2017).

U.S. Department of Defense (2010) ‘Quadrennial Defense Review Report’. Available at: https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf (Accessed: 2 February 2018).