Entropic Security

Information, Materiality, and Cybersecurity

Noran Fouad

Submitted for the degree of PhD in International Relations, University of Sussex, September 2020

Some parts of this thesis appeared in: 'The Peculiarities of Securitising Cyberspace: A Multi-actor Analysis of the Construction of Cyber Threats in the US (2003-2016)', in Tiago Cruz and Paulo Simoes (eds.), *Proceedings of the 18th European Conference on Cyber Warfare and Security*, 2019, pp 633-640. Also, in: 'Security as a Context, Generative Force, and Policy Concern for the Co-production of Cyberspace: Historical Overview Since WWII until the End of the Cold War', in Audun Josang (ed.), *Proceedings of the 17th European Conference on Cyber Warfare and Security*, 2018, pp 507-514.

Entropic Security: Information, Materiality, and Cybersecurity

ABSTRACT

This thesis advances a novel interdisciplinary exploration of cybersecurity. To date, one of the principal ways the field of cybersecurity has been theorised is through securitization theory. Cybersecurity is therefore identified by the Copenhagen School as a significant new security sector governed by the wider logics of existential threats, exceptionality, and emergency measures. This thesis, however, argues that cybersecurity actually differs from many other security sectors because of the peculiar ontological nature of 'information' that sits at the heart of this burgeoning field. Building upon recent scholarship on the philosophy of information, information sciences, and software studies, this thesis argues that three aspects of information are particularly significant for shaping, enabling, and producing the field of cybersecurity: (1) the intrinsic indeterminacies surrounding informational operations; (2) the non-anthropocentric agential capacities of codes/software; and (3) the simultaneous physicality and non-physicality of information. Through a detailed analysis of cybersecurity discourses in the United States of America (2003-16), the thesis thus goes on to show how these peculiar ontological characteristics of information generate security logics that are quite different from conventional accounts of securitization, and which are better captured through notions of *negentropy*, *emergence*, and *noise*. This ultimately culminates, the thesis argues, in a revised understanding of cybersecurity as *entropic security*.

ACRONYMS

AI	Artificial Intelligence
ANT	Actor-Network Theory
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNIs	Critical National Infrastructures
CNOs	Computer Network Operations
CSS	Critical Security Studies
DARPA	Defence Advanced Research Projects Agency, the USA
DDOS	Distributed Denial of Service attacks
DHS	Department of Homeland Security, the USA
DoD	Department of Defence, the USA
ICSs	Industrial Control Systems
ICTs	Information and Communication Technologies
IDSs	Intrusion Detection Systems
IPSs	Intrusion Prevention Systems
NSA	National Security Agency, the USA
OOO	Object-Oriented Ontology
PPPs	Public-Private Partnerships
STS	Science and Technology Studies

ACKNOWLEDGMENTS

First and foremost, I would like to express my sincere gratitude to my supervisors, Prof. Stefan Elbe and Dr. Stefanie Ortmann, for their immense support, encouragement, patience, and guidance throughout this project. They have always challenged me to think deeper about my arguments and encouraged me to explore new and exciting intellectual territories. I have benefited greatly from their constructive feedback and stimulating discussions, that not only have helped me complete this thesis, but also have made me a better researcher. They have given me confidence in my research abilities and in my capacity to become a good academic, and for that I cannot thank them enough. I would also like to extend my gratitude to Dr. Shane Brighton, who co-supervised my thesis in the first year. I learnt a lot from his challenging and insightful feedback on my research outline, which prompted me to further develop my thinking about the project.

This thesis has also benefited from feedback, discussions, and conversations in many academic contexts. I especially want to thank the members of the Department of International Relations at the University of Sussex; the participants of the GLOBE International Relations Winter School at the University of Lausanne (2019); the participants of the Sussex-Copenhagen PhD Workshop at the University of Copenhagen (2018); the participants of 17th and 18th European Conference on Cyber Warfare and Security (2018, 2019); and the participants of the BISA Postgraduate and Early Career Researchers Conference (2019).

I gratefully acknowledge the funding I received from the University of Sussex to conduct this project through the Chancellor's International Research Scholarship (CIRS).

I am deeply thankful to all my fantastic friends for their continuous support and for making my PhD experience enjoyable and rewarding. Special thanks to David Juenger, Ebru Demir, Florian Zabransky, Karam Abughazale, and Zhamilya Kussainova.

And last but not least, my deepest gratitude goes to my wonderful mother, father, and brother who have always believed in me more than I could ever believe in myself. I would have never been able to achieve anything in my life without their never-ending love, support, and encouragement.

TABLE OF CONTENTS

CHAPTER (1)
INTRODUCTION

For many years, cybersecurity has mostly been approached in International Relations through the lenses of traditional security theories and concepts. Because its emergence as a novel security field occurred after many of the long-established theoretical and methodological frameworks in International Relations and Security Studies were already developed, cybersecurity always faced the challenge of 'fitting in'. It has therefore been repeatedly scrutinised for its compatibility with conventional security logics and understandings, particularly with that of military security. Many literatures study cybersecurity by employing the conceptual frameworks of war, terrorism, and deterrence, and by assessing the gravity of the cyber threat using attack-based conceptualisations and traditional forms of violence as benchmarks (see Farwell & Rohozinski, 2011; Carr, 2012; Rid, 2012; Gartzke, 2013; Lindsay, 2013; McGraw, 2013; Kaplan, 2017; Nye, 2017). Imposing these militaristic frameworks onto the field of cybersecurity has revealed multiple tensions, however. In particular, the inherent complexity and technicality of this cybersecurity field have proven challenging to theorise and problematic to fit within conventional approaches to security.

Today, the majority of cybersecurity literatures remain policy-oriented in nature and tend to be conceptually under-theorised (Stevens, 2018, p.2). Studies utilising the Copenhagen School's securitization theory to studying discourses and practices of cybersecurity are one of the few exceptions in this regard (Bendrath, Eriksson, & Giacomello, 2007; Dunn Cavelty, 2008a, 2008b; Johan Eriksson, 2001; Hansen & Nissenbaum, 2009). Building upon its analytical framework, securitization theory principally theorises cybersecurity as *another* emerging security sector that can be studied through human subjectivities and the logics of existential threats, exceptionality, and emergency measures that also characterise other prominent security sectors – like military security, economic security, or environmental security. This generates a conceptually far more sophisticated approach to the study of cybersecurity, especially when compared to the policy-oriented literature. Yet, even securitization theory, this thesis argues, fails to adequately capture the peculiar *informational* ontology of the cybersecurity field. The historical rise of information

technologies and information sciences have, in fact, long challenged the centrality of human agency, and have also enabled a discussion on the agential capacities of machines and other non-human 'things'. Whilst such debates on technology and agency are becoming more prevalent in the analysis of other fields of security (for example: Dunn Cavelty et al., 2017; Kaufmann, 2019; Shaw & Akhter, 2014), it is not adequately reflected in the study of cybersecurity; i.e., the security of information technology per se and the construction of its logic(s). It is not sufficient, in short, to simply consider cybersecurity as yet another security sector, in the way securitization theory does.

This thesis therefore asks: *what do security and securitization look like when this peculiar informational ontology of cybersecurity is acknowledged, and when information is even theorised as a generative force of its own (in)security*? In order to explore this question, the thesis adopts a novel inter-disciplinary approach that accounts for the complexity of cybersecurity and which brings together the multi-disciplinary literature on the philosophy of information, information sciences, and software studies, as well as literatures on new materialism. Attending to 'information' as the core subject matter, referent object, and agency in cybersecurity, the thesis argues, adds important insights to its theorisation in Security Studies and to the understanding of the material conditions that influence its securitization and socio-political construction. Accordingly, the thesis develops a non-anthropocentric, informational framework to the study of the field of cybersecurity by theorising cybersecurity as *entropic security,* in which security is practiced through the logics of *negentropy*, *emergence*, and *noise*.

This introductory chapter starts by exploring the conceptual and policy challenges of cybersecurity and problematising its under-theorisation. It then moves to an analysis of the key limitations of securitization theory and the way it has been applied to cybersecurity. The chapter next elaborates how the thesis will address those limitations as a basis for the alternative theorisation of cybersecurity it aims to develop. In the third section, the chapter introduces the concept of the 'infosphere' to conceptualise cybersecurity as an ontologically differentiated field rather than a discursively constructed sector as argued by the cyber securitization literature. The fourth section states the main argument of the thesis and the methodology through

which it will be tested. The chapter ends, finally, with an explanation of the thesis outline and chapters' division.

1. Problematising cyber (in)security

Ever since the 'Morris Worm' first hit the earliest manifestation of the internet, the ARPANET, in 1988, hostile cyber operations have been growing exponentially in both number and sophistication; ranging from those conducted by non-state actors to state-backed attacks.[1] Concurrently, the range of 'insecure' objects has also widened considerably to include not only governments, but also individuals, businesses, and, most recently, even electoral processes. Operations have been targeting the multiple layers of what is referred to as 'cyberspace'. This includes physical systems (computers, cables, routers, and all hardware), virtual spaces (programs, codes, protocols, and all software), the cognitive domain (data, ideas, and meanings on digital systems), as well as the human users of information. These hostile cyber operations take a wide variety of forms. For example, a very common and widely known form is phishing campaigns, also known as social engineering, that trick targets into submitting personal or financial data or download malicious files to their systems. Operations known as Distributed Denial of Service attacks (DDOS) can flood a certain computer server with requests and stop it from providing services to its intended users. Cyber espionage is yet another example, in which information is obtained without the target's consent. The physical processes of computer systems can be also disrupted by sabotage campaigns, while a malicious software (malware) can wipe all the target's data or prevent access unless a ransom is payed; known as ransomware. This list could be extended much further.

During the past few years, several high-profile or allegedly state-backed operations were repeatedly reported by the media. These include the breach of the Democratic National Committee (DNC) in the United States of America (USA) in 2015 and 2016, the WannaCry ransomware attack which affected more than 200,000 computers in 150 countries, and the NotPetya which is widely considered the costliest cyber incident in history with an estimated loss of 10 billion dollars ('Top 5 Most Notorious Cyberattacks', 2018). However, the scope of the cybersecurity challenge is

[1] For further information on the Morris Worm and its implications see (Orman, 2003).

much wider still. Cybersecurity is as much about the less-than high-profile operations, as it is about the highly publicised ones. Such lower level incidents take place on a daily basis and may not even be discovered or reported by the targets, and hence not covered by the media. According to published statistics about data breaches in the USA, for example, the number of Americans affected by identity theft has reached 60 million in 2018. Based on a recent IBM report, a data breach takes on average 196 days to be discovered by the target, and costs companies 3.86 million worldwide ('10 Cyber Security Facts and Statistics for 2018', n.d.).

As a consequence of such events, cybersecurity has risen in prominence on the agenda of governments around the world, and it now constitutes an integral part of public, private, and academic discourses on contemporary security and insecurity. As a field for contemporary security studies, moreover, cybersecurity is marked by divergent approaches and differing opinions. Academic debate is significantly divided, for example, on the nature and extent of the security problem. Whilst 'cyber sceptics' criticise what they believe to be 'cyber hype' and question the damaging effects of cyber attacks to date (Gartzke, 2013; R. M. Lee & Rid, 2014; Lindsay, 2013; Rid, 2013a), there are also those who believe that 'cyberspace' has revolutionised modern conflict and should be dealt with as a whole new domain of warfare (J. Carr, 2012; Clarke & Knake, 2010; Junio, 2013; McGraw, 2013). Furthermore, inherent multi-disciplinarity and complexity has led to significant contention - both on the academic and policy levels - about how to define cybersecurity, the relevant importance of referent objects it comprises, and the nature of threats it should be defended against.

Added to these conceptual debates is a more policy-related one, stemming in part from increasing cyber dependencies and the massive development of information and communication technologies (ICTs). Those developments have widened the scope of potential attacks (Geers, 2011, p. 117); have lowered their costs and entry barriers (Weinstein, 2014, p. 7); and have ultimately privileged cyber offence over defence (Rattray, 2009, p. 272). Complex policy challenges also result from the need for information-sharing (Chittister & Haimes, 2006); public-private partnerships (M. Carr, 2016); the problem of attribution and deterrence; and the absence of acceptable international norms for states' behaviour in cybersecurity (Nye, 2017). Furthermore,

governments' intrusions in rivals' networks, and their involvement in the black markets of vulnerabilities and zero-day exploits, have produced new threat discourses and questions of response.[2] These practices have now been normalised as part of state 'defence' and are therefore not adequately questioned by academics and security experts, despite their role in undermining human security (Dunn Cavelty, 2014, p. 710, 2016, p. 20; Herzog & Schmid, 2016). On the other hand, the market-oriented views of the private sector, which tend to prioritise functionality over security, have also led to a culture of acceptance of software insecurity (Chong, 2016). This normalisation of private and public insecurity has created a situation in which patching (fixing) vulnerabilities (exploitable coding errors) on a regular basis is not yet an adopted behaviour by private sector organisations, especially the developers and operators of the Industrial Control Systems (ICS) that run critical national infrastructures (CNIs) (R. M. Lee, 2016).

Yet, despite the obvious intellectual demands of the field, most academic literature on cybersecurity remains fairly policy-oriented and conceptually under-theorised. One of the important exceptions in this regard is the cyber securitization literature (Bendrath, Eriksson, & Giacomello, 2007; Dunn Cavelty, 2008a, 2008b; Eriksson, 2001; L. Hansen & Nissenbaum, 2009). The significance of these literatures stems from securitization theory's explanatory power for understanding how and why a 'new' realm like cybersecurity is constructed as a security sector, and how cyber practices are legitimised when their 'securityness' is accepted by the relevant audiences. However, this thesis argues, the theory's conceptual anthropocentrism means that there are also multiple materialities and complexities of cybersecurity that the cyber securitization literature overlooks, as will be shown in the next section.

2. Securitization theory applied on cybersecurity

The Copenhagen School's securitization theory was developed by Barry Buzan, Ole Wæver, and Jaap de Wilde in their book 'Security: A New Framework for Analysis'

[2] Unknown vulnerabilities, or exploitable bugs in coding, are sometimes called 'zero-day vulnerabilities' or shortly 'zero-days'. They are the vulnerablities that are unknown to the software vendors and for which no patch is available. Hence, the name 'zero-day', which refers to the number of days the vulnerability was known to the target (Ablon & Bogart, 2017).

(Buzan, Wæver, & Wilde, 1998).[3] The theory emerged as a new framework to Security Studies amidst the debates between the so-called 'traditionalists' and the 'wideners-deepeners'. On contrary to the traditionalists who adopted military/statist conceptualisation of security, the wideners-deepeners widened the security agenda to include non-military issues and deepened the analysis of the referent objects of security beyond the state. Securitization theory was thus introduced as a widening-deepening theoretical framework that revisits the 'logic of security' and analyses the process through which issues are transferred to the security realm, in a way that differentiates them from the merely political (Buzan et al., 1998, pp. 1–5).

In answering the question on what constitutes security, the widening attempts of the theory are demonstrated in its argument that security is not necessarily related to the state as the only referent object, or military threats as the only security issues, as was the case in the realist theorisation of security. Consequently, the theory presented a sectoral analysis that identified five sectors in which security takes place: the military, the political, the economic, the societal, and the environmental sectors. It assumed that each of these sectors has its own audience, referent objects, distinct security agenda, and a certain set of qualities essential to its existence (Buzan et al., 1998).[4] It defined security as a process through which a *securitizing actor* presents an issue as posing an *existential threat* to a *referent object*, requiring *extraordinary measures* to ensure the object's *survival*. In order for securitization to succeed, the 'securitizing move' initiated by the actor has to be accepted by the targeted audience, who then grant this actor special powers and legitimise any breaking of rules to handle those threats. Thus, for an issue to qualify as 'security', it has to be put 'above politics' or to be presented as 'a special kind of politics'. This process can be studied by an analysis of security as a *speech act* and a discourse that comprises social and political construction of threats (Buzan et al., 1998, pp. 23–24).

[3] Original illustrations of securitization can be found in earlier works by Buzan and Wæver before they were finally clustered in a systematic theoretical framework in their book in 1998. For example, see: (Buzan, 1991; Wæver, 1988, 1995; Wæver, Buzan, Kelstrup, & Lemaitre, 1993)

[4] This sectoral analysis was first introduced by Buzan in a way that implicitly regards the state as the main referent object in all sectors (Buzan, 1991); a view that was later revised by Wæver to widen the scope of security referent objects beyond the state (Wæver, 1993).

Although cybersecurity was not part of its original formulation, the securitization theory did not rule out the possibility of adding more sectors to the analysis. Albert and Buzan discussed the sectoral analysis in a later article, in which they clarified that the five sectors identified as the 'principle sectors' of securitization were chosen because they constituted the main discourses of security when the theory was introduced. This implies the possibility of including more sectors, if they prove to be part of the security discourse in any specific period of time (Albert & Buzan, 2011, pp. 415–416). As cybersecurity began to be part of the international security agenda, some studies consequently applied the theory's framework to understand the process of its securitization, particularly in the USA as a case study (Bendrath, Eriksson, & Giacomello, 2007; Dunn Cavelty, 2008a, 2008b; Johan Eriksson, 2001; Hansen & Nissenbaum, 2009). They asked mainly whether cybersecurity has been securitized or not, and in answering this question reached contradictory conclusions. Some of them argued that cyber securitization succeeded in the USA (Bendrath et al., 2007; Hansen & Nissenbaum, 2009), while others argued that it failed (Dunn Cavelty, 2008a, 2008b). More recent contributions called for applying the securitization theory to understand the complexities of cybersecurity in 'the non-West' (Lacy & Prince, 2018), and extended the discussion on cyber securitization to other contexts, such as Singapore (Kallender & Hughes, 2017) and Japan (Aljunied, 2019).

Related to this cyber securitization literature are a wide range of studies that uses the securitization theory's discursive methodology - if not the theory as such - to explore how cybersecurity discourses, utterances, and threat representations are different from other sectors. They note that cybersecurity discourses operate in the absence of a minimum level of agreement on the nature of threats, and sometimes with no empirical evidence of attacks to justify them. That is why such discourses mostly rely on symbolisations, by drawing comparisons between cyber threats and other conventional ones, characterised by 'stable threat conventions' (Emerson, 2016; F. Hare, 2009; Jarvis, Macdonald, & Whiting, 2016). Added to this is the biologisation of technology and the use of 'viruses' and 'worms' metaphors (Dunn Cavelty, 2013); the spatial analogies of cyberspace (Betz & Stevens, 2013); viewing cybersecurity as inherently ungovernable and anarchic (Barnard-Wills & Ashenden, 2012); and the use of

fear-based analogies and hypothetical cyber-doom scenarios, such as cyber 9/11 or cyber Katerina (Lawson, 2013; Lawson, Yeo, Yu, & Greene, 2016). Lene Hansen and Helen Nissenbaum's theorisation of cybersecurity as a *distinct* security sector, to be added to the securitization theory's five sectors, by demonstrating its unique 'security grammars' is one notable contribution in this regard (Hansen & Nissenbaum, 2009). [5]

However, this emphasis on the discursive construction of security by the theory has been problematised by multiple studies, often classified as the 'second-generation' (Holger Stritzel & Chang, 2015, p. 550) or the sociological model of securitization (Balzacq, 2009). They criticise the theory for dismissing the extra-discursive and socio-political contextual influences on processes and practices of securitization. Hence, they suggest different ways to incorporate those contextual influences by analysing the macro and micro environments of securitization (Balzacq, 2011, p. 37; Wilkinson, 2011, p. 98); actor-audience relationships (Balzacq, 2005, pp. 184–185; Balzacq, Leonard, & Depauw, 2015, p. 7); forms of resistance to security frames (Holger Stritzel & Chang, 2015); and the multiplicity of securitizing audiences (Salter, 2008b). In the same vein, the application of the theory to the study of cybersecurity has been criticised for its limited conceptualisation of the securitizing actors whose discourses are relevant to the construction of security. This is seen in the cyber securitization literature's excessive focus on official and government's discourses; and thus, overlooking the role of non-state, private actors in producing and managing cybersecurity discourses (Dunn Cavelty, 2016, p. 94).

Notwithstanding the plausibility of such contributions, this thesis argues that there is more to the limitations of the theory's assumptions, and its emphasis on the discursive construction of security, than disregarding contextual influences and non-state securitizing actors. Specifically, the thesis criticises the theory and its application on cybersecurity for its *anthropocentric theorisation of agency*; i.e., tying *the capacity to*

[5] As argued by Hansen and Nissenbaum, the first cybersecurity grammar is *hypersecuritization*, through which cybersecurity discourses focus on disaster scenarios that have not taken place. The second is *everyday security practices*, by linking the scenarios of digital disasters to familiar experiences from everyday life, like credit card fraud, identity theft, etc. The third is *technification*, that creates political legitimacy for security experts by presenting cybersecurity as a domain that requires technical knowledge that the public do not have (L. Hansen & Nissenbaum, 2009).

act to human subjectivity and disregarding the role of the non-human in co-constructing security. Even when non-human things were included in the theory, they were primarily approached as 'facilitating conditions' outside the realm of agency (Aradau, 2010; Salter, 2019). If security is discursively constructed as assumed by the theory, and if discourse is a function of the *human* actor, then the ability to act and influence security ultimately resides in humans. It is always the human who is the securitizing actor, the audience, and the producer of security-making speech acts. Security is inter-subjective, but essentially all its subjects are humans. This assumption holds constant even if non-state actors are included (as suggested by the critique of the cyber securitization literature), and even when the socio-political context is considered (as argued by the second-order securitization literature).

Drawing upon the new materialism literature (for example: Barad, 2007; Bennett, 2009; Harman, 2018), the thesis argues that neglecting the materiality and agency of *non-human* 'things' in studying security in general, and cybersecurity in particular, is problematic. As put by Miller, "things that people make, make people" (Miller, 2005, p. 38). Though technological artifacts are human-made, they are capable of evolving in ways not necessarily envisioned by their creators, and influencing all aspects of human life, including security experiences and practices. As will be further demonstrated in the next chapters, the very idea of computer viruses and worms – that constitute 'the cyber weapon' – is an exemplar of how information systems are capable of deviating from the *human intentionality* embedded in their design. Cyber threats also reflect how information systems in their operations can challenge *human control* of security environments due to their intrinsic uncertainties. Therefore, against securitization theory's assumption that security is 'what actors make it' (Buzan & Wæver, 2003, p. 48), it is important to acknowledge the role of *contingency* in security construction as an ontological property of non-human objects (Rothe, 2017, p. 90). Accepting that the world is not reduced to humans, human control, and human intentionality enables us to understand how non-human 'things' co-produce contingency and enact (in)security. Action and actancy, as argued by Latour, should not be reduced to intentionality, consciousness, or free will and therefore tied exclusively to humans. Rather, actancy should be defined by the *influence* 'anything' can have on

other agents and this thing's capacity to modify those agents' actions (Latour, 2005, p. 71).

Accordingly, the thesis counters the anthropocentrism in the cyber securitization literature by shifting towards *information* and analysing cybersecurity as an ontologically informational field. Contending that cybersecurity is inherently informational means that it is essentially constituted, conceptualised, experienced, and managed through information as its core subject matter, referent object, and agency. Speaking of an informational ontology is only possible though if the humanist understanding of agency is challenged. This is because when agency is tied to the capacity of humans to act, humans become 'the centre of ontology' (Hoijtink & Leese, 2019, p. 10). Importantly, investigating the informational ontology of cybersecurity is, in many ways, ultimately a study of *materiality*. This means that, firstly, it is an acknowledgement of the informational essence of the *cyber* and its constitutive technologies and sciences beyond speech acts and linguistic utterances. As argued by Bennett, studying materiality means acknowledging that non-humans are real agents or actors rather than social constructs or mere instruments (Bennett, 2010, p. 47). Thus, the thesis considers the role of information as such in shaping, enabling, and/or limiting the construction processes of cybersecurity discourses and practices. Here, the thesis defines information by its syntactic (signs, signals, bits, etc.), semantic (meanings conveyed through those bits), and pragmatic elements (signifying the relationship between meanings and the receiver's knowledge) (Deacon, 2010, p. 152). This definition and the various other ways of defining information will be further explored in the next chapters.

Secondly, instead of reducing the referent objects of security to humans and human life, the thesis approaches information as a *peculiar* referent object of cybersecurity. In fact, the vast majority of the empirical securitization literature has been preoccupied with the study of securitizing actors and security grammars, rather than focusing the analysis on the properties and materialities of the *referent object* - not just its mere identification as part of a security discourse. The thesis, by contrast, deepens the analysis of the referent object, which is arguably one of the least explored aspects of securitization theory. It does so by examining the peculiar properties of

information as the ultimate referent object of cybersecurity. This peculiarity will be examined throughout the thesis in light of three key properties of information: (1) the intrinsic indeterminacies surrounding its operation; (2) the non-anthropocentric agential capacities of its syntactic elements (codes/software); and (3) its simultaneous physicality and non-physicality.

Thirdly, the materiality of information is studied in the thesis by showing how its peculiar ontological characteristics generate security logics that are quite different from conventional accounts of securitization. The logics of existentiality, exceptionality, and emergency measures - as introduced by the theory and adopted by the cyber securitization literature - assume a high level of *human control* and *intentionality* in the construction of security. Yet, this assumption too is not readily applicable to the field of cybersecurity, because it undermines the role of information in co-constructing its own (in)security. The contradicting conclusions reached by the literature on the success of cyber securitization processes in the USA, for instance, reflect this tension between the complexity of cybersecurity and the anthropocentric logics of the theory (Bendrath et al., 2007; Dunn Cavelty, 2008a, 2008b; Hansen & Nissenbaum, 2009;). Concluding that cyber securitization has failed because policy measures have not been *exceptional* enough to match the theory's criteria of security seems paradoxical. Considering the omnipresent prominence of this field of security in policy and academic debates as mentioned above, and particularly in the US case, a reconsideration of this criteria of 'securityness' is essential. This is an aspect that Dunn Cavelty, a key scholar in the cyber securitization literature, has acknowledged in a later work (Dunn Cavelty, 2020). As will be explained in the thesis, exceptional measures may not always be possible even if actors intend to introduce or apply them, given the limitations that information as an actant can impose on human control and intentionality in cybersecurity.

To capture the distinct security logics co-produced by the peculiarities of information in cybersecurity, the thesis develops the information-theoretic notion of *entropic security*. Entropy is a concept that first originated in thermodynamics, but later moved to information theory and several other academic fields, including economics, geography, and social theory. In information theory and cybernetics, entropy is mostly defined as uncertainty and disorder, randomness and non-linearity, or disruption in

communication channels (D. Li & Du, 2017, pp. 6–8). The thesis uses these three definitions analogically to advance an understanding of cybersecurity as entropic security, practiced through the logics of *negentropy*, *emergence*, and *noise*.[6] First, the thesis examines the intrinsic uncertainties and tendency towards disorder in the operation of information systems, and how this ontological property influences the *meaning* and *essence* of 'security' in cybersecurity. On that basis, cyber defence practices are reconceptualised as 'anti-entropic practices' directed against the entropic force of increasing disorder and insecurity; i.e., aiming at *negentropy* (negative entropy). Second, the thesis studies the entropic nature of cybersecurity by investigating the randomness and non-linearity generated by the agential capacities of codes/software. A particular focus is given in this regard to the role of codes/software in co-producing enmity and the subjects/objects of cybersecurity through the logic of *emergence.* Third, entropy as disruption in communication channels is used analogically in highlighting the significance of *mundane* cybersecurity as opposed to the existential. In this respect, the thesis analyses the (non-)physicality of information and its impact in co-constructing cyber threats through the logic of *noise*, that can invoke urgency without existentiality. Negentropy, emergence, and noise are all manifestations of the notion of entropy that challenge the assumptions of human control and intentionality embedded in the logics of security in the securitization and cyber securitization literature.

3. From a discursively-constructed sector to an 'infosphere'

Securitization theory introduced 'sectoralisation' as an analytically significant lens to facilitate the study of security and reduce its complexity. As Buzan and Little argue: "In IR, sectoral analysis refers to the practice of approaching the international system in terms of the type of activities, units, interactions, and structures within it" (Buzan & Little, 1998, p. 72). In Albert and Buzan's work on sectoralisation, they asked an important question on whether security sectors are mere analytical lenses which overlap, or ontological realms that have autonomous existence (Albert & Buzan, 2011). They did not give a definitive answer, but in their discussion they limited the criteria of

[6] Note that the notion of entropic security developed in this thesis is not related to 'entropic security' in the field of cryptography. In cryptography, the notion of entropic security was introduced by Russell and Wang in 2002 to specifically refer to an encryption scheme that relies on the aggressor's uncertainty regarding the function of the transmitted message (Russell & Wang, 2002).

sector differentiation to human actors, their perceptions, and their discourses. For example, they argued that sectors like the political or the economic could be classified as 'ontologically real' because they have a specific basal code; e.g., what constitutes having or not having power in a political system. According to them, the same argument cannot be made about the environmental or societal sector, given the absence of this communicational basal code. In short, they approached sectoralisation as a fundamentally empirical question, whose answer may vary according to place, time, and actors' discourses.

Although sectoralisation played an important role in widening the agenda of security studies beyond military security, it remains problematic given its intrinsic link to anthropocentric discursive constructions. Without renouncing the inherent connections between cybersecurity and other security sectors, the thesis assumes that cybersecurity is ontologically differentiated by its fundamentally *informational* nature – an assumption that will be fleshed out in the next chapters. Focusing on this informational ontology, rather than human speech acts, allows for theorising the peculiarities of cybersecurity and investigating its ontological makeup in ways that are not currently achieved by the existing security literature. This theoretical move from the 'cyber' to the 'informational' is also necessary because it provides a deeper account for the inherent multi-disciplinarity of cybersecurity.

The thesis, therefore, presents a novel inter-disciplinary exploration of cybersecurity by bringing the philosophy of information into International Relations and Security Studies. The philosophy of information as a newly emerging field of research interrogates the concept of information and provides important philosophical insights about its nature, principles, and dynamics (Adriaans & van Benthem, 2008; Floridi, 2010, 2013, 2016). This field evolved with the massive development of ICTs, and particularly computing and internetworking technologies. These developments brought information to the centre of philosophy as one significant force in the functioning of the world. Through the philosophy of information, one can study the structure of information and its representation in both machines and humans. Though 'philosophy of information' can refer to the philosophical study of information sciences - in the same way we can study the philosophy of humanities, for instance - this field also aims at presenting

'information as a major category of thought within philosophy itself' (Adriaans & van Benthem, 2008, p. 3-4). That is, the philosophy of information intends to use an 'information-oriented stance' in approaching epistemological and ontological questions.

Similarly, the thesis adopts an information-oriented stance in studying cybersecurity by establishing a dialogue between the philosophy of information on one side and International Relations and Security Studies on the other.[7] In so doing, the thesis presents cybersecurity as an 'infosphere' rather than a discursively constructed sector. The notion of the 'infosphere' is drawn from the work of Luciano Floridi (Floridi, 2009, 2010, 2013, 2014), a professor of philosophy and ethics of information and one of the prominent contributors to this multi-disciplinary field.[8] Floridi justifies the need for a philosophy of information by looking differently at the role of ICTs in our world. He assumes that ICTs are not simply 'enhancing' human life, but rather 're-ontologising' it. By re-ontologisation Floridi refers to the fundamental transformations to reality and to humans as a result of the information revolution, that he captures through the concept of the infosphere (Floridi, 2010, pp. 6-7). An infosphere, as described by Floridi, is an informational environment combining several informational entities that interact with one another in both online and offline spaces. It combines all those entities' properties, processes, and relations (Floridi, 2014). Although Floridi was referring to existence in its totality when he introduced the idea of the infosphere, this concept can also contribute to developing an informational approach to the study of cybersecurity. That is because Floridi's infosphere resembles cybersecurity in a number of ways.

Firstly, the infosphere is 'hyperhistorical'. This marks a transition from pre-history, when no ICTs existed; to history, in which progress and welfare is *related* to ICTs; and then finally to hyperhistory, when progress is *dependent* on ICTs. In this stage, ICTs are not just important, but a prerequisite for economic and societal development. It is also characterised by an exponential rise in the amount of data that needs to be stored and processed, which Floridi called the flood of 'zettabytes'; commonly referred to as

[7] The importance of integrating the philosophy of information into the debates in International Relations was first pointed out in an unpublished conference paper by Tim Stevens, in which he investigates the challenge that 'information' poses to new materialism in studying information conflicts (Stevens, 2012).

[8] Floridi acknowledged that the concept goes back to the 1970s and has its roots in the concept of 'biosphere', or the space on Earth in which life exists (Floridi, 2014, p. 40).

'big data' (Floridi, 2014). Likewise, it can be argued that as a hyperhistorical infosphere, cybersecurity threats are driven by the increasing dependence on information technologies and big data. In this respect, cybersecurity is different from security sectors in which more development may bring more security, be it economic, military, or political development. As Floridi puts it, "Only a society that lives hyperhistorically can be threatened informationally, by a cyber attack. Only those who live by the digit may die by the digit" (Floridi, 2014, p. 4).

Secondly, Floridi's infosphere witnesses what he calls 'third-order technologies' and the erosion between online and off-line existence. It signifies the state of technology as both a user and prompter of innovation, such as the case of the internet of things (IoTs), in which humans are kept outside the loop of communications. Devices connect to one another, exchange protocols, send and receive data, update their files, all possibly without the intervention of the human beneficiary. Eventually, "Being out of the loop could mean being out of control" (Floridi, 2014, p. 39). Thus, instead of being merely tools that facilitate human life, ICTs are becoming forces of their own that shape reality. Humans in turn become informational organisms, or *infORGs*, that interact with a variety of other non-human informational agents. Many aspects of cybersecurity are fundamentally ungovernable and/or uncontrollable by humans. That is why cybersecurity, understood as an infosphere, should be approached as a field of contingencies that ultimately escape the span of absolute human control. One possible political implication of this is shifting the essence of politics and security from managing people's lives towards managing the 'life cycle of information'. This life cycle of information includes information occurrence, transmission, processing, and usage (Durante, 2017).

Finally, in an infosphere, power over data and ICTs does not reside in the state as the sole agent; it is distributed among a wide-range of non-state actors, enabled and empowered by such technologies (Floridi, 2014). And hence, the analysis of the state as a political organisation is no longer the core of understanding politics, rather, it is the 'organisation of relationships between agents of different types and natures' (Durante, 2017). The thesis extends this argument to cybersecurity as an infosphere that ultimately breaks the key dichotomies of subject/object, human/non-human, and

public/private. As put by Floridi, "ICTs are not merely re-engineering but actually re-ontologizing our world" (Floridi, 2010, 10-11). There is a subsequent need then for studying the impact of this re-ontologisation on the study of security at large, and specifically on the study of ICTs security as such. Through its inter-disciplinary informational framework and its information-theoretic notion of entropic security, the thesis can thus attend to the peculiar ontology of cybersecurity by transcending the anthropocentric limits of sectoralisation and its language that have characterised the scholarship on cybersecurity to date.

4. Research design

To summarise, the central argument of this thesis is that the *informational* ontology of cybersecurity poses profound conceptual challenges to securitization theory and the wider literature on cybersecurity. The thesis aims to demonstrate that approaching information as a generative force of its own (in)security requires an alternative conceptual framework to the one introduced by the Copenhagen School. The next chapters of the thesis will therefore develop such a novel exploration of cybersecurity as *entropic security*, constructed through the three logics of *negentropy, emergence*, and *noise*. Crucially, this alternative exploration assumes a *non-anthropocentric* conceptualisation of agency and actancy; problematises the ontology and materiality of information as a referent object in cybersecurity; and contextualises the logic(s) of security in analysing cyber securitization processes. It does so by focusing analytically on three main properties of information: the intrinsic indeterminacies of information systems; the agential capacities of codes/software; and the simultaneous physicality and non-physicality of information.

In order to theoretically capture the ontology of information, and to develop a framework for studying the informational peculiarities of cybersecurity, the thesis mobilises inter-disciplinary literatures in the philosophy of information and information sciences - together with the closely related field of software studies which focuses on the social, cultural, and political impact of software (Fuller, 2008). The thesis also draws upon this literature to introduce three specific security logics as manifestations of the notion of entropy – negentropy, emergence, and noise – that make up this field of cybersecurity, and that challenge the logics of existentiality, exceptionality, and

emergency measures as presented in securitization theory. In addition, the thesis also draws upon literatures on new materialism to problematise the question of materiality and agency in the study of cybersecurity.

This novel inter-disciplinary theorisation will then be illustrated in relation to cybersecurity discourses and practices in the USA between 2003, when the country's first cybersecurity strategy was announced (The White House, 2003), until the end of the Obama administration in 2016. Multiple cybersecurity policy documents issued by the government are analysed, in addition to congressional hearings, in which several non-state actors testify, including members of the private sector, security experts, academics, and think tanks. This multi-actor approach fills a gap in the state-centric cyber securitization literature, as explained earlier. Further, widening the scope of analysis to include non-state actors allows for an understanding of mundane cybersecurity beyond the existential, the exceptional, and the high-profile cyber incidents that are more evident in the military and intelligence discourses.

Although the research question is not case-specific, focusing the research design on analysis of one in-depth case study is intended to increase the coherence of the results and facilitate the research process, particularly given the extended timeframe and the multi-actor approach used. Several reasons drive the selection of the USA for this case study. Firstly, it is the case study used in the majority of the existing cyber securitization literature to date. This will enable the thesis to tease out how an alternative theoretical approach to the same case on the same topic can produce different - but not necessarily contradictory - insights. Secondly, it is in the USA that the majority of the 'cyber' technologies originated and developed and where the key cybersecurity debates started. Thus, if an alternative theoretical framework to studying cybersecurity is to be developed, the analysis of the US case would be fundamental. Finally, the theoretical hypothesis of this thesis also requires an extensive analysis of cybersecurity discourses and practices of multiple actors over an extended period of time; and the ready availability of a vast amount of cybersecurity-related data in the USA therefore makes it an ideal case study.

The principal official policy documents analysed include those issued by the White House: *Cybersecurity Strategy* (2003), *Cyberspace Policy Review* (2009),

Comprehensive National Cybersecurity Initiative (2010), *International Strategy for Cyberspace* (2011), *Executive Order: Improving Critical Infrastructure Cybersecurity* (2013), and the *Presidential Policy Directive: Critical Infrastructure Security and Resilience* (2013). Added to this are documents issued by the Department of Defence (DoD): *National Military Strategy for Cyberspace Operations* (2006), *DoD Strategy for Operating in Cyberspace* (2011), and *DoD Cyber Strategy* (2015). And finally, the *Blueprint for a Secure Cyber Future* (2011) issued by the Department of Homeland Security (DHS). These are all the official strategy documents dealing strictly with cybersecurity. They were issued by those entities during the study period (2003-2016) and can be retrieved via their official websites. Given the vast amount of congressional hearings that deal with cybersecurity-related issues, the thesis only focuses on those that include 'cybersecurity' or 'cyber' in their title, in two committees: the Committee on Homeland Security in the House of Representatives, and the Committee on Homeland Security and Governmental Affairs in the Senate. The total number of hearings used is fifty-four. The choice of these two committees is based on their direct link to cybersecurity policy-making process and their general security nature, rather than being sector-specific, which matches the scope of this thesis.

Together with the theoretical literature on information, the qualitative analysis of the empirical data represents an understanding of discourse and materiality as essentially intertwined. As Karen Barad argues in her theory of agential realism, discursive practices are not exclusive to humans (Barad, 2003, 2007). Discourse is not synonymous with speech acts, as suggested by the original securitization theory. Rather, discourse is the force that enables/conditions those acts. Thus, if cybersecurity is to be studied as an infosphere in a non-anthropocentric approach, the *intra-action* between materiality and discourses has to be considered. That is, as Barad puts it, discourses are material and materiality is also discursive (Barad, 2003, 2007). More on the relationship between discourse and materiality, as well as their methodological implementation in the thesis, will be discussed further in Chapter 3.

5. Thesis outline

The remainder of this thesis proceeds in six chapters. *Chapter 2* is a conceptual chapter that provides an overview of cybersecurity. It presents a brief historical account of the

evolution of computing and internetworking technologies, which constitute what we commonly refer to as 'cyberspace' – from the World War Two until the end of the Cold War. This account challenges the common and largely ahistorical approaches to studying cybersecurity by arguing that security has always been an integral part of the co-production of those technologies – as a context, generative force, and policy concern. It also shows how such information technologies evolved beyond the intentionality of their human inventors, which in turn influenced how their security was conceptualised in different historical stages. In addition to this historical background, the chapter also analyses the current state of conceptualising cybersecurity for further clarification of the concept and distinguishing it from other related but analytically different terms. This is followed by an examination of the main policy challenges that define the current debates on cybersecurity, both on the academic and policy-making levels.

Chapter 3 introduces the theoretical and methodological framework of this thesis. It lays the foundation for the theorisation of cybersecurity as an infosphere and the analysis of the peculiar nature of its securitization process. In doing so, the chapter combines security and risk literatures with two other strands of theoretical/philosophical literature: the philosophy of information and new materialism. Firstly, it employs new materialism to challenge the concept of agency and its relationship to human subjectivity in securitization theory. Accordingly, agency in the infosphere is approached as an interaction between a non-anthropocentric informational agent and a human securitizing actor in co-producing security. Secondly, the chapter critiques the under-theorisation of the referent object in the securitization literature, and hence, uses the philosophy of information to theorise for the peculiarity of information as the ultimate referent object of cybersecurity. Thirdly, the chapter challenges the way securitization locked the logics of security within existentiality, exceptionality, and emergency and instead theorises cybersecurity as a field of contingency that can be understood through the logics of negentropy, emergence, and noise.

Chapter 4 introduces the notion of entropy and explains how it can be used as a security analogy in cybersecurity. It uses the definition of entropy as uncertainty in information theory and disorder in cybernetics to analyse the indeterminacies of

information systems and their tendency towards disorder and insecurity. Theoretically, the chapter analyse uncertainty as a property of information's existence that cannot be reduced to the empirical challenge of 'not knowing'. In practical terms, the chapter investigates the multiple sources of uncertainties in the operation of digital information systems and the kind of challenges they pose for cybersecurity policies, which the chapter calls the *entropic space of cybersecurity*. This includes the uncertainties associated with vulnerability analysis, intrusion detection, attribution and damage analysis, and the lack of technical knowledge about such systems. Finally, the chapter examines how such properties co-produce a specific perception of security in the infosphere that is primarily entropic, in which defence is more accurately described as *anti-entropic practices* aiming at *negentropy*; i.e., negative entropy.

Chapter 5 examines the agential capacities of information, particularly in its syntactic form (codes/software). It shows how such capacities challenge the idea of human control that is central to the logic of emergency and exceptionality in securitization theory. In view of this, the chapter employs the concept of *emergence* as introduced in complexity theory and as one definition of entropy in order to capture the agential role of information and the limits of human control in cybersecurity. To do so, the chapter explores agency as an intrinsic property of the ontology of information, whose peculiarity distinguishes information from ordinary matter or other non-human things. It investigates various theoretical approaches to defining agency in information sciences, particularly in software and digital studies. In addition to this theoretical exploration, the chapter examines the elements of autonomy and unpredictability in the actual operation of codes/software, and how they are capable of granting agency back to both humans and other objects. These agential capacities are further analysed with application on cybersecurity discourses and practices, in which *the logic of emergence* can be traced in the construction of enmity and co-production of the subjects and objects of security.

Chapter 6 turns towards the third ontological peculiarity of information - its simultaneous physicality and non-physicality - and considers the implication of this (non-) physicality for the logic of existentiality as introduced by securitization literature. The chapter investigates the different ways the physical and non-physical in digital

information systems interact, change, and define one another. It further demonstrates the various security and privacy concerns that this complex (non-)physicality engenders, in regard to the geolocation of data centres, data routing, undersea fiber-optic cables, and hardware/software manufacturing. Moving from general security implications, the chapter analyses the role of this (non-)physicality of information in co-constructing the *logic of noise* that accentuates *mundane* cybersecurity in face of the existential. The chapter shows how this property of information is capable of reducing existentiality to being just *another* discourse in cybersecurity and co-producing discourses and practices activated by the logic of noise, in which cyber threats are portrayed as urgent and immanent, albeit not existential.

CHAPTER (2)
THE CO-PRODUCTION OF CYBERSECURITY: CONCEPTUALISATION AND HISTORICAL OVERVIEW

Introduction

When the Copenhagen School's securitization theory widened the concept of security to include non-military sectors, it focused on identifying their referent objects, agendas, and logics of threats and vulnerabilities as the main elements of contestation in conceptualising security, rather than their subject matter (Buzan et al., 1998). This is understandable, since defining what the 'military' is in military security, the 'economy' is in economic security, or the 'environment' is in environmental security is a reasonably straightforward task, given the long-standing resonance of those terms. The same does not apply to cybersecurity, however. Due to its novelty, technicality, and multi-disciplinarity, what exactly the 'cyber' is in cybersecurity remains quite vague, making the whole concept of cybersecurity comparatively far elusive. Any attempt to theorise this field therefore requires an exploration of the different ways it can be conceptualised and an answer to a very straightforward, yet paradoxical question: what is cybersecurity?

In most academic studies, the story of cybersecurity is often told as a fairly new one that dates back to the 1990s, when the term was first used in US policy circles, after being coined in a science fiction short story called 'Burning Chrome' by William Gibson in 1982, followed by his novel 'Neuromancer' in 1984. Consequently, the cyber securitization literature usually takes the 1990s as a starting point to trace the process of securitizing 'cyberspace' (see Bendrath, Eriksson, & Giacomello, 2007; Dunn Cavelty, 2008b; Hansen & Nissenbaum, 2009; Lobato & Kenkel, 2015). Implicitly, this suggests that cybersecurity initially emerged as a non-security sector, which then subsequently became discursively *securitized*. Although it is true that 'cyberspace' and 'cybersecurity' were novel terms at that period, their ontological status cannot be reduced to such mere discursive utterances. Tying the existence of cybersecurity to human discourses alone would be ahistorical and is one reflection of anthropocentrism in conceptualising 'security' and security 'sectors'. If the security of 'cyberspace' as a constructed metaphor ultimately signifies the security of digital information systems, i.e., computers and

networks, with all their associated software, hardware, and data - technologies that possess long historical roots - then such an ahistorical approach to studying its evolution would be both insufficient and over-simplified.

This chapter argues that the historical process of constructing cybersecurity has, in fact, always been a process of *co-production*, in which human intentionality has been just one among many other constitutive elements. This applies both to the evolution of the computing and inter-networking technologies that constitute what is commonly referred to as *cyberspace*, and the conceptualisation of the essence of their *security*. This chapter thus seeks to demonstrate that the history of 'cyberspace' should be analysed as a complex process of restructuring, not just technically, but also politically and socially, in which the interests of various actors competed, and security considerations were intertwined with technical ones, and in many respects co-produced them.

Co-production is an idiom used to contextualise the production of scientific knowledge away from the deterministic, mono-causal approaches of its natural or social development. It is used in Science and Technology Studies (STS) literature to analyse several aspects in the development of science and technologies, including: the emergence of new objects and their stabilisation, intelligibility and mechanisms of transporting ideas, and cultural practices that legitimise such ideas and assign specific meanings to them (Jasanoff, 2004, pp. 5–6). Although 'co-production' is not explicitly an inquiry about agency, it can still enable us to broaden the concept of security away from the dichotomy of the human vs. the non-human. It allows for an understanding of technological development as a processes of intra-action between discourses and materialities as two non-antagonistic constitutive forces (Jacobsen & Monsees, 2019).

Accordingly, in answering the question *what is cybersecurity*, this chapter presents a historical overview of the development of the 'cyber' technologies and the conceptual evolution of their security since the emergence of the first computer, following the end of the World War Two (WWII), until the advent of the internet. It aims to show how computing and internetworking technologies as information systems evolved in ways that were not envisioned by their human inventors, which in turn influenced how their security has been conceptualised in different stages. As argued by

some studies in STS and digital humanities, information-based systems are more flexible and malleable than other technologies, and their usage seldom depends solely on their deliberate design. Those information artefacts are co-produced across a long period of time in cumulative processes, developing into “complex and recalcitrant textures”, that are not just linked to their users’ agency, but also to their own (Kallinikos, 2010, pp. 12–19). The chapter extends this argument to the construction and co-production of those systems’ *security*.

This chapter is thus more than just an endeavour to define cybersecurity and give a brief historical overview of its evolution. It is also an attempt to counter the anthropocentrism in studying cybersecurity by showing how the historical development of cyber technologies, and their attendant security policies, were not entirely as planned by their human inventors. It also shows that security was not imposed on ‘cyberspace’ by political discourses, but has actually been intrinsic to the existence of its components and technologies. To make this argument, the chapter starts with a brief historical exploration of the security context of the Cold War and how it influenced the development of science in general, and computing and internetworking research in particular. It highlights the generative influences of security considerations on the evolution of computers and the internet through the funding power of the military and its role in creating a market demand that shaped the supply of both technologies. The second section investigates the historical roots of computer and network security and how their conceptualisation had been evolving from concerns over physical security and unauthorised access to the fear of malicious hacking and malware. Finally, the third section examines the current state of conceptualising cybersecurity, both on the academic and policy levels. It engages with other concepts that have strong links to cybersecurity, particularly ones that use information-based terminology, for conceptual clarification and delimitation. The chapter ends with an analysis of the cyber threat scope and the most significant policy challenges that dominate the current debate on cybersecurity.

1. Security as a context and a generative force for the co-production of ‘cyberspace’

In one form or another, security has always been an integral part of the development of 'cyberspace': as a context in which it was developed, as a generative force behind many of its technologies, and as a policy concern in different phases of its evolution. Considering cybersecurity to be a completely new security challenge is problematic, since it overlooks the long history of interventions to achieve the security of computer networks and all the technologies associated with them (Ellis & Mohan, 2019, p. xviii). To illustrate this point, this section focuses on the evolution of computing and internetworking technologies since the end of WWII until the advent of the internet. Although some roots of 'cyberspace' or cyber technologies can still be found in the development of other electronic devices before the war, like punch cards (Heide, 2009), computers and networks are chosen as a starting point given their clearer links to the sort of modern cyberspace that we experience nowadays (Kello, 2017, p. 3).

Studying the history and development of cyber technologies (computers and networks), along with their complex processes of co-production, cannot be done in isolation from the wider security context of the Cold War. That is because the Cold War had far-reaching implications on the course of scientific research as a whole, and the military-civilian partnerships that were formed to advance it. During that period, WWII was framed as a 'scientific war' won by technological advancements achieved through the military's collaboration with academia, especially given the decisive role of the atomic bomb in ending the war and of the radar in winning it (Campbell-Kelly et al., 2014, pp. 65–85). There was a strong belief in both the USA and the Soviet Union that science could still win the Cold War for one of them. Consequently, advancement in science and technology became an integral part of their national security strategies (Wolfe, 2013, pp. 2–6).

Together with the fear from an apocalyptic conflict with the Soviet Union (Chernus, 2008), this discourse contributed to raising the research and development (R&D) budget even higher than the war time, with the biggest share coming from the armed forces. Even after the National Science Foundation (NSF) was established in 1951 as a civilian institution to aid research, only 20% of computer research for instance was funded by it, while 50-70% received funds from the Department of Defence (DoD) (Edwards, 1997, pp. 56–60). That is what Eisenhower famously referred to as the

'military-industrial complex' (Eisenhower, 1960, pp. 1035–1040), and others called the 'military-industrial-academic complex' (Leslie, 1993).

One important institution that performed a significant role in this regard was the Office of Naval Research (ONR). Established in 1946, ONR was the first military agency to finance basic, unclassified research in academic and industry laboratories. Since it was the only federal agency to finance research immediately after the war, the ONR used its contractual authority to shape science policies, by selecting the fields, institutions, and individuals to be funded. Security imperatives were a major consideration for the ONR's contracts, particularly after the 1950s, with the rising congressional pressure to prove the relevance of research to national security and defence purposes (Sapolsky, 1990). The Advanced Research Projects Agency (ARPA) was another institution that influenced the post-war scientific research, particularly in fields like networking. ARPA was established in 1958, as a research agency affiliated to the DoD, following the surprising launch of the Sputnik satellite by the Soviet Union. Sputnik fostered the fear from a growing scientific gap that could allow the Soviets to attack the USA with ballistic missiles.[9] Consequently, ARPA was established with the responsibility of keeping the USA more technologically advanced than its adversaries and preventing any surprising events like Sputnik (Hafner & Lyon, 1998, p. 20).

It could be argued that ONR and ARPA were products of existing processes of scientific and technological co-production, mediated in part by discourses of the scientific gap and the fear from a Soviet attack. They were also a co-production agent that actively shaped the post-war scientific research, combining a complex set of scientific and military interests. This collaboration between the military and academia was legitimised by the security context of the Cold War. Many scientists were advisers to the government and advocated the increasing military spending on 'basic research'. Some even adopted a 'two-title policy' for their research: a scientific title and a military-relevant one. An example for that was the scientific research on computational

[9] The establishment of ARPA was also partially influenced by the Korean war (1953-1956), which led to lifting the spending cap Truman put on military research, and starting a remobilisation process of science to achieve military goals (Forman, 1987, p. 158).

machines, which was re-oriented to be a research on command and control systems to suit the military interests (Sapolsky, 1990).

1.1. The evolution of computers: from calculating devices to networked information appliances

> "I think there is a world market for maybe five computers." - Thomas J. Watson, IBM chairman, 1943 (Hempell, 2006, p. 9)

The academic literature on the history of computers and networks is full of scientifically deterministic approaches that present an idealistic image of their development, by focusing on the success stories of their individual inventors (for example, see: Hafner & Lyon, 1998; Lavington, 2012). Very few literature acknowledge the influence of the DoD and security considerations (for example: Edwards, 1997), and how such technologies themselves had agential roles in their development. A closer analysis of the evolution of computers and networks reveals that their development path was unanticipated by their initial inventors. Computers started as calculating devices in the 1940s, and kept changing until they became a 'networked information appliance' by the 1990s (P. E. Ceruzzi, 2003, pp. 1–12). The same applies to the internet, since the first network that resembles today's internet, the ARPANET, was designed initially to facilitate resource-sharing among academics, not interpersonal communications (Abbate, 1999, pp. 1–5). Yet, this should not lead to a conclusion that such unplanned processes were necessarily *accidental*, and consequently undermine the analysis of their socio-political context. As Jasanoff argues, "The design of technology is likewise seldom accidental; it reflects the imaginative faculties, cultural preferences and economic or political resources of their makers and users" (Jasanoff, 2004, p. 16).

Generally speaking, the history of computers can be linked to the evolution of information machines since the industrial revolution. The revolution brought about a growing need for information processing through technology, and resulted in the invention of typewriters, accounting equipment, desk calculators, and punched cards. Yet, the direct roots of modern computers can be more precisely found in WWII and the military's need for breaking adversaries' ciphers, creating tables for artilleries, and conducting ballistic calculations (Campbell-Kelly et al., 2014, pp. 54–59). From the 1940s until the 1960s, the US military was the main driving force behind technological

developments in computers, not just through funding as part of the government's grand strategy during the Cold War, but also by being the main customer for computer products. Even though most computer research was conducted by universities and commercial laboratories, it was funded by the military and guided by its needs.

The first instance of the generative force of security in the development of computers goes back to the Colossus: the first electronic computer that was developed in 1943 by scientists contracted by the British government to decrypt adversaries' ciphers. Although the foundational idea behind digital computers was published in 1937, only the defence purposes of the war stimulated its application (Randell, 1982, pp. 349–354). The emergence of electronic machines gave rise to several computer-related disciplines, including cybernetics and artificial intelligence. It was also transferred to other military applications, such as communication, intelligence, and command and control (Edwards, 1997, pp. 16–20).[10] Together with the Bombe - a machine developed to break the German cipher device called 'Enigma' - the Colossus sparked several computer projects outside the UK. This happened particularly in the USA, which took the lead in advancing computer research following the end of the war (Randell, 1982, pp. 349–354).[11]

Another machine that was generated out of the security imperatives of the war was the Electronic Numerical Integrator and Computer (ENIAC). The need for automated ballistic calculations for the army encouraged the development of ENIAC, financed by the Ballistic Research Laboratory (BRL), an army affiliate (Burks, 2014, p. 314).[12] If it was not for the security needs of the war, the ENIAC might not have been developed, as it was rejected and deemed as overly radical by the scientific community at that time (Flamm, 1988, pp. 47–48). The BRL continued to finance the development of the ENIAC into the EDVAC (Electronic Discrete Variable Automatic Computer); another military

[10] Computer science as a discipline first appeared in the 1950s as part of mathematics and electrical engineering departments. All through the 1960s, there were some challenges in defining what it is as a discipline and demarking and delineating it (P. E. Ceruzzi, 2003, pp. 89–108).

[11] For more details on the comparison between the state of computing research in the USA and the UK and reasons behind the US lead, see (Bowles, 1996).

[12] The ENIAC was not the first attempt to develop electronic computers; it was preceded by other efforts, not just in the USA, but also in Germany and the UK. However, these had little impact on the development of modern computers. Additionally, the ENIAC was more complex and developed than all other electronic systems back then (Campbell-Kelly et al., 2014, pp. 65–85).

machine created to aid in a variety of tasks, including the development of a hydrogen bomb. The EDVAC marked the birth of internal programming, unlike the ENIAC which was externally-programmed (Watson, 2012, pp. 91–92). The ENIAC and the EDVAC presented one big step in the history of government's support of 'big science', especially that the amount of money these projects required was beyond the capacity of the private sector (Edwards, 1997, pp. 49–51).

Furthermore, the security needs of the military encouraged a sceptical private sector, that did not initially acknowledge the importance of electronic computers, to get involved. For instance, the International Business Machines Corporation (IBM), which later dominated the commercial production of computers, was reluctant to enter the market until the military needs during the Korean war pushed it to develop a computer called 'IBM Defence Calculator' or '701', sold to the military (Flamm, 1988, p. 64). The ENIAC and EDVAC also gave boost to Project Whirlwind, which was started by MIT to create a flight simulator for pilots training for the air force. Following the end of the war, it was integrated in the new computer-controlled air defence system, called the Semi-Automatic Ground Environment (SAGE). The sophistication of SAGE led to the development of various technologies that shaped today's computers, such as real-time computing, modems, and video and graphical displays (Agar, 2012, pp. 375–376).

Programming languages were another significant milestone in computer development, owing a lot of their success to the military. Two main programming languages were developed since the start of the 1960s: Cobol and Fortran. Fortran was introduced by IBM and proved successful because of IBM's domination of the market (P. Ceruzzi, 2012, p. 61). On the other side, though it was a business-oriented language, the DoD not only pushed for the development of Cobol, it also encouraged its standardisation by announcing that 'it would not lease or purchase a computer without a COBOL compiler' (Vee, 2017, pp. 108–109).

Gradually, the usage of computers started to broaden, as the technology showed potential for much more than military needs. Many computer amateurs began to view the idea of having affordable mini-computers for personal use as an important step towards human liberty. This encouraged several entrepreneurial start-ups to enter the market of personal computers, starting with Intel's development of the

microprocessors, often regarded as 'the enabling technology for personal computers'. It was followed by the production of Altair 8000, the first version of a personal computer, in 1975. This accelerated the process of software production by various companies, such as Apple and Microsoft. And then computers became cheaper and affordable for non-military and non-business users, accompanied by the development of the World Wide Web (WWW) (Campbell-Kelly et al., 2014, pp. 222–251).

1.2. The evolution of the internet: from resource-sharing to communication platform

There are two main narratives in the literature on the development of the internet: one that presents it as an entirely technical project that evolved through spontaneous, unplanned processes (for example, see: Hafner & Lyon, 1998); and one that claims the network was developed just to maintain the robustness of military communication in case of a nuclear attack (for example, see: P. Siegel, 2008, p. 531). Approaching the internet evolution as a co-production process, however, leads to a more complex conclusion that lies in-between the two narratives. The development of the internet can be described as an 'organised chaos', produced by the overlapping interests of ARPA, NSF, programmers, developers, and even users (Marson, 1997, p. 36). Both military and academic interests contributed to the evolution of a civilian internet, while corporate networking was initially sponsored by the state (Murphy, 2002, p. 32).

Although the first network that resembles today's internet, the ARPANET, was not developed as a military network, the technology upon which it was based was generated out of security considerations. ARPANET was enabled by packet-switching, originally developed in the 1960s to secure the survivability of military communications by distributing them among different nodes to survive on redundancy in case of a strike (Ryan, 2010, pp. 11–22).[13] However, the radical nature of the idea hindered its immediate application. Only in the 1970s when ARPANET was created did packet-switching appear as a sound foundation for networking. ARPA financed the ARPANET

[13] Packet-switching works by breaking up a message into a series of 'packets', each with origin and destination labels. Those packets travel through the nodes in the network, choosing among multiple alternative paths based on efficiency or availability, until they are finally re-assembled at the destination. Thus, the disruption of any node does not impact communication's survivability, since packets can be always re-routed to an alternative path (Aksoy & DeNardis, 2007, p. 280).

project as the first version of a distributed network to allow its contracted academic institutions to remotely share their expensive computers (Brendon, 2001). Nevertheless, though it was not a military network, ARPANET was used for seismology and defence-oriented climate research. Also, it was not entirely an academic network, given the participation of the Army and the Air Force (Abbate, 1999, pp. 36–41).

Security needs also encouraged the application of packet-switching to two communication technologies used by the military in the 1970s: radio and satellites. A network called PRNET was established by ARPA to secure the military's command and control through radio packets; and another one under the name SATNET was created for the transfer of the military's seismic data. The existence of three heterogeneous networks - ARPANET, PRNET, and SATNET - and the need to connect them stimulated the development of the internetworking protocols TCP/IP as one cornerstone of the modern internet's architecture (Ryan, 2010, pp. 31–44). Furthermore, the military had an important role in the expansion of the network by obliging academic institutions contracted by ARPA to join it and mandatorily implement TCP/IP, despite the resistance of some to the idea of resource-sharing and internetworking (Ruttan, 2006). Additionally, the military's interest in a tightened security system for authentication and information-sharing was a first step towards the civilian internet. This was done by breaking the network down into two separate ones: a military network, MILNET, where a strict security system was implemented, and ARPANET continuing as a research network, and thus facilitating its expansion in the 1980s (Abbate, 1999, pp. 142–145).

The final and most critical step in opening the internet to the public was the privatisation of its backbone and the permission of its commercial use. The internet privatisation was neither easy nor inevitable, and was influenced by several technical, social, and political aspects, as well as the security considerations of the Cold War. It was facilitated by the US national security strategy, and the perceived scientific gaps between the USA and other international actors. This period witnessed wide congressional debates on funding supercomputers and networking, particularly in 1982, after Japan launched a project to supersede the USA in artificial intelligence research. Consequently, data networking became an integral part of the national policy agenda, and the Congress endorsed the public access of the internet. This all facilitated the

process of privatising the internet's backbone, which was completed by 1993 (Abbate, 1999).

In fact, many of the current debates on internet governance and security have their roots in this privatisation process, since it was not very carefully planned. For instance, following the privatisation, the NSF ruled out the backbone commercial providers from the jurisdiction of the Telecommunication Act, which regulated the activities of traditional communication carriers. The NSF did not put in place an alternative framework to prohibit discriminatory behaviour by those carriers. The absence of such framework resulted in many problems that are evident in the current struggle over net neutrality in the USA.[14] In addition, the NSF did not impose any security requirements on backbone commercial providers, nor did it put any alternative arrangements for the security of the civilian internet after separating it from the military network. Thus, it could be argued that many internet security challenges are not the result of security being an afterthought in the development of the internet, but of the absence of an adequate preparation for the transfer of the internet's administration to commercial providers and for scaling it up (Shah & Kesan, 2007, pp. 100–105).

To summarise, the internet was neither just an academic project developed purely out of the enthusiastic ideas of its creators, nor was it entirely a military-oriented invention. The military's support, both in providing funds and creating a market demand, proved crucial in the evolution of the internet, starting from the early days of ARPA's adoption of packet-switching, to the development of the new technologies of satellite and radio switching. This all happened despite of a sceptical academic community. Moreover, the diversity of the military operations produced a philosophy of decentralisation and heterogeneity in dealing with the network, as opposed to the industry's sponsored centralisation (Hicks, 1998). Hence, the co-production of the internet combined "the desire for cutting-edge research, openness of information, and adaptability to military needs" (Abbate, 2001, p. 150).

2. Security as a policy concern: from computer and internet security to cybersecurity

[14] For more information on the net neutrality debate, see (Hart, 2011; Krämer et al., 2013; Pickard & Berman, 2019).

As a policy concern, the security of computers and networks has long historical roots that can be traced back to the introduction of the very first computer, even before the emergence of networks, malicious hacking, or malwares. At each stage, this security was conceptualised differently, with diverse threat perceptions, referent objects, and utterances that reflect the technology's development state. In its early stages, computer security was shaped by the military, the same way computer research and industry were influenced by its interests. The DoD played an influential role in setting the security standards that governed early computer systems. This role diminished later with the increasing involvement of corporate actors, and even individuals, in the field of computer security. In these initial stages, and before the evolution of internetworking, computer security was mainly centred on three main issues: physical security, unauthorised access, and software bugs. Such threats defined what constituted a 'computer crime' at that time, upon which legal frameworks were shaped. This conceptualisation of security reflected a belief in the controllability of machines, i.e., threats are external to machines and are calculable and controllable, and therefore defendable.

2.1. Physical security, unauthorised access, and software bugs

Following the end of WWII, the military was concerned about the security of its computer systems against physical attacks, theft, or natural disasters. As a result, computers' physical security became an integral part of the general security of military installations. Among the early perceived threats were the electronic radiations emanating from mainframe computers, that allowed spies to decipher communications over computer systems (Yost, 2007). To deal with the issue during the 1950s, the government announced its first security standards for emanation levels, called TEMPEST, and the DoD obliged vendors to abide by them before they could sell any computer equipment to the government (Russell & Gangemi, 1991, p. 37). Computers were also surrounded by containers to act as physical shields. Computer sabotage and manipulation did exist at that time, but were mainly physical and performed by insiders (Brenner, 2007, p. 706).

The growth of time-sharing in the late 1960s, in which multiple users can share computer resources simultaneously, was perceived as an additional threat that could

intensify unauthorised access. Therefore, RAND Corporation and the System Development Corporation (SDC) prepared what was known as the 'penetration studies' to identify vulnerabilities in time-sharing and resource-sharing systems. Additionally, a task force was established by the Defence Science Board in 1967, combining RAND researchers, defence contractors, scientists, NSA and CIA officials, to examine ways through which the computer security standards of military environments could be applied to open environments. This task force produced a report in 1970 to examine the responsibilities of the computer industry in producing secure systems, which was also the birth of many cybersecurity terminologies that are used nowadays, such as vulnerabilities, threats, trap-doors, dependabilities, certifications, among others (Meijer et al., 2007, p. 641).

With resource-sharing also came the concerns over data privacy, which was what computer security was all about in technical literatures at that time (for example: Ellison, 1978; G. Wiesel, 1973; Reddy, 1979; Winkler & Danner, 1974). As a result, cryptography started to gain ground as an essential component of computer security, and the National Bureau of Standards announced, for the first time, the 'national standards for cryptography'.[15] Many companies, especially in the banking and petroleum sectors, invested heavily in encrypting their communications. For instance, IBM's spending on computer security reached 40 million dollars over a period of five years, and a major part of it was directed to cryptography research (Yost, 2007). Another important security concern in that period was software bugs: errors in coding. Prior to 1965, programming was done in closed environments and only programmers had access to written software. But as more people were getting involved in the process of software design, program correctness or fixing buggy software became an independent field of computer security research in 1974 (Meijer et al., 2007).

Nevertheless, concerns over unauthorised access and software bugs did not overshadow physical security as a perceived threat to computer security, even with the rise of phone phreaking in the 1970s, or hacking into phone systems for conducting free

[15] The National Bureau of Standards is a non-regulatory agency in the Commerce Department in the USA. It was later renamed The National Institute of Standards and Technology (NIST) (*Guide to NIST (National Institute of Standards and Technology)*, 1997).

phone calls.[16] This is because the majority of security breaches to computer systems back then were primarily physical attacks. Examples include: the 1970's bombing of computer sites at the University of Wisconsin and New York University, the 1973's shooting of a computer in an American firm during protests in Australia, and the destruction of an IBM computer at Vandenberg Air Force Base in California in 1978 (Easttom, 2011, p. 38).

On the legal and policy side, there were some attempts to face the rising threat of computer crimes, defined at that time as any physical destruction or unauthorised access to computer systems. This includes the Federal Computer Systems Protection Act, introduced in the Congress in 1977.[17] Though it was not adopted, it marked the first step towards recognising the security aspects of computer systems by the legislature (Easttom, 2011, p. 38). Computer security was also acknowledged by the General Accounting Office, as one of the legislative agencies that provide services to the Congress. It issued multiple reports to the Congress recommending methods to combat any act that involved alteration of computer hardware or software, especially in federal computer systems, by employees or insiders (For example, see: The Comptroller General of the United States, 1976). Additionally, other reports suggested limiting the number of federal employees who deal with computer systems to overcome the threat of unauthorised access (Marion & Hill, 2016, pp. 62–122); and analysing the physical security of computers against threats of fire, bombing attacks, among others (see: The Comptroller General of the United States, 1976b). The first actual law to be adopted in this regard was the Florida Computer Crimes Act in 1978, which criminalised all forms of unauthorised computer access, even if it did not involve any malicious intent, which was seen as a radical move at that time (Casey, 2011, pp. 35–36).

Yet, despite this increasing attention from the government and security practitioners, very limited knowledge about computer security was available to the general public at that time. The majority of news articles discussing computer systems mainly referred to their use in various settings, such as criminal courts ('Crime

[16] The most famous case of phone phreaking at that time was John Draper's or Captain Crunch case. For more information, see: (Schwabach, 2014, pp. 192–193).

[17] This bill is sometimes called the Ribicoff Bill after the senator who introduced it.

Computers', 1977), or in exchanging information among law enforcement agencies (Babcock, 1977), not their security. Those articles that focused on the security aspects of such systems were concerned with what they referred to as 'white collar crimes' in businesses, or the misuse of computers by employees to achieve financial gains (Kramer, 1977, 1978). Very few articles discussed topics like unauthorised access or data privacy ('HEW Computer Security', 1977).

2.2. Malicious hacking and malware

During the 1960s and 1970s, hacking was approached positively, as part of the process of developing computer technologies. Because computers were not commonly used and only accessed by researchers or military personnel, hacking was not widely known outside the computer science community. Even when hacking took place, it was done by students or computer programmers for exploration purposes. It was not associated with any malicious intents and was not subject to any sort of punishment (Marion & Hill, 2016, pp. 62–122). However, the emergence of networking, the commodification of information, and the 'digital fences' implemented in computer systems with increased privatisation, created a 'cyber e-capital' that required protection. Therefore, the hacking culture started to be met with resistance, and a distinction was made between hackers (explorers) and crackers (robbers) (Dyer-Witheford, 2002, p. 137).

Similarly, since the 1950s, the idea of self-copying and self-replicating programs was associated with the process of system design and development. Viruses and worms were part of the architecture of internetworking, as an essential tool for testing and experimenting the network. For this reason, even with increasing reports about computer viruses in the early 1980s, many security experts did not take them seriously and thought they were no more than an 'urban myth'. It took time for them to realise that viruses can go beyond being experimental programs towards malicious usages. Many incidents starting the 1980s played this role of shifting the emphasis to malicious hacking and malwares as a security threat to networks and computers.[18] This

[18] On 1983, a movie called 'War Games' caught the public's attention by displaying the seriousness of hacking as a security challenge. The movie showed a teenager hacking into the computers of the North American Aerospace Defence Command, and almost triggering a third world war (Kaplan, 2017, pp. 1–3).

transformed security conceptualisation in the field towards threats emanating from the machine, characterised by uncertainty and incalculability.

Examples include the first malicious virus to ever be reported in 1981/1982, that infected Apple II computer system; the 'Brain virus' that targeted Microsoft's DOS system in 1986 (Skoudis & Zeltser, 2004, pp. 17–18); Ian Murphy's, or Captain Zap, hacking into the AT&T computer system and changing the clocks (Brenner, 2007, p. 707); and hacking into the Los Alamos National Laboratory and the Sloan-Kettering Cancer Centre and stealing medical records by a group called 414 (Watson, 2012, p. 267). Arguably, the most important of all such incidents was the Morris worm in 1988, which is often referred to as the 'first internet worm' (Orman, 2003). This self-replicating worm, designed by Robert Morris, had a major influence in bringing internet security to the forefront of public attention and marking the beginning of denial of service attacks as significant cyber threats (Meijer et al., 2007).[19] It exposed the security vulnerabilities in the network, disabled many connected systems, and infected an estimated number of 6000 computers. Following this incident, a Computer Emergency Response Team (CERT) was established by the DoD, with the responsibility of coordinating responses in case of attacks, preparing security reports, and raising users awareness about computer and network security (DeNardis, 2007).

As those operations were becoming more frequent and sophisticated, legislation to counter them were also developing. The first federal legislation on cybercrimes under the title 'Computer Fraud and Abuse Act' (CFAA) was issued in 1986. Before this law was enacted, courts used to apply traditional laws on such crimes with flexible interpretations. It was also preceded by some other efforts, like the amendment of the Comprehensive Crime Control Act in 1984 to include crimes of unauthorised access to computer systems; efforts that did not sufficiently respond to the rising challenge of computer crimes. The CFAA protected computers of federal entities, financial institutions, and foreign commercial entities, against any unauthorised access of national security information, financial records, or any information held in federal departments or consumer reporting agencies. Subsequently, the law was used for the

[19] Denial of Service (DOS) attacks are those that flood a certain target with superfluous requests, which affects the target website's availability, by slowing it down or making it unreachable (Lee, 2013, p. 122).

first time in the conviction of Robert Morris in 1988 and Herbert Zinn in 1989, who broke into the DoD computer systems (Easttom, 2011, pp. 72–77).

Several publications in that period mirrored this rising concern over computer and internet security, such as the Orange Book, a report published by the DoD in 1983, creating a common language for communication over computer security (Yost, 2007). The academic literature of the 1980s also revealed this shift from physical security towards software and hardware vulnerabilities, and the belief in the uncontrollability of machines (Ames, 1980; Fine, 1982). Network security, in addition to computer security, started to be emphasised in multiple literature (Kak, 1983; Rutledge & Hoffman, 1986); as well as the security of particular networks, such as the military (Landwehr, 1981; Stillman & Defiore, 1980); and the challenges facing multi-user systems (Konheim, 1981; Oberman, 1983). By the late 1980s, more literature began to discuss the increasing risks of viruses and worms to network security (Gardner, 1989; Joseph, 1988).[20] Furthermore, there was massive news coverage on computer and network security in the 1980s. Computer security made headlines in various news articles, discussing system vulnerabilities (Bakke, 1983; Burnham, 1985; Doyle, 1984; Francisco, 1982); rising computer crimes (Mc Cue, 1983); and the insider threat (Fitzgerlad, 1984). They called for several measures to tighten computer security (Ahern, 1982; 'More Computer Security Needed', 1984), including the need for skilled computer specialists (Palma, 1980), good management (Hancock, 1981), and increasing public awareness (Byles, 1988).[21]

In conclusion, it could be argued that the military had a strong influence on advancing computing and internetworking technologies. But these technologies later evolved in complex, unplanned processes into their modern versions and usages, beyond the intentions of their creators. Further, security was not a political discourse imposed on 'cyberspace'. The security of cyber technologies is as old as those technologies themselves and can be considered an integral aspect of their evolution.

[20] It is important to note here, however, that the vast majority of literature on computer and network security at that time was part of the computer science or engineering literature, not social sciences.

[21] In 1988, the Time magazine published an important article on the significant implications of computer viruses that widely caught the public attention. This article was exceptional because it portrayed an image of total cyber insecurity by using biological metaphors that compared computer viruses with epidemics (Elmer-Dewitt, 1988).[21]

This, in turn, moves the question of securitization from whether cybersecurity is securitized or not, as discussed in the cyber securitization literature, towards an investigation of how and why it is securitized and in what contexts. Likewise, this argument blurs the line between securitization and desecuritization in the theory's framework and calls for a problematisation of the concept of security as such.

3. The current state of conceptualising cybersecurity

Although computing and networking technologies evolved historically within the realm of security, the same does not apply to the terms 'cybersecurity' and 'cyberspace'. The cyber terminology did not emerge first in a security context and there was no intention for it to be used in security policy-making processes. This produced a condition in which these two terms are used differently in different contexts, with little to no agreement on what they really imply or include (Futter, 2018). The wide disagreement on conceptualising cybersecurity and defining its core referent objects extends both to the academic and policy levels.

3.1. Conceptual delimitations

Cybersecurity, as argued by Dunn Cavelty, is a form of security that 'unfolds in and through cyberspace' (Dunn Cavelty, 2013, p. 107). Before migrating to academic and policy debates, the term 'cyberspace' first appeared in a science fiction short story called 'Burning Chrome' by William Gibson in 1982, followed by his novel 'Neuromancer' in 1984. The novel portrayed cyberspace as a 'consensual hallucination' and a virtual environment that is not 'real' (Betz & Stevens, 2013, pp. 149–150). The prefix 'cyber' itself though is linked to cybernetics, which Norbert Wiener introduced in the 1940s as the science of control and communication in the animal and the machine, with a specific focus on human-machine interactions (Wiener, 1948). Following Gibson's novel, a 'cyberpunk' culture started to develop, referring to a dystopian and futuristic style of writing. By mid-1990s, the term 'cyber' began to be used in policy circles in the USA as a catch-all-phrase that encompasses what was previously classified as 'information operations' and 'information warfare'. These operations included espionage, sabotage, communication fraud, and others that were revolutionised by informational technologies. But in Western discourses, the 'cyber' terminology signifies a specific link

to Computer Network Operations (CNOs): operations that have computer networks as both their attack tools and targets (Futter, 2018).

In academic literature, earlier demonstration of the concept of cyberspace reflected an understanding of it as a synonym of the internet, and thus limited to its virtual manifestation (Bieber, 2000; Jordan, 1999; Loader, 1997; Mody, 2001). However, as the concept began to gain ground in the literature, some studies diverted from this narrow perspective towards defining cyberspace as a 'construct' composed of multiple 'layers'. In this sense, cyberspace embodies a physical infrastructure (computers, cables, routers, and all hardware); a virtual layer, which is sometimes called 'code' or 'syntactic' level (programs, codes, protocols, and all software); and a 'semantic' or cognitive layer (ideas and information stored in the system). Some literatures also add a 'regulatory' level, of all the rules governing cyberspace, and a human level, related to individuals who deal with information systems (Applegate, 2015; Deibert et al., 2012; Libicki, 2007; McGuffin & Mitchell, 2014; Singer & Friedman, 2014). Accordingly, cybersecurity becomes all policies and tools undertaken to protect the cyber environment, with its virtual, physical, semantic, regulatory, and human components. Nevertheless, there remains broad disagreements on the relative importance of each of those 'layers' and the nature of threats they should be defended against.

Further, 'cyberspace' is sometimes portrayed as just another space in which the dynamics of other security sectors can be detected. This is reflected, for instance, in the way cyber threats are commonly approached by adding the 'cyber' prefix to conventional terms whose perception as threatening has long-standing resonance; such as cyber war, cyber espionage, cyber terrorism, and cyber crime (J. Carr, 2012; Goodman, Kirk, & Kirk, 2007; Singer & Friedman, 2014). All such terms are widely used, albeit with little demarcation or clear definitions. In these formulations, any cyber-induced targeted operation would be framed as an 'attack' that falls under one of these categories. The problem with this attack-based conceptualisation is that it neglects mundane, everyday cyber threats and other cyber operations that are considerably influential on the long-term functionality of systems, such as cyber exploitation, which remains under-studied (Dunn Cavelty, 2016, p. 93). As a result, a rather more pragmatic, technical approach is adopted by some scholars to classify cyber threats. Instead of using

'cyber attacks' as an all-encompassing category, they talk instead of CNOs that can take the form of computer network attack (CNA), computer network exploitation (CNE), or computer network defence (CND) (Brantly, 2014; Mazanec & Thayer, 2015). Rid also proposed classifying cyber threats into three categories: espionage, sabotage, and subversion (Rid, 2012, pp. 16–22).

However, many literatures are trapped in drawing comparisons between cybersecurity and other conventional sectors, in which the realities of those sectors control the perception of the cyber reality and determine its danger discourse. Some scholars assume that war, terrorism, espionage, and crime should have the same characteristics in cybersecurity as they do in conventional sectors, for them to be conceptualised as such. For instance, they adopt Clausewitz definition of war as violent, instrumental, and political to discard the possibility that war can take place in cyberspace (Lee & Rid, 2014; Limnell & Rid, 2014). According to them, only attacks that cause physical damage or massive destruction to the state's system can qualify as cyber terrorism (Stohl, 2007; Weimann, 2005). They assume conventional definitions of violence which is tied to lethality, and disregard how the serious implications of cyber threats on the social, economic, and political stability of societies may have transformed the concept of violence itself (Limnell & Rid, 2014; McGraw, 2013; Stone, 2013). In assuming cybersecurity is a realm into which other strategic agendas are extended, the extent to which logics and practices of cybersecurity may have actually transformed the concept of 'security' as such goes unexamined.

Hence, it could be argued that the prefix 'cyber' has become a buzzword (Futter, 2018), and the term 'cyberspace' has proven little relevance to socio-scientific analysis, even if widely used (Stevens, 2015, p. 74). Given this ambiguity of the cyber terminology, cybersecurity can be easily confused with other related but different concepts. This may include internet security, which is only one aspect, or 'layer', of what cybersecurity aims to protect. Another is internet governance, which is concerned with coordinating and managing the internet through IP address administration,[22] content regulation, copyright protection, technical standard formations, etc. (Mueller, 2010, p. 10). And

[22] An IP address resembles a home address. Every device on a network has a unique set of numbers that identifies it, called the IP address, and which allows it to interact with other devices on the network (Panek, 2019, p. 15).

although internet governance also includes security-related issues like protection against spam and cybercrime (Drake, 2005, p. 15), this is just a subset of what cybersecurity is about. A more intricate relation exists between cybersecurity and all concepts that use information-based terminology. For instance, cybersecurity is sometimes used interchangeably with ICT security. The key difference is that ICT security is commonly used to signify the security of information infrastructure rather than information as such (here to mean data), while cybersecurity combines both (Von Solms & Van Niekerk, 2013). This can be counter-argued, however, by acknowledging that the security of information and that of the infrastructure it is stored on are predominantly inseparable.

It is also common for information security to be used as synonymous with cybersecurity. Information security is defined in terms of the confidentiality, integrity, and availability of information (or data). Whereas cybersecurity is linked to computers and networks and takes place entirely in the digital realm, this is not necessarily the case in information security. The data that is the subject of protection in information security does not have to be stored on nor transmitted via digital devices; it can be written on paper and transmitted through verbal conversations for example (Von Solms & Van Niekerk, 2013). Here, it is important to note that sometimes using 'cyber' or 'informational' language constitutes a political choice that reflect conflicting interests among actors. For instance, the Chinese and Russian governments use terms like information security, information weapons, and information warfare to replace the Western or Anglo-American language of the 'cyber'. According to them, information security is not reduced to operations that use or target computer networks; it also includes propaganda facilitated by mass media in order to influence the politics of a certain country (Giles & Ii, 2013). This distinction does not mean, however, that a certain operation cannot be both a CNO and information warfare at the same time. An example for this is the hack against the US Democratic National Committee in 2016. This operation used and targeted computer networks, but also the data stolen was part of information warfare to influence the elections (Futter, 2018, pp. 210–211).

Yet, disentangling the two concepts of information security and cybersecurity does not deny the informational ontology of the latter. Cybersecurity is not synonym for

information security, but it is essentially informational. As defined by Dunn Cavelty, cybersecurity is "a multifaceted set of technologies, processes and practices designed to protect networks, computers, programmes and data from attack, damage or unauthorized access, in accordance with the common information security goals: the protection of confidentiality, integrity and availability of information" (Dunn Cavelty, 2014, p.89). This definition makes it clear that cybersecurity is distinguished by the *digital* nature of the tools and targets of cyber incidents, but these tools and targets are primarily manifestations of *digital information*. This *informational* essence of cybersecurity will be explained and substantiated further in the next chapter. For now, it suffices to say that the limitations of the cyber terminology that the thesis responds to are not reduced to linguistic utterances; they are rather theoretical and ontological. Studying the informational ontology of cybersecurity is therefore not a call for replacing the cyber terminology with informational language in policy debates or academic research. Rather, attending to information is a bid to reach a level of theoretical abstraction for analysing the foundation of cybersecurity, beyond the discursive usage of particular terms.

3.2. Policy challenges

By reviewing academic literatures that deal with cybersecurity strategies and policy challenges, certain topics stand out as the most researched and widely debated, while others remain largely under-studied. As is the case with disagreements on conceptualisation, moreover, analysing cybersecurity strategies reflect varying understandings of the nature of 'cyberspace' and cybersecurity and the relative importance of cyber threats. In this regard, the cybersecurity literature mostly explores some of the material conditions that affect cybersecurity, but within a policy-oriented and mostly anthropocentric framework. Generally, this literature can be divided into two main themes: one that studies the strategic and operational challenges of cyber offence and defence; and one that focuses on cyber governance, state sovereignty, and public-private partnerships (PPPs).

3.2.1. Offence/defence strategies and the cybersecurity dilemma

Many studies compare the relative usefulness of cyber defence and cyber offence as part of a cybersecurity dilemma that results in cyber insecurity for all states. Broadly speaking, ICTs here are instrumentalised and seen as tools for human actors, and mainly states, for achieving certain strategic purposes. Mostly, there is a broad agreement that cybersecurity is offence-dominated. This is explained, for example, by the wide attack surface and the fact that easy accessibility to information technology lower the barriers of entry for would-be cyber attackers (Clarke & Knake, 2010; Gjelten, 2013; Kello, 2013; Lynn, 2010). Nevertheless, few other studies provide a counter-argument by analysing the advantages of cyber defence, and the possibility of using anonymity and deception effectively in defending against cyber threats (Gartzke & Lindsay, 2015). They point out the higher costs and shorter life-cycle of offensive operations compared to defensive ones, in addition to the defence-favouring cybersecurity market (Rid, 2013a, pp. 167–169).

One important aspect in this debate is the attribution problem and its relation to cyber deterrence. The attribution problem refers to uncertainties in identifying the source of a cyber attack, the kind of damages it caused to the targeted system, and the offensive capabilities of adversaries (Mazanec & Thayer, 2015, p. 34). Together with the increasing developments in cryptography, these uncertainties make the application of traditional deterrence theory on cybersecurity quite problematic. However, some studies argue that deterrence is still possible and have already been done successfully in many cases (Rid & Buchanan, 2015). For instance, Nye argues that cyber deterrence can still be achieved through the threat of punishment; defence and resilience that denies the attacker's advantage; interdependencies that raise the cost of the attack; and finally dissuasion by norms and threats to the state's soft power (Nye, 2017). This distinction between offensive and defensive operations is surpassed by other scholars who argue that cyber intrusions and exploitations can be used as a method of state defence. According to them, these 'defensive operations', conducted mainly for espionage purposes, can be misinterpreted by the targeted states (Buchanan, 2016b), and thus render the offence-defence balance debate obsolete (Huntley, 2016).

Nonetheless, the implied assumption that the line between offence and defence is now blurred should be approached with caution. Although states may conduct cyber

intrusions with defensive motives in the background, it is arguably problematic for academic literatures to deal with them as such. Just because an intrusion does not disrupt or cause damages to the target, does not mean that it is not offensive in nature. Such intrusions are still unauthorised and rely on the use of malware, which is commonly viewed as the 'cyber weapon'. Hence, some studies started to discuss the relationship between cyber espionage performed through CNIs on one side and international law and international cyber norms on the other (Georgieva, 2020; Hurel & Lobato, 2018; Sabbah, 2018; Mačák, 2017) This is important particularly given the complex interdependencies of cybersecurity and the fact that withholding information about the targeted vulnerabilities to be used by the state could eventually affect the security of everyone. This risk intensifies if we consider the materiality and agency of information as such and the challenges they pose to the idea of human control implicit in such understanding of 'cyber defence' – as will be further explained in the next chapters. For example, a malware used in targeting a certain system can spread to untargeted ones, even within the geographical location of the initiator, and result in several unintended consequences. Hence, there is a risk of condoning such operations by labelling them 'defensive'.

3.2.2. Cyber governance, state's sovereignty, and PPPs

Another approach to studying cybersecurity policy challenges is one that focuses on the issue of governance and the question of state sovereignty in a multi-stakeholder cyberspace (Cornish, 2015; Ronald J. Deibert & Crete-Nishihata, 2012; Shackelford, 2014). On one side, states try to maintain control over cybersecurity through militarisation, nationalisation, and other measures that may impede effective governance (Choucri & Clark, 2013; Fliegauf, 2016; Slack, 2016). For example, some studies criticise the growing cyber budget of the Pentagon and the influential role of the US Cyber Command (Lee & Rid, 2014); the Cold War and nuclear deterrence analogies used in cybersecurity policy discourses (Lawson, 2012); and the securitization of intellectual property theft to justify the government's measures of internet control (Halbert, 2016). However, on the other side, state sovereignty is also increasingly challenged in cybersecurity. One manifestation of this is cryptography, which relatively protects citizens privacy, but at the same time provides anonymity to criminals and

terrorists by encrypting their communications and facilitating network breaches (Moore & Rid, 2016). Moreover, with increasing encryption, intelligence services and law-enforcement agencies find it difficult to track citizens' communications. Encryption is even making corporations 'technically-prevented' from complying to states' demands for tracking users' activities (Buchanan, 2016a).

Relatedly, one of the most controversial issues in cybersecurity is the power dynamics between states and private actors, or the public-private nexus. Given the multi-stakeholder nature of cybersecurity, any successful strategy or policy would depend on effective partnerships between public and private actors. However, there are various impediments that complicate PPPs in cybersecurity, particularly in regards to managing CNIs. There is an incompatibility of interests between a state that perceives cybersecurity as a public good and a national security issue, and a private sector operating under profit-oriented business models.

This problem crystallises in the information-sharing dilemma in cybersecurity. Early warning and attack alerts in cybersecurity normally depend on the first target's ability to first detect the attack, but most importantly, to share this information with the rest of potential targets. Information shared in these processes can include security policies, practices, and technologies, in addition to vulnerability information, liaison activities, anomalies, attack signatures, and attribution-related information. On one hand, governments are often reluctant to share vulnerability information with the private sector to protect its sources, and also to be able to exploit those vulnerabilities themselves in offensive or defensive operations. On the other hand, information-sharing is considered a business risk by the private sector. Sharing vulnerability or attack information risks financial losses, reputational harm, legal liabilities, or intellectual property rights theft, and may eventually affect profits (M. Carr, 2016; Dunn Cavelty, 2016; Dunn Cavelty & Suter, 2009; Etzioni, 2011; Muller, 2016; Scott, 2012). In the USA, there is a general concern that shared information can be compromised or used by the government for surveillance purposes, particularly given the NSA's strong involvement in cybersecurity.

Importantly, the public-private relations through which cybersecurity is constituted are more complex than is generally acknowledged in the literature.

Specifically, they involve interactions that are not strictly 'cooperative', and measures that can negatively affect human security. Edward Snowden's leaked NSA files for example revealed how the NSA exerted pressure on private companies for surveillance purposes, including Microsoft, Apple, Facebook, Google, among others, using court orders, withholding their licences, or hacking into their systems (R. Deibert, 2015, p. 11). These measures altered the software and hardware of targeted devices, a process they called 'interdiction' (Biham, Carmeli, & Shamir, 2016, p. 777); weakened encryption by utilising supercomputers capable of cracking encryption algorithms; and enforced backdoor access to software (Harding, 2014, p. 259). Added to this is the controversial involvement of the state in the black markets of vulnerabilities and exploits. Based on leaked reports, states are increasingly involved in such markets to build cyber arsenals to be used for offensive and/or defensive purposes. Such practices, in turn, undermine the long-term security of individual users; increase the market price of those vulnerabilities and exploits; and risk channelling information to the wrong hands (Dunn Cavelty, 2014, p. 710, 2016, p. 20; Herzog & Schmid, 2016).

The problem also extends to software manufacturers and the modes of production in the market. Software vendors usually rush into introducing their products into the market with an intention to fix vulnerabilities later in the process, so that they can compete for profits. They mainly prioritise functionality over security, which led to a culture of acceptance of software insecurity. This commercialisation of cybersecurity transfers cyber risks and liabilities to the end user. Through the End Use License Agreements (EULAs),[23] vendors are transferring all risks and responsibilities to the end user, making themselves 'bulletproof'. The fact that many software is now free, makes it difficult to hold those companies legally liable for any exploitable vulnerabilities in their products. This explains why there is currently no legal or formal framework to oblige vendors to follow certain steps in software design or to adopt best practices in coding or encryption (Chong, 2016).

Against this background, the thesis will explore the intrinsic uncertainties and tendency towards disorder that characterise the operation of information systems as

[23] EULAs are agreements shown to the user when using a software, containing all the rights and restrictions related to the software operation.

one challenge for cybersecurity. The challenges of information-sharing mentioned above will not be reduced to the practices of particular actors, be they state or private, but will also be linked to the properties of information as such. For example, the thesis will explore the ontological uncertainties of information systems that hinder the existence of particular information to share to begin with. This is extended not just to future unknowns, but even to present and past unknowns and *unknowables*. Entropic security, in this light, analyses cybersecurity challenges not *just* as a reflection of human discourses or conflicting interests, but also as a product of the materialities of information per se.

Conclusion

This chapter has advanced a conceptually driven overview of cybersecurity, which engages with its definition, historical evolution, and major policy challenges. The chapter presented three main arguments. First, it has sought to counter a frequent tendency in the existing literature to view cybersecurity ahistorically. It showed how the roots of cybersecurity can be found in the development of computing and internetworking technologies following WWII until the internet was created – long before the terms 'cyberspace' or 'cybersecurity' even came into being. Secondly, and by way of extension, it demonstrated that security was not imposed on a purportedly non-securitized 'cyberspace' through a set of exceptional political discourses. Rather, security has always been an important contextual influence, generative force, and policy concern in different stages of the evolution of all the technologies that constitute what we experience as 'cyberspace'. Thirdly, the chapter showed that both the historical development of these technologies and the evolution of their security conceptualisation were not entirely planned by a particular actor(s). Rather, they evolved through a process of co-production, in which the interests of multiple actors competed, and their malleability generated new modes for their application.

As a context and a generative force, security was an indispensable element of the discursive and institutional tools of the co-production of scientific knowledge during the Cold War, which the internetworking and computing research was part of. Perceptions of the 'scientific gap' and discourses that weaponised science were institutionalised, as in the cases of the ONR and ARPA, and subsequently utilised by

those institutions in legitimising the influence the military exerted on scientific research, even on what academics regarded as 'pure science'. Furthermore, the foundational ideas that modern computers and the internet are based on, such as digital computations and packet-switching, were primarily generated by the war and post-war security needs, in a context of scepticism by both the scientific community and the private sector. And although computers started as calculators and the internet started as a resource-sharing network, both evolved into their modern versions and usages beyond the intentions of their creators.

As a policy concern, the security of computers and networks has always been present, though with different conceptualisation and diverse threat perceptions that reflect the technology's development state. Originally, when computers operated in controlled environments, there was an understanding of machines as necessarily controllable, and of threats as always extrinsic to them. That is why, computer security at that time was confined to unauthorised access and physical security. Yet, following the advent of networking and the dissemination of computers, the machines themselves began to be perceived as possibly threatening through software and hardware vulnerabilities. And therefore, malicious hacking and the use of malwares to target such vulnerabilities started to be viewed as a security threat upon which the modern cyber threat perception is based.

Though the current state of defining cybersecurity is marked by wide disagreements, it can still be defined as all the policies and tools undertaken to protect the multiple layers of the cyber environment, be it the virtual, physical, or semantic. Thus, concepts like internet security or ICT security becomes subsets of what cybersecurity is about. And despite the intersection between cybersecurity and information security, the earlier can still be distinguished by the digital nature of the attacks' tools and targets. Nevertheless, cybersecurity remains ontologically informational, or more precisely, *digitally* informational. Added to the conceptual ambiguity, there is a vast range of policy challenges that intensifies cyber insecurity and complicates the theorisation and study of cybersecurity. They include the cybersecurity dilemma and offence-dominance, PPPs, information sharing, commercialisation of security, and governments' involvement in black markets of vulnerabilities and exploits.

CHAPTER (3)
THEORISING CYBERSECURITY AS AN INFOSPHERE: THE PHILOSOPHY OF INFORMATION MEETS SECURITY STUDIES

> "So when we speak about and everybody is searching for the illusive analogy in the physical world to cyberspace. You know, is it—is it like a global commons, you know, is it like clean air or clean water? I think cyberspace is more like light than air and I think it presents challenges in that respect." - Jane Holl Lute, Deputy Secretary, DHS (DHS Cybersecurity, 2013, p36)

Introduction

The relative conceptual novelty of cybersecurity, its technicality, and its multi-disciplinarity have driven many policy makers and scholars to treat it as a distinct security sector. On the policy level, cybersecurity is sometimes presented as a 'unique problem' and 'an extraordinarily difficult strategic challenge' that requires a 'unique process' to manage (The White House, 2003, p. 2). Theoretically, this 'uniqueness' has been approached by constructivist studies that analyse the discursive peculiarities of cybersecurity (Jarvis et al., 2016; Lawson, 2013; Lawson et al., 2016), of which the cyber securitization literature is a prominent example (Bendrath et al., 2007; Dunn Cavelty, 2008a; Eriksson, 2001; Hansen & Nissenbaum, 2009). More recent contributions started to shift from human discourses towards a study of *materiality* in co-constituting cybersecurity practices (Stevens, 2015), and an analysis of cyber-incidents and malwares as actants (Balzacq & Dunn Cavelty, 2016). Yet, such contributions do not fully capture the peculiar *informational* ontology of cybersecurity. As will be demonstrated in this chapter, attending to *information* as a subject matter, referent object, and agency in cybersecurity adds important insights to its theorization in Security Studies and to the understanding of the material conditions that influence its socio-political construction.

Accordingly, the thesis introduces a novel analytical framework to the study of cybersecurity as an infosphere – a framework that goes beyond human subjectivity by also acknowledging the materiality of the informational non-human. This alternative framework is based on three main theoretical assumptions that this chapter aims to explain and substantiate. Firstly, *cybersecurity is ontologically informational*. Information lies at the heart of all the technologies, sciences, and practices that enable

this field and its very existence. Secondly, *information is a peculiar entity*. It is not just *another* 'thing'; rather, it has an autonomous status that sets it apart from matter and/or energy. Finally, it follows that *cybersecurity should be theorised differently* from other security fields. This is because information and its peculiar properties co-produce distinct meanings and logic(s) for 'security' in cybersecurity, which require new theoretical frameworks to understand.

In establishing these three hypotheses about cybersecurity, the chapter sets out a dialogue between the emerging field of the philosophy of information and Security Studies – particularly Critical Security Studies (CSS) which incorporates new materialist understandings of security. The chapter aims to prove that these different bodies of literature – the philosophy of information, new materialism, and Security Studies – can bear on one another in providing a deeper understanding of cybersecurity than the existing framework of securitization theory. On one hand, the philosophy of information and information theory are employed to analyse the *ontology* of information as a peculiar referent object of security. On the other hand, new materialism is utilised to theorize information as a generative force in cybersecurity and for breaking the link between discursive performativity and human subjectivity in the study of security. Together, they contribute to a *non-anthropocentric* informational framework that develops a revised understanding of cybersecurity as entropic security, governed by the logics of negentropy, emergence, and noise.

The chapter unfolds in three sections. The first section explores the informational ontology of cybersecurity. Mobilising the philosophy of information, the chapter analyses the concept of information and demonstrates its intrinsic relationship to the sciences and technologies constituting the 'cyber'. The second section then draws upon new materialism to problematise the concept of agency in studying security. It establishes a genealogical link between new materialism and post-humanism on one side, and information and cybernetics on the other. The chapter then takes this new materialist argument about the agency of non-human things a step further, by arguing that information too possesses a distinctive agency. Based on an understanding of information as the essence of the 'cyber' and as a peculiar non-human actant, the third section moves to the argument that cybersecurity should therefore also be theorised

differently. It focuses on the methodological aspects of theorising information as an active actant and of using discourse analysis in examining the empirical data. In so doing, it also contests the security logic(s) of existentiality, exceptionality, and emergency, whilst simultaneously opening the way for the alternative logics of negentropy, emergence, and noise that will be developed further in the following three chapters.

1. The informational ontology of cybersecurity

Cybersecurity debates are marked by an abundance of referent objects that cut across different sectors. As argued by Lene Hansen, cybersecurity is better analysed through the "*competing* articulations of *constellations* of referent objects, rather than separate referent objects" (Hansen & Nissenbaum, 2009, p. 1163). The cross-sectoral connections in the construction of referent objects can be seen in how the cyber threat is often conveyed in relation to the security of other sectors, particularly the military, the political, and the economic. 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. The following statement is one example: "Our national security, public safety, economic competitiveness, and personal privacy are at risk" (Emerging Cyber Threats to the United States, 2016, p11).

However, there is also something unique about cybersecurity that makes it an independent area of security policies and politics and not subsumed in other security sectors. There is a reason why we still call a hostile cyber operation that steals military secrets as a cybersecurity threat not simply a military security one, even though it intersects with the latter. We categorise cyber espionage that targets the intellectual property rights of industries as primarily a cybersecurity challenge more than an economic security one. This is because the ultimate referent object of cybersecurity is *information*. Even if necessarily connected to the operation of the economy, military, and the daily lives of individuals, it is information that is the threat tool and object. It is information systems that are the immediate target of hostile cyber operations, and they are the object that cybersecurity measures seek to defend. As argued by the executive director of the Cybersecurity Industry Alliance, "Cyber infrastructure is attacked and defended differently than the physical infrastructure" (H.R. 285, 2005, p.21), and this

difference lies primarily in information. But what exactly is information, and what makes it central to the ontology of cybersecurity?

There is, in fact, no widely agreed and clear understanding of what information really *is* – despite the abundant use of the term 'information age', and the rapidly growing inventions of machines and processes to analyse, share, and store information, such as computers and networks. There are mathematical, algorithmic, physicist, biological, semiotic, and several other different approaches to define it in different sciences. It is considered a foundational concept for all of them, even if not accurately defined. This philosophical impasse the term has passed through in different stages of its history has been a hurdle towards developing a unified or universal theory of information (Deacon, 2010, pp. 146–152). The first use of 'information' as a scientific term dates back to Norbert Wiener and his work on cybernetics – which was defined as the science of control and communication in the animal and the machine and regarded as the 'big bang of the information age' (Wiener, 1948). The birth of information theory, however, is usually associated with Claude Shannon's theory of communication that was introduced in 1948 (Shannon, 1948). Shannon was an American mathematician and electrical engineer who is regarded today as 'the father of information theory' – with some even arguing that he 'invented the information age' through his theory of communication (Soni & Goodman, 2017). Though a lot of the general philosophical exploration of information is based on their ideas, neither Wiener nor Shannon actually presented a definition or a theorisation of information per se. They rather dealt with information as a measurable quantity that they aim to maximise by minimising the noise in the transmission channel or medium (Burgin, 2010, pp. 2–3).

Nevertheless, there is a newly emerging field of research that interrogates the concept of information and introduces important philosophical insights about its nature and dynamics: the philosophy of information. The philosophy of information is a multi-disciplinary field with contributions from physicists, mathematicians, computer scientists, linguists, biologists, among others. It evolved with the massive development of ICTs, and particularly computing and internetworking technologies, that brought information to the centre of philosophy, as one significant force in the functioning of the world. The philosophy of information is broader and more inclusive than other

approaches like digital philosophy, cyber philosophy, or computational philosophy that were also associated with the development of these technologies. As argued by Floridi, a prominent contributor to this new field, information philosophy is more concerned with information than computation because “it analyses the latter as presupposing the former” (Floridi, 2013, p. 15).

The multi-disciplinarity of the philosophy of information as a field of research has already produced a wide variety of approaches to defining information. As noted by Floridi, information is “a polymorphic phenomenon and a polysemantic concept” (Floridi, 2009, p. 3). It has been regarded as “interpretation, power, narrative, message or medium, conversation, construction, a commodity, and so on” (Floridi, 2016, pp. 2–3). It can refer to the *process* of informing or changing the recipient’s knowledge (information-as-process). In this sense, the intangible nature of the process means that information can be hardly measured. This process of informing is different from *information processing*, in which tangible entities, such as data and documents, are processed. Information may also denote *knowledge*, or the reduction of uncertainty (information-as-knowledge). It is sometimes used as an attribution of objects as ‘informative’, be they documents or data (information-as-thing) (Buckland, 1991, pp. 3–4).

Alternatively, for the purpose of this thesis, information can be divided into three categories that speak directly to the field of cybersecurity: syntactic information, in the form of signs, signals, or bits; semantic information, or the meanings conveyed through those bits and signals; and pragmatic information, when those meanings and ideas conveyed are new to someone (Deacon, 2010, p. 152). The syntactic definition is the basis for Shannon’s theory of information, or the ‘mathematical theory of communication’. According to him, the meaning that the signals carry is insignificant to the engineering problem of communication; i.e., information is totally a mathematical concept (Lombardi, 2016, p. 30). For that reason, Flordi argues that Shannon’s mathematical theory should be described as the ‘mathematical theory of data communication’, or the study of the ‘syntactic level of information’ (Floridi, 2009). On the other side, many scientists emphasise the significance of the semantic aspect of information: its meaning, reliability, and relevance. This semantic conceptualisation

distinguish information from data; assuming that data becomes information when meaning is added (Ratzan, 2004, p. 4).[24]

Those multiple categories of information are central to cybersecurity. The syntactic layer is considered the 'centre of gravity in cybersecurity', as a fundamental quality that distinguish cyber threats from conventional ones. All cyber threats must go through the syntactic layer to qualify as such; i.e., to originate from code alternations or the use of malicious codes (Friis & Ringsmose, 2016, p. 4). Hostile cyber operations can also combine the semantic and the syntactic layers, such as the disinformation campaigns in which compromised computers – often called bots – are used to spread false information. Here, the meaning of information and its content is of absolute significance. Cyber incidents that aim at espionage, for example, are classified based on the semantics of the information they target, be it military secrets, personal identity, economic or business-related information, etc. Additionally, pragmatic information is fundamental for cybersecurity policies, since knowledge about vulnerabilities (exploitable coding errors) and cyber incidents is a key challenge. In consequence, many technical accounts of cybersecurity speak of it as 'information assurance' instead, defined as 'the art and science of securing computer systems and networks' (Ormes & Herr, 2016, p. 3). It is also typical to find 'information security' in many technical studies used as a synonym to cybersecurity to strictly signify the security of digital systems (For example: Bishop, 2003; Dlamini, Eloff, & Eloff, 2009; Knapp, Franklin Morris, Marshall, & Byrd, 2009).

Further, information lies at the core of the philosophy of computer science, computer engineering, and software engineering; i.e., the sciences and technologies constitutive of the 'cyber'. This can be seen in some definitions of computer science as 'the body of knowledge of information-transforming processes' or as simply 'the study of information'. This information can be data processing or methodological rules governing data structures (Primiero, 2016). Computing is also sometimes defined as

[24] The assumption that information has to encompass meaning is opposed by some scholars who believe that information has an objective existence that does not depend on its perception, understanding, or interpretation. And that is why, a distinction between 'information' and 'meaningful information' is sometimes made (Stonier, 2012).

"the systematic study of the ontologies and epistemology of information structures" (Primiero, 2016, p. 104). For that reason, it is argued that computation *is* an information processing and transformation process that operates by algorithms, or a set of instructional information. Instructional information is a type of semantic information that specifies actions to be performed by the receiver of information (Fresco and Wolf 2016, 84). The main function of a computer is thus the "material execution and mechanical realisation of those information-transforming processes" (Primiero, 2016, p. 91).

Correspondingly, although computers are syntactical devices, their operation is not restricted to syntactic information, but also involve semantics. For instance, a computing system used in an airplane has to operate with various natural semantic information about the condition of the airplane, including altitude, fuel injection, etc. (Piccinini & Scarantino, 2016). Information is also intrinsic to the physical layer of computational systems. Computer programs have their 'syntax and construction rules' that establish control over the physical layer of computational systems, define their operation, and dictate how they should perform by executing certain actions. Such information can be referred to as 'operational information'. It creates a semantic relation between the ontology of the physical layer and the operational language of software (Primiero, 2016, pp. 91–92).

Here, it is important to make a clarification about the position of the *digital* in the analysis. As the previous chapter argued, cybersecurity can be distinguished from information security by the digital nature of the incidents' or threats' tools and targets. Why, then, does the thesis use 'information' instead of 'digital information' to theorise the ontology of cybersecurity? Typically, computation is always associated with the digital; it depends on manipulating digits, or variables with discrete/finite values (Piccinini & Scarantino, 2016). Digital computational processes combine all the previously-mentioned elements of defining information: "the quantitative definition of bits, the syntactic construction of operations, the meaning of instructions, the abstract format of algorithm and the epistemically loaded designer' intention" (Primiero, 2016, p. 104).

Yet, the thesis does not confine its theoretical analysis to the digital because there are many more insights that the non-digital literature on information can add to the study – especially given that much of the digital information literature ignores semantic aspects that are also key in cybersecurity. Added to this, there are some philosophical and theoretical debates about the connections between the analogue and the digital that may render an analysis confined to the digital overly restrictive. Some physicists, for instance, argue that any computer is 'partly digital and partly analogue' (Dyson, 2001), or that all digital devices are in essence analogical devices (Pias, 2005). For example, an LCD screen can be considered a hybrid system between digital and analogue, since it displays discrete pixels but emits light that may be measured using an analogue continuum (Berry & Dieter, 2015). Engaging in this debate is beyond the scope of this research; the main point here is that there is a theoretical and an analytical sense in using information rather than digital information as a framework for this study, while acknowledging the digital nature of cybersecurity. There is a lot that the general philosophical explorations on multiple forms of information can contribute to our understanding of cybersecurity and its peculiarities. Additionally, using information rather than digital information as an analytical framework avoids reducing information to a particular device or technology.

To summarise, if cybersecurity is to be defined as the security of computers and networks, which are primarily information systems, then it may well be argued that cybersecurity is fundamentally *informational*. This is ultimately an acknowledgment of the informational essence of the *cyber*, its technologies, and its sciences beyond linguistic utterances. Such an approach reaches a necessary level of abstraction that speaks to the fundamental being of cybersecurity. It also overcomes the ambiguity of the cyber terminology which has done little to deal with the complexity of this realm by resorting to information to understand its peculiarities. Investigating the informational ontology of cybersecurity ultimately renders it a study of materiality. As we will see below, it challenges securitization theory's conceptualisation of agency and its focus on the discursive construction of security, whilst also speaking to CSS attempts to incorporate new materialism or post-humanism in studying the agency of non-human objects in co-constructing security.

2. Agency and 'information' that matters

> "Language matters. Discourse matters. Culture matters. There is an important sense in which the only thing that does not seem to matter anymore is matter." (Barad, 2003, p. 803)

As mentioned earlier, the discursive study of cyber securitization has proven problematic. In part, this is the result of the state-centric approaches employed by the cyber securitization literature that are inapplicable to the multi-stake holder nature of cybersecurity. Importantly, it is also because focusing only on speech acts overlooks questions of materiality and agency. There are several material realities about the nature of computer disruptions, their effects, and knowledge about them in technical communities that cannot be understood as part of discursive constructions (Dunn Cavelty, 2019, pp. 138–140). This includes, for example, the exponential rise in the number of cyber operations through self-replicating malwares that enjoy a considerable level of autonomy in execution. Added to this is the increasing use of AI both as a facilitator of cyber incidents and as part of cybersecurity defence measures (Stevens, 2020). This all necessitates an analysis of information, not just as a referent object of cybersecurity and its securitization processes, but also as an active actant in its own right.

The idea that a non-human entity like information can be an *actor* with agential influences on security construction coincides with what is often called 'the material turn', 'non-human turn', 'thing studies', 'posthumanism' or 'new materialism' in social sciences. This so-called turn produced new philosophical paradigms such as object-oriented ontology (OOO) (Bogost, 2012; Bryant, 2011; Harman, 2018), vital materialism (Bennett, 2009, 2015), agential realism (Barad, 2003, 2007), and actor-network theory (ANT) (for example: Latour, 2005; Law, 2002; Law & Singleton, 2005) to challenge the binary division of the world into human subjects and non-human objects. It is a call for widening the scope of research and philosophical debates away from the centrality of whatever is relevant to humans, be it reason, cognition, language, etc. (Kaltofen, 2018, pp. 44–45). All such contributions share a critical view of the dominant status of the Anthropocene, but differ in the extent to which they move beyond this dominance in articulating the relationship between the humans and the non-humans (McDonald & Mitchell, 2017). They theorise matter as an active, politically significant force that has

meaning beyond social, political, or economic structures, and has agency that transcends politics of representation. From this lens, the concept of agency in International Relations and Security Studies can be problematised.

In International Relations and Security Studies, the posthuman approach represents a criticism of the inadequacy of existing ontological and epistemological perspectives to capture non-human agency, be it that of machines, animals, bacteria, the environment, etc. For many years in the discipline, agency has been tied to the human subject, and the capacity to act has been linked to cognition, intentionality, desires, and decision-making; qualities regarded as exclusive to humans (Braun et al., 2018). Similarly, despite the CSS attempt to widen security to include actors other than the state, agency has been limited to humans and human collectivities. If threats are conceptualised as manifestations of suffering, and if the ability to express such suffering is a function of humans, then security is tangled to human subjectivity (McDonald & Mitchell, 2017; Mitchell, 2014a, 2014b). However, a strand of research focusing on materiality and non-human agency started to gain momentum in recent years. Examples include the study of the materiality of critical infrastructure (Aradau, 2010), borders security (Bourne et al., 2015), airport security (Valkenburg & van der Ploeg, 2015), emotions (Solomon, 2015), among others. Nevertheless, this approach is still not present enough on the mainstream research agenda, and there remains little agreement on what the 'post' in a posthuman approach should look like (Cudworth et al., 2018).

2.1. Information and the evolution of the 'material turn'

Information and cybernetics had a major role in the evolution of posthumanism and new materialism. If approached genealogically, posthumanism can be linked to the Macy Conferences on Cybernetics that took place between 1946-1953.[25] In these conferences, the human subject was decentralised in relation to other objects, and in particular to information (Wolfe, 2010, p. xii). Cybernetics brought forward an analysis of information as a free-flowing entity among biological and non-biological systems, which opened the

[25] The Macy conferences were interdisciplinary conferences held in the USA and are sometimes considered the most significant scientific events after WWII. Concepts like 'information', 'analogue/digital', and 'feedback' were introduced in these conferences as part of regulatory frameworks that can apply to both humans and machines (Pias & Foerster, 2016).

way towards blurring the lines between humans and machines. The theoretical contributions of Wiener and Shannon in cybernetics and information theory resulted in thinking about humans as information processing entities; in turn, making them comparable to intelligent machines. Both humans and machines were seen as autonomous and goal-directed entities; an idea that challenges the humanist subject. As one of its pioneers, Ross Ashby argued that cybernetics is not concerned with "what *is* this thing?", but rather asks "*what does it do*?" (Ashby, 1958, p. 1).

In the Macy conferences, Wiener and John von Neumann (another influential mathematician) presented information as the most significant entity in the relationship between humans and machines. By approaching information as more fundamental and significant than matter/energy, similarities between humans, animals, and machines as informational entities became possible. In addition, Wiener's ideas about self-organisation in machines meant that they are able to self-evolve beyond human intentionality. This produced an understanding of self-evolving computer programs as 'alive' themselves. If everything in life is informational, then computer code is a 'form of life' per se (Hayles, 2008, pp. 1–64). Accordingly, as argued by one scholar, "it is impossible to understand posthumanism properly without understanding cybernetics" (Mahon, 2017, p. 31).

Moreover, with increased digitisation, and the advancements in AI and robotics, the level of control humans maintain over machines began to largely diminish. Such developments form the basis on which some futuristic trans-humanist approaches in social sciences conceptualise the 'posthuman' and problematise the 'human' as a category. From their perspective, humans are undergoing a process of evolutionary transformation towards becoming posthuman, i.e., being replaced, outpaced, and outsmarted by the technological non-humans. They contend that technologies are growing autonomously beyond human comprehension or control (Schwarz, 2017). For example, several studies on cyborgs (for example: Haraway, 2006), brain-computer interfaces, and biomedical engineering argue that the human body has transformed as a result of ubiquitous technological developments, either through upgrade, enhancement, extension, or invasion (Kaltofen, 2018, p. 42).

However, unlike the techno-reductionist views of transhumanism, posthumanism takes a different stance on technology. It does not challenge anthropocentrism by using biological, evolutionary, and hypothetical scenarios that assume humans are transforming into something else or being replaced entirely by the non-human. Rather, according to posthumanism, technology is one factor among many in breaking the binary division between the humans and non-humans. Moreover, posthumanism and new materialism assume a 'flat ontology' in which agency is distributed equally among humans and non-humans (Salter, 2015). They do not replace the human primacy with that of the non-human; they aim to abolish all social hierarchies and exclusivism in conceptualising agency altogether (Ferrando, 2013, p. 29). Thus, acknowledging the autonomy of technology and machines beyond human subjectivity does not mean they have overtaken agency. On the contrary, agency is to be approached as an assemblage that blurs the traditional separation between humans and the technological non-human, as part of a 'posthuman subject' (Braidotti, 2013).

Such an approach, however, has not migrated well to the study of cybersecurity or to the field of International Relations in general. Technology has been approached either deterministically as a casual force or instrumentalised in studying the intentionality of a particular actor using a constructivist lens. Nonetheless, as argued by Bousquet, technology is "Less because it's not an external material agency that unilaterally transforms a passive social body, and more because it actually permeates every aspect of the social" (Bousquet, 2013, p. 96). The same applies to the theorisation of cybersecurity in the literature, where the logic(s) of security and risk are tied to human actors' intentionality or discursive practices. A new materialist or post-humanist revisiting of cyber securitization would thus require an analysis of information as an entity that *matters*. That being said, if all matter in all security sectors has agency, the thesis argues that cybersecurity remains peculiar given its informational ontology. That is, *all matter matters, but information matters differently* – as will be shown next.

2.2. The peculiarities of information

> "Information is information, not matter or energy. No materialism which does not admit this can survive at the present day." (Wiener, 1948, p.132)

In emphasising the agency of matter, many strands of new materialism include all non-human things in their entirety without distinguishing between the agential capacities they possess. In addition, some of them adopt a *relational* ontology, according to which things are only real if they have an effect on other objects. Latour's ANT, for example, assumes that there is no force embedded in things beyond their relations with other objects, from which they acquire agency (Harman, 2009). Nevertheless, it could be argued that "*all things equally exist, yet they do not exist equally*" (Bogost, 2012, p. 11). Matter or 'things' are not all of one type or one form of agency (Bryant, 2014). As noted by Harman, flat ontology should not be an end in itself. It is not enough to reject the position of humans as the centre of ontology. Rather, the analysis should extend to investigating the different features and powers possessed by different 'things'. As he said, "an object is *more than its pieces* and *less than its effects*" (Harman, 2018, p. 53). Things can have an autonomous reality and intrinsic properties that are not necessarily reduced to their effects.

In the same vein, the thesis argues that information is a peculiar entity. It is not the mass-energy that scientific conceptualisation of matter signifies and not an ordinary non-human thing that only gains agency in relation to other objects. The roots of information's peculiarity can be found in Wiener's cybernetics. One central idea behind cybernetics is Wiener's argument that information plays a fundamental role in every aspect of the universe. According to him, all physical entities are inherently *informational*; i.e., all objects are 'informational objects'. He even argued that all living things, including human beings, are 'informational entities' in how they store and process physical information in the form of genes, DNAs, proteins, etc. (Wiener, 1948). As a result, some argue that the information revolution has changed humanity more than any other revolution in history, because it influenced and changed objects on the 'deepest level of their being', which is information (Bynum, 2016, p. 205). The physicist Wheeler took this argument even further in his article "It from Bit" by arguing that even matter-energy and all particles and physical entities (all *its*) owe their existence to information (to *bits*) (Wheeler, 1992).

Importantly, cybernetics presented information as different from matter and energy. Although it was not clear what Wiener meant by 'information is information', it

can be inferred that he regarded information as 'autonomous'; something that has a distinct structure (Janich, 2018, p. 4). Information is much more complex and varied in its operation than matter or energy. It can be an objective abstract setting if approached mathematically, and a subjective entity that depends on a recipient. Although mainstream physics assumes a centrist position between objectivity and subjectivity in analysing the ontology of information, some physicists would argue that information is the only real thing in life. That is, matter and energy are just a reflection of information they embody, and the observer is just a subsystem that follows informational rules (Harshman, 2016). As argued by the information theorist Tom Stonier: "*Information exists*. It does not need to be *perceived* to exist. It does not need to be *understood* to exist. It requires no intelligence to interpret it. It does not have to have *meaning* to exist. It exists" (Stonier, 2012, p. 21).

Besides, information is distinguished by its inherent multiplicity. It has diverse sources, contents, and bearing media. It can be static (e.g., images or sentences), or dynamic (e.g., videos). It can be stored, transferred, modified, delayed, terminated, etc. It is used for communicative and non-communicative purposes (Sloman, 2011). Based on the receivers, it can be visual information, auditory, cognitive, etc. It can be *about* anything, from weather information, to political, economic, or military information (Burgin, 2010). It can be structural when imbedded in a system and kinetic when processed, transferred, or transformed (Stonier, 1991). It is temporal and ephemeral; its value changes over time and can also lose its value entirely at a certain point of time. It is not fungible, since it does not have 'identical interchangeable parts' and does not lose its components when given away. It is both a *process* and a *commodity*, and can be quantified in its syntactic form, or evaluated in entirely qualitative terms in its semantic form (Ratzan, 2004, p. 3). It is 'expandable', and its expansion is limitless. It is 'compressible' and can be summarised or concentrated. It is 'substitutable' and can replace many physical materials. It is 'transportable', since it travels faster than physical objects and can be transmitted at speed of light or even faster as argued by quantum mechanics. It is sharable, and although it does not decrease in quantity when shared, it may decrease in value according to the new recipient and their knowledge (Burgin, 2010).

Another very important quality of information is its transformational capacity. In one of its definitions, information is presented as 'the difference that makes a difference'. This entails both *agency* and the capacity to *transform* and change. Information is always in a constant state of conversion. It is always changing, interacting with multiple other informational and non-informational agents, and transforming both itself and its surrounding environment. There are multiple ways through which the transformational capacity of information can be observed. For instance, information may transform during the process of its interaction with other information. Here, it is information that is changing itself through an internal, dynamic, and objective process. In other cases, information may remain static while its perception by agents transforms. This is also an internal process of transformation, but one that is subjective rather than objective. Alternatively, an agent may deliberately change information in an external, objective manner. But when the changed information causes changes in the perception of another agent, the process turns into an external, subjective (intersubjective) one (Gershenson, 2012, pp. 104–105). The transformational property links information to energy and leads some to argue that energy may even eventually "*turn out to be information*" (Burgin, 2010, p. 102). That is why, information theory is sometimes portrayed as a framework that specifies the types of transformation that can take place given available resources. It is also why computation is defined by some as a process of information transformation (Timpson, 2016, p. 223), together with the assumption that information is processed only through data transformation (Burgin & Dodig-Crnkovic, 2013).

As a result, any self-organising system that is capable of making choices among many possibilities with the aim of achieving particular causal effect in its environment is one that generates information. Transforming inputs/causes into outputs/effects performed by self-organising system, unlike mechanical systems, involves information generation. As one study argued, "the act to discriminate, to distinguish, to differentiate, is information" (Hofkirchner, 2012, p. 9). When information is generated, novelty is also generated. The idea that information is essentially transformative and that transformation generates novelty is used by some scholars to talk about the role of information in evolution (Gershenson, 2012, p. 106). Moreover, the transformation of

information also produces diversity and variety. In contrast to uniform sequences and formalised mechanical systems, information is constituted by variety (Hoffmeyer, 2008, p. 156).

This multiplicity and transformational capacity of information is one important manifestation of its complexity. According to Ashby in his work on complex systems and cybernetics, variety as such is a measurement of complexity. He argues that information is a 'reflected variety', which is basically the difference perceived between one object and another (Hofkirchner, 2013, p. 168). Similarly, Gregory Bateson – another key figure in cybernetics – argued that information and variety are synonyms and that variety is a synonym for difference (Hoffmeyer, 2008, p. 156). Ashby called this the Law of Requisite Variety, which contends that a system with complex variety requires an equal degree of variety in models of management: "only variety can destroy variety" (Grösser & Zeier, 2012, pp. 94–95). Thus, complex information will result in more variety, requiring complex agents to perceive and propagate it (Gershenson, 2012, p. 106). Arguably, the evolution of information processing systems would not have taken place without the possibility of information transformation (Stonier, 2012).

This complex nature of information is sometimes used to explain the complexity of the world despite the simplicity of the physical laws that govern it. This view presents an alternative explanation to cosmology and the origin of the world by replacing energy and matter with information. That is, information, not energy, is the primary actor in the universe's history. As argued by Seth Lloyd, a professor of mechanical engineering and physics, if energy makes physical systems do things, information tells them *what* to do (Lloyd, 2006). Additionally, it is argued that information is more fundamental than matter (Gleick, 2011, p. 12). It replaces the traditional view of classical materialism that regarded matter - the material particles or atoms and their chemical interactions - as a force that explains everything in the world. Information, in turn, represents a new development in this cycle of transformation from matter to mass to mass-energy. This means that physical reality is better explained by information than the 'mathematical relations' and the 'laws of nature' that govern matter. And thus information, not matter or energy, is the primary entity of change in the world (Mcmullin, 2010).

If we accept the definition of information as 'the capacity to organise a system', then DNA, crystals, and almost everything that involves patterns of organisation or organised structures necessarily carry information. Even irregularities or chaos in some systems are sometimes the result of algorithms. This is because, as argued by the philosopher of information Tom Stonier, algorithms can be designed to have unpredictable results that may seem chaotic. Information is also implicitly found in all laws of physics. For example, motion is in itself an 'information act'. Force and momentum are energy, while motion is information that specifies the trajectory and structure of moving particles. That is, moving particles carry energy and their motion carries information. In addition, the term 'direction' can also be described as 'an information term'. Basically, any change in time or distance denotes a change in the 'information status' of a certain 'moving body' (Stonier, 2012).

The argument that the whole world is one giant computer, or quantum computer, is derived from this viewpoint. It assumes that the universe is composed of bits, since all atoms and particles register 'bits of information', and thus when the universe computes, it is basically computing itself. If computers are defined as machines that process information, then *anything* can also compute, including the universe (Lloyd, 2006). This argument belongs to a strand of literature referred to as 'digital ontology' or 'digital metaphysics'. It primarily assumes that the ultimate nature of reality is informational and computational, and that the physical world can be explained by an 'information-theoretic origin' (Steinhart, 1998). Even before the invention of computers or the idea of a digital computer, it was scientifically understood since the 19th century that 'all atoms and elementary particles register bits of information', and when they happen to collide 'those bits are transformed and processed'. Yet, starting from the 1990s, it became clearer that those particles also *compute* and can be programmed. Hence, assuming that the universe is a computer is more than just a metaphor. The 'computational theory of the universe' has the power to explain complexity by reading the history of the universe as a history of subsequent 'information-processing revolutions'; a process that constantly engenders 'a stream of ever-more-complex structures' (Lloyd, 2010).

This belief in the ontological primacy of information has echoes in some empirical studies that analyse the transformation of security and military conflicts in the informational age. For instance, Arquilla and Ronfeldt - who wrote the influential paper 'Cyberwar is Coming!' (Arquilla & Ronfeldt, 1993) - view information as 'an essential part of all matter', and that it is as fundamental to the world as matter and energy. Consequently, according to them, information "should be treated as a basic, underlying and overarching dynamic of all theory and practice about warfare in the information-age" (Arquilla & Ronfeldt, 1996, p.154). Similarly, Dunn Cavelty and Brunner argue that information is *the* major source of power both in its material form of computers and infrastructure, and also in the 'immaterial realm' of codes. As they put it "Information becomes a weapon, a myth, a metaphor, a force multiplier, an edge and a trope – and the single most significant military factor" (Brunner & Cavelty, 2009, p.633). In his discussion of 'network-centric warfare', Dillon also contend that "information is the prime mover in military as in every other aspect of human affairs, the basic constituent of all matter" (Dillon, 2002, pp. 72-73).

However, it is important to note here that this ontological primacy of information is not an entirely resolved matter. Although this idea is adopted by the majority of information philosophers, it is still contested by others, particularly some physicists. The physicist Julian Barbour, for instance, opposed Wheeler's argument 'it from bit' by arguing that the argument should be 'bit from it'. According to Barbour, information and 'bits' cannot come to life without being underpinned in 'things'; bits are merely dots on screens that are only given meaning by the physical universe, or by matter. For him, information is an *abstraction* not *reality*: "Try eating a 1 that stands for an apple" (Barbour, 2015, p. 204). This is a philosophical debate that McHarris sees as a resemblance of 'the problem of the chicken and the egg' that drives the discussion into 'an infinite loop' (McHarris, 2015, p. 233). Both sides of the debate, however, admit degrees of uncertainty about their argument. For instance, the physicist Anton Zeilinger says "What I believe but *cannot prove* is that quantum physics requires us to abandon the distinction between information and reality [emphasis added]" (Zeilinger, 2005). In criticising Wheeler, Barbour also acknowledges that his analysis "*weakens* but not

necessarily *destroys* the argument that nature is fundamentally digital [emphasis added]" (Barbour, 2015, p. 197).

Though this remains an unresolved debate, it still signifies that information must be regarded as a highly peculiar entity. This peculiarity, moreover, renders any approach that deals with information simply as *another* non-human thing or domain deeply problematic. To reiterate, *all matter matters, but information matters differently*. And if the ontological status of information in regard to matter in the formation of reality is a debatable issue, it is not as such in the field of cybersecurity. That is, as explained in the first section in this chapter, information is the core of all the layers that constitute 'cyberspace' and cybersecurity and therefore its ontological fundamentality in this field is arguably more obvious. Once this informational ontology of cybersecurity is properly acknowledged, questions must therefore be raised about how the peculiarity of information impacts upon the construction and conceptualisation of security. The next three chapters therefore will each focus on one of three ontological properties of information that have the most profound ramifications for cybersecurity: (1) the intrinsic indeterminacies of information operation; (2) the agential capacities of syntactic information (codes/software); and (3) the simultaneous physicality and non-physicality of information. Using the aforementioned literatures on the philosophy of information, information theory, and software studies, the thesis will investigate how these three properties co-produce peculiar logic(s) or meaning(s) of 'security' in cybersecurity. This all, however, first requires delineating a new methodological framework to the study of cybersecurity different from the one introduced by securitization theory.

3. An informational framework to the study of cybersecurity

The realization that information is a generative force in co-producing cybersecurity discourses and practices challenges the position of agency in securitization theory and the cyber securitization literature more generally. It is an argument that securitizing cybersecurity as an infosphere is a process that takes place through the distributed agency of information *and* human actors. In such a process, information per se plays an essential role in the construction of its (in)security, or of its securitization. Saying that a non-human entity like information has agency means that, as argued by Bennett, it has

its own 'trajectories, propensities, and tendencies' outside the boundaries of human's control, subjectivities, or semiotic influences (Bennett, 2009, 2015). In the thesis, studying the agency of information is illustrated in the different ways it challenges human control and intentionality in cybersecurity constructions, and produces different security logics that cannot be studied within traditional anthropocentric theoretical frameworks, like securitization theory. As argued by Audra Mitchell's theorisation of posthuman security, instead of viewing the human as necessarily in control of security contexts, it is important to acknowledge the uncertainties and unpredictability that the agency of non-human objects produces (Mitchell, 2014b).

Further, to counter the anthropocentricism in the cyber securitization literature, the thesis gives more weight in the analysis to information, albeit without suggesting that it supersedes or replaces human agency. For example, in her introduction to vital materialism, Bennett says:

> "I will emphasize, even overemphasize, the agentic contributions of nonhuman forces (operating in nature, in the human body, and in human artifacts) in an attempt to counter the narcissistic reflex of human language and thought. We need to cultivate a bit of anthropomorphism – the idea that human agency has some echoes in nonhuman nature – to counter the narcissism of humans in charge of the world" (Bennett, 2009, p. xvi).

Similarly, the thesis theorises information as generative and productive of the meaning of cybersecurity through its peculiar properties, alongside humans and in interaction with them, even though it focuses more on information as such. This analysis also entails that humans are not the only referent objects of cybersecurity, but information as such is a significant one too. Consequently, what matters for studying security is not the mere identification of referent objects, but a deep understanding of their ontology. That is what the thesis does by focusing on information and its peculiar properties. Instead of reducing objects to our knowledge about them or their relation to human subjects, we should investigate their own being regardless of human representations (Bryant, 2011).

Additionally, the thesis introduces an analysis of cybersecurity that follows information as such (the non-human entity), rather than cyber incidents (the phenomenon). This distinguishes the thesis from an ANT-inspired approach to the study

of cybersecurity like that of Dunn Cavelty and Balzacq's (Balzacq & Dunn Cavelty, 2016). Their study examines the agency of cyber-incidents in constructing their own spaces, that in turn demands different types of political interventions. In doing so, they focus on the Stuxnet attack: a high-profile cyber incident that targeted the Iranian nuclear centrifuges in 2010, allegedly planned by the USA and Israel. On contrary, this thesis theorises information as such, rather than attack incidents, as an active actant. It also does not focus on particular political interventions to address cyber incidents. Rather, it studies the overall meaning and construction of cybersecurity beyond a single incident or a specific intervention. That is to say, information matters, not only when a cyber incident takes place, *but also when it does not*. The co-constitutive influences of information on cybersecurity are examined, not just in association with high-profile, state-backed cyber operations, but also in the case of the *mundane*, banal ones, or even when they do not take place at all. This non-anthropocentric approach breaks the link between agency and human discourses in securitization theory.

3.1. Discourse, materiality, and non-human agency

Speech acts and discourses, traditionally regarded as exclusive to humans, hold a central position in securitization theory. They are both a signification of actancy and a force that makes security possible. Hence, we cannot possibly problematise the humanist underpinnings of the 'securitizing actor' in the theory without contesting its conceptualisation of the discursive practices that constitute security. This is one of the major influences that the 'material turn' had on International Relations, by challenging the field's pre-occupation with meaning-making practices, textual and inter-textual analysis, and the question of representation (Lundborg & Vaughan-Williams, 2015).

Representationalism is central to the metaphysical stance of the social constructivist paradigm at large, which securitization theory is part of. It refers to the world view that ontologically and epistemologically distinguishes between 'things' and 'words'; 'the observer' and the 'observed'; and the 'knower' and the 'known'; i.e., the representations and the represented. In its essence, representationalism is pre-occupied with accurately representing reality, or 'correct correspondence' (Barad, 2007, p. 137). When things and representations are thought of as distinct, they are denied any capacity of influencing one another. Believing in the power of words to

represent things is not only present in the original formulation of securitization theory, but also in some strands of CSS which adopt a wide conceptualisation of discourse to include the materiality of practices, but still 'privilege words over things' (Aradau et al, 2014, p.58). For instance, some of the second-order securitization literature criticised the theory for excluding contextual influences on securitization processes (Balzacq, 2011; Wilkinson, 2011), but still left the non-human objects outside the realm of security. The contextual approach to securitization that this strand introduced to counter the linguistic focus of the original theory remain anthropocentric; i.e., deeply connected to humans and their perceptions and less attentive to the materiality of the non-humans that co-produce those perceptions.

In technology, software, and media studies, the term 'materiality' is used in abundance, though rarely defined. In some instances, physicality is viewed as a defining character of matter, and therefore some studies refrain from using the term 'materiality' when they discuss properties of software or data for example, and use words like 'stuff' instead (Leonardi, 2010). On the other hand, some of the STS literature use materiality to imply the social conditions that surround the development of technology and scientific discoveries; what could be described as 'the materiality of practice'. Similarly, in media studies, the materiality of the context is discussed in terms of the political economy or geographical considerations of media development, in addition to questions of ownership, control, reach, etc. (Dourish, 2017). Some of these aspects are also viewed from a political philosophy or a Marxian perspective, in order to analyse the material economic conditions of ICTs development that support their speed and manipulability, such as alliances between corporates and governments, international governance regimes, among others (Dourish & Mazmanian, 2013, p. 98).

Nevertheless, acknowledging the *vitality* and *vibrancy* of non-human objects in the new materialist scholarly contributions led to an increasing focus on materiality as *agency* in studying media infrastructures and digital technologies (Parks & Starosielski, 2015). Related to this are studies that attend to the cultural role of information and 'digital goods' and their symbolic weight in material cultures, as well as the study of how information and digital networks are shaping *space* (Dourish & Mazmanian, 2013, p. 94). This is the strand of research in studying materiality that the thesis primarily speaks to

by analysing the generative capacities of information in co-producing the field of cybersecurity.

Materiality and discourse, however, should not be viewed as two opposing frames of analysis. Materiality (the non-human things that make up our existence) and discourse (meaning-making practices) can be both regarded as co-constitutive forces of security. For example, as explained by Aradau, the scanned image of a liquid that is checked separately in an airport for security concerns is co-produced by a *screening device* that identify this liquid as a 'distinctive object', and also by *discourses* on terrorism and precautionary measures. That is, the 'dangerousness' of the liquid in this example is co-constituted by both materiality *and* discourse (Aradau et al, 2014, pp. 58-62). Barad also argues that materiality and discursive practices should be theorised in productive terms. This does not mean simply considering the role of materiality *in addition* to discourses, but most importantly, their *intra-action* or entanglement. Discursive practices are not a property of human actors; they are rather "material (re)configurings of the world through which boundaries, properties, and meanings are differentially enacted" (Barad, 2007, p. 183). Similarly, materiality is also discursive, and neither matter nor discourses have an ontological or epistemological superiority over the other. It is possible to connect words, things, and the material in understanding the complexity of 'their becoming', without having to consider the human as either a cause or an effect (Barad, 2007).

By reconceptualising discourse and breaking its traditional link with linguistic utterances, we can then view non-human entities, or information in this thesis, as 'produced and productive, generated and generative' (Barad, 2007, p. 137) and as an active agent in the co-construction of its own (in)security. As Aradau argues in her work on the securitization of critical infrastructure, the materiality of non-human things is capable of enabling and constraining what is securitized. Securitization, she explains, should be studied as a process of *materialization* in which the generative capacities of matter and 'things' and the role of materiality in co-constituting reality are considered (Aradau, 2010). This means too that the effects of non-human things should not be reduced to human linguistic framings. Rather, discourse and materiality should be

approached as agents in a process of co-production and hence, their relationship should be studied (Jacobsen & Monsees, 2019).

Drawing on these contributions, the thesis reconceptualises the discursive in analysing the policy documents and congressional hearings, as part of the empirical case study. Discourse is not approached as language or speech act, but rather as the force that enables or conditions language. Bridging the gap between the material and the discursive aims at analysing information not merely as an object of protection or a facilitating condition in cybersecurity, but as a generative force of its own (in)security. It follows that the process of securitizing cybersecurity as an infosphere is in essence a process of materialisation. In such process, information plays a key role in co-producing the logic(s) of security and shifting them beyond the traditional distinctions between security and risk.

3.2. The logic(s) of security-risk

One important implication of employing a non-anthropocentric informational approach to study cybersecurity is challenging the fixation of security logics and their humanist foundations. As explained in the Introduction, securitization theory has fixed a meaning for security by tying it to existential threats and exceptional measures. A security threat only qualifies as such when it is linked to the survival of the referent object, and securitization succeeds when 'above-politics' measures are proposed and legitimised. These logics were criticised for consolidating state's power and sovereignty in the realm of emergency (M. C. Williams, 2003); for reflecting a 'Cold War mindset' that restricts the theory to the statist logics of militarisation (Booth, 2007); for neglecting the political implications of securitization (Aradau, 2004, pp. 405–406); and for its liberal-democratic conception of 'normalcy' (Aradau, 2004, p. 392).[26] As a result, some scholars think of security as undesirable and problematic (Balzacq et al., 2015). For instance, Didier Bigo defined security as some sort of a political technology or a 'dispositif', in which exceptionalism and exclusion are institutionalised, normalised, and banalised, through processes of insecuritization (Bigo, 2000, 2002, 2006, 2008). Therefore, many CSS

[26] Aradau's work triggered a wide debate on whether securitization and desecuritization are essentially negative, as she proposed, and how relevant her alternative 'emancipation' concept is to the assumptions of the theory (for example, see: Alker, 2006; Behnke, 2006; P. Roe, 2012; Taureck, 2006).

criticise securitization theory by rejecting the concept of security entirely and replacing it with alternative paradigms, such as emancipation (Aradau, 2004; Aradau & Van Munster, 2016; Booth, 1991, 2007).

Another way such logics are scrutinised and replaced can be found in the risk literature. Risk was introduced in Security Studies with the assumption that it has transformed security, either by replacing or intensifying it. The argument that risk is the new security is centred on the sociologist Ulrich Beck's idea of *risk society* (Beck, 1992, 1999, 2002, 2006). Beck's thesis 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). Several security studies utilise Beck's ideas to argue that risk has changed the international security agenda (Rasmussen, 2001, 2004); shifted the focus of strategic studies to risk-based instead of threat-based security strategies (M. J. Williams, 2008); and replaced the security dilemma with a 'security paradox', that deals with the management of uncertainty rather than the management of insecurity (Kessler & Daase, 2008). Others analyse the negative implications of this arguable replacement of security with risk. They argue that risk has strengthened states' sovereignty in exceptional ways (Aalberts & Werner, 2011; Stockdale, 2013), and has been commercialised and commodified by private companies to enhance their profits (Krahmann, 2011).

However, this strand of research was criticised by many in the field of CSS, arguing against its realist ontology and introducing a framework based on Foucault's concept of *governmentality*. By conceptualising risk as a 'social technology', CSS scholars contend that Beck's thesis fails to capture the diverse ways and mechanisms put forward to govern risk and to render the uncertain future knowable and actionable (Aradau et al., 2008, p. 150). They see risk as part of a neo-liberal rationality and a *dispositif,* composed of multiple material and discursive elements, for governing what is perceived as ungovernable (Aradau & Van Munster, 2007). Assuming this inevitable association between the neoliberal governmentality and risk has led to a fixed perception of the security-risk nexus. That is, they argue that risk intensifies and expands security, or acts as a force multiplier, by privileging decisions based on dangerousness, normalising exceptionalism, and reinforcing authoritative presentations of insecurity (Aradau et al.,

2008; Aradau & Van Munster, 2007; De Goede, 2004; Hagmann & Dunn Cavelty, 2012; Salter, 2008).

The bottom-line is that fixing security and risk logics has led to an understanding of each of them as a distinct paradigm. This, in turn, resulted in an under-theorisation of risk and of the security-risk nexus in the study of cyber securitization processes. If security is assumed to be always existential and exceptional, many practices and discourses that are enabled by risk would be seen as inferior to the study of security. For instance, in her explanation for why cyber securitization has failed, Dunn Cavelty argued that "Despite the fact that there is national security rhetoric in abundance, the actual countermeasures in place rely on risk analysis and risk management" (Dunn Cavelty, 2008b, p. 30). Similarly, although Hansen and Nissenbaum recognised that some of the peculiar grammars of cybersecurity they presented resonates with risk theory, they did not incorporate risk in their study: "since 'security' rather than ''risk'' is the dominant policy as well as academic concept, it is not pursued in further detail in this paper" (Hansen & Nissenbaum, 2009, p. 1164).

Fixing the logics of security has been criticised by some studies for contradicting the idea of intersubjectivity in security constructions assumed by securitization theory. They view it as a prioritisation of the security analyst over the practitioner and an assumption that the former has better understanding of the essence of security than the latter (Ciută, 2009; Floyd, 2016). Others argue that the meaning of security is always subject to negotiations and constant challenging depending on the context, which may result in its eventual transformation beyond fixed logics (Stritzel, 2011, pp. 346–347). Similar arguments can be also made concerning fixing the logic and meaning of risk. Assuming that risk is inherently an un-securitized or a de-securitized articulation, as argued by Corry (Corry, 2012), overlooks the ways through which risk has been used to facilitate and enable securitization in some cases rather than having a desecuritizing effect (for example, see: Elbe, 2008).

However, this thesis takes a different line of criticism to the fixation of the logic(s) of security and risk and their nexus in the study of cybersecurity. It argues that security and risk in the infosphere are not *just* what human actors make of them, and therefore their logics should not be tied exclusively to those actors' intentionality,

perception, and representation. Emergency measures should not be perceived as subject only to human securitizing actor's intentions and to human audience's acceptance. As will be substantiated in the next chapters, even with the presence of an intentional actor and a desire to go beyond the 'ordinary' or 'normal' in cybersecurity, the materialities of information would serve as a barrier that limits such actions. Similarly, the conceptualisation of existentiality – not its normative disposition – should be further interrogated. There remains a gap in determining what it means for a threat to be existential and analysing the link between existentiality on one side and immediacy, urgency, and the physical on the other. In application, many studies focus on problematising the extraordinary measures assumption rather than existentiality; assuming that it suffices to present a threat as 'so severe' or serious for it to be considered existential (for example: Collins, 2005, p. 571). By extension, whether digital information can be existentially threatened or constructed as such is an important question that the cyber securitization literature did not engage with. In short, adopting a non-anthropocentric approach that considers the materiality of information reveals the problematic anthropocentrism of the securitization theory's fixed logics.

Conclusion

This chapter developed a non-anthropocentric informational framework for studying cybersecurity that brings together security and risk literatures, the philosophy of information, and new materialism. It substantiated three main assumptions that form the core of this framework: (1) cybersecurity is informational; (2) information is a peculiar entity; (3) cybersecurity should be theorised differently. This framework thus challenges the securitization theory and the cyber securitization literature by breaking the link between subjectivity and human agency, investigating the ontology of information as the ultimate referent object of cybersecurity, and moving security logics away from existentiality, exceptionality, and emergency.

Firstly, cybersecurity is informational in essence. The connection between 'cyber' and 'information' in popular, academic, and policy discourses has roots in the evolution of cybernetics and information theory. Information is fundamental to computer science, software engineering, and all the sciences and technologies behind the tools and targets of cyber incidents. Computer science is even defined sometimes

as the science of information-processing or information-transforming processes. All categories of information, be it syntactic, semantic, or pragmatic, are the core of cybersecurity threats and policies. Moving towards information thus marks a study of the ontology and materialities of cybersecurity as opposed to the securitization's theory focus on discourses and speech acts.

Secondly, information is peculiar. Unlike new materialism that did not distinguish between the agential capacities of different types of matter or non-human things, the thesis argues that information is different. Information can be distinguished from matter and energy by its complexity, multiplicity, and transformational capacity. It is a fundamental force behind all objects' being and for driving many changes in the world. Specifically, in the next chapters, the thesis will focus on three main properties of information that co-produce the logics of cybersecurity. The first is intrinsic uncertainties of information systems; the second is the agential capacities of codes/software; and the third is the simultaneous physicality and non-physicality of information. Each of these three properties will be discussed in a separate chapter in relation to the logics of security in the infosphere.

Thirdly, given the informational ontology of cybersecurity and the peculiarities of information as such, it can be argued that cybersecurity is in turn peculiar. Understanding this peculiarity demands a new conceptual and methodological framework that deals with the anthropocentric limitations of securitization theory. In this framework, information is approached as a co-constitutive force of cybersecurity, whose agency is inherent to its existence and not necessarily bound to its relationship with other objects. Though it does not deny the significance of the human subject, the thesis gives more weight to information to counter the anthropocentrism currently present in the cybersecurity literature. Methodologically, the thesis focuses on information rather than particular cyber incidents as agential in cybersecurity. In addition, discourse analysis is used in examining the empirical data by considering the intra-action between the material and the discursive together with the performativity of information. Using this non-anthropocentric informational framework, the thesis aims to move cybersecurity beyond the fixed logics of security and risk, towards the

logics of negentropy, emergence, and noise, in constructing the notion of entropic security.

In the following chapters, the thesis will show how the indeterminacies of information systems; the agential capacities of codes/software; and the complex (non-)physicality of information engender peculiar logic(s) of security in cybersecurity, that differ profoundly from the aforementioned logics of securitization, and that are better studied through the notion of 'entropic security'. Entropic security, as an information-theoretic notion, moves cybersecurity from *absolute security to negentropy*, from *emergency to emergence*, and from *existentiality to noise*. This will be demonstrated by examining the disordered nature of the field of cybersecurity and its tendency towards increasing insecurity due to the intrinsic uncertainties of information systems. The thesis captures these uncertainties and disorders through the concept of entropy and reconceptualises cyber defence as 'anti-entropic practices' aiming at the avoidance of absolute insecurity; i.e., aiming at negentropy (Chapter 4). In addition, the thesis will examine the peculiar agential capacities of codes/software and how they challenge human control through the logic of emergence. This is done by exploring how codes/software undermine the centrality of human intentionality as a basis for constructing enmity; and how they co-produce the subjects/objects of cybersecurity (Chapter 5). Finally, the (non-)physicality of information will be studied in light of how it reduces existentiality to being just *another* discourse in cybersecurity. This analysis will highlight the significance of *mundane* cybersecurity that can evoke urgency without existentiality, and therefore can be studied through the logic of noise (Chapter 6).

CHAPTER (4)
UNCERTAINTIES AND DISORDERS IN INFORMATION SYSTEMS: CYBER DEFENCE AND THE LOGIC OF NEGENTROPY

> "If you really want to secure your computer, it is best to turn it off, disconnect it from the Internet, and if you really want to be secure, do not allow any person to get near it, open up the cover, pull out the hard drive, and hit it with a hammer until it no longer can be read." - Philip Reitinger, DHS (Protecting Cyberspace as a National Asset, 2010, p. 8)

Introduction

Information, the previous chapter argued, is different from matter and energy. This difference entails a wide set of properties that are inherent to the existence of information and that give it an autonomous status. Such properties are co-constitutive of peculiar logic(s) for cybersecurity that stands in tension with securitization theory's and many of its critiques' assumptions about security. This chapter focuses specifically on one property of the operation of information systems to illustrate this argument: intrinsic uncertainties and disorders. Studying uncertainties through an informational lens differs from existing understanding in the field of Security Studies. Although there is no independent literature on uncertainty as such (Pettersen, 2016, p. 41), it has been extensively studied as part of theorising the concept and politics of *risk*. Uncertainty is sometimes viewed as a counter concept to risk, assuming that the latter is linked to probability instead (Burgess, 2016; Petersen, 2016), or as integral to it (Aven, 2016). In other accounts, both risk and uncertainty are analysed as neo-liberal constructs (O'Malley, 2012), composed of multiple material and discursive elements, for governing what is projected as ungovernable (Aradau & Van Munster, 2007). Notwithstanding those different formulations, uncertainty has been largely approached as a point of distinction between security and risk; e.g., risk deals with the management of *uncertainty*, while security is concerned with the management of *insecurity* (Kessler & Daase, 2008).

This chapter, however, approaches the concept of uncertainty in a different way. It gives more weight in the analysis to uncertainty as such, as well as its temporalities and trajectories, than the ways it is tamed or governed by a human actor. Importantly, it presents an argument that uncertainty is an intrinsic property of the

ontology of information and the operation of information systems. This property, in turn, co-produces a conceptualisation of cybersecurity that goes beyond the traditional distinctions between the logics of security and risk. This is a kind of security that the thesis conceptualises as 'entropic security'. The chapter uses the definition of entropy as uncertainty and disorder both literally and analogically in presenting the logic of *negentropy* as the essence of cybersecurity and cyber defence.

In a literal sense, entropy defined as uncertainty in information theory is used to investigate the indeterminacies of information systems and their implications on cybersecurity practices. It seeks to show the ontological nature of such uncertainties and their pervasiveness across the past, the present, and the future. Analogically, entropy understood more generally as disorder in cybernetics and thermodynamics is used to explore the peculiar temporalities, logic(s), and essence of cybersecurity. Here, the analogy of entropy adds a temporal, processual aspect to the conceptualization of security and captures the complex interdependencies of cybersecurity. This informational analysis of uncertainties and disorders, the chapter argues, allows for a conceptualisation of cyber defence as *anti-entropic practices* aiming at fighting the force of increasing disorder and absolute insecurity in cybersecurity; i.e., aiming at *negentropy* (negative entropy).

To unpack these arguments, the chapter starts with an explanation of the concept of entropy defined as uncertainty in information theory. It shows how entropy has always been intrinsic to the theorisation of information and its ontology on one side, and to the practical operation of information and communication systems on the other. The second section moves from theory to practice by analysing the uncertainties of the cybersecurity environment, which the chapter conceptualises as the 'entropic space of cybersecurity'. It focuses on four main examples of how this entropic space manifests itself: vulnerability analysis, intrusion detection, attribution and damage analysis, and the lack of technical knowledge. In the third section, entropy is defined as disorder, based on cybernetics and thermodynamics. Here, entropy is used analogically to construct an understanding of the essence and logic(s) of cybersecurity as essentially entropic, i.e., tending towards disorder. It introduces the logic of negentropy as a way of understanding the essence of cybersecurity and cyber defence.

1. Entropy as uncertainty in information theory

Entropy first emerged in the 19th century as a major concept in the physical sciences, specifically in thermodynamics (Greven et al., 2014, p. 1) - a field that studies energy and its transformations (Ness, 2012, p. 1). Later, the concept moved to information theory in Claude Shannon's mathematical theory of communication (Shannon, 1948), and in Norbert Wiener's cybernetics (Wiener, 1948). Although entropy has been conceptualised and employed differently in these two fields, it can still be argued that "The Physicist's entropy and Shannon's entropy are two sides of a coin" (Siegfried, 2000, p. 66). Likewise, and as will be shown below, both formulations of the notion of entropy can provide important insights about the ontology of information and contribute to the theorisation of cybersecurity as entropic security.

Information has always been connected to the concept of entropy in the development of information theory. Shannon defined information as the measure of entropy in any system. His main concern was how to get the most amount of information to travel in communication media, regardless of its content, and minimising the degree of noise or uncertainties, which he called *entropy* (Vedral, 2018). He assumed that when entropy (here to mean uncertainty) increases, the amount of information also increases (Behrenshausen, 2016, pp. 30–76).[27] At first glance, this assumption that information is entropy may seem counterintuitive. Justifying this claim requires an understanding of the probabilistic conceptualisation of information that Shannon introduced. In probability theory, information is defined by the surprise factor. If it is known that a certain event is probable, then getting informed about its occurrence is no news, and thus no information. Inversely, if something is not likely, knowing about its occurrence represents a large amount of information (Lombardi, 2016). This can be seen as a relationship between probabilities and subjective degrees of belief (Milne, 2016). In the same vein, according to Shannon, information is inversely proportional to probability - though he gave probability an objective existence regardless of meaning. By probability he meant statistical probability.

[27] Some scholars regarded this assumption about the direct proportionality between information and entropy and both concepts being synonyms as a logical contradiction in Shannon's argument. For more information, see (Stonier, 2012).

Applied to communication, Shannon assumed that when a message is sent by a source, this represents an activation of one possibility among many, because theoretically all messages are likely to occur. Hence, there is an intrinsic level of uncertainty in communication systems linked to the choices that the sender makes about sending a message. If the message is predetermined and known by the receiver, there will be no need for communication (Gregoire & Catherine, 2012, pp. 114–115). It is like tossing a coin: getting one side is one bit of information that reduces the uncertainty of two probable states. Here, information is not a given; it is rather "the progressive unfolding of this relation between uncertainty and certainty" (Malaspina 2018, 41). When an event of a message unfolds, information works in a dynamic way, under various predictability and unpredictability levels.

In practical terms, the fact that information systems involve multiple layers of processing and interpretation leads to inevitable distortions. Distortions can result from overload, noise, truncation, inconsistency, imprecisions, etc. Accordingly, any information representation can be seen as essentially 'controlled distortions of the original information' (Ratzan, 2004, p. 3). Furthermore, the interaction of information systems with thermodynamic subsystems results in the propagation of uncertainty and growing entropy. For instance, in communication devices, information sent transmits as energy from one end to the other, i.e., pulses of light or waves. It is inevitable that during the transmission process some energy gets distorted, subject to disturbances in the channel through which that information is being transmitted. This means that information that reaches the receiver can never be as the original, and thus it cannot be deterministic.

In addition, uncertainty is intensified in the case of digital information systems as compared to analogue ones. As argued by one study, "The essence of the bit is the uncertainty inherent in it" (Kafri & Kafri, 2013, p. 135). Analogue means of communication are less sensitive to noise due to 'data redundancy'. For example, in the case of an analogue transmission of a picture, what is received is an exact version of the original one. If the transmission process is subject to noise, e.g., blur, the quality of the received image may be reduced, but it will not be totally destroyed. So, if one or more pixels are corrupted, it will just leave a blank spot, while the rest of the picture remains

enact. But in case of digital transmission, the existence of noise can corrupt the entire picture. For example, the colour blue in a digital picture showing a blue sky would be encoded by a number of bits that if distorted will distort the entire picture's colour (Kafri & Kafri, 2013, p. 120). Because computing involve a huge number of operations, it is prone to error, and any such error will lead to loss of information (Keyes, 1977).

The underlying idea behind this analysis is that entropy is a default state. Any system that does not have uncertainty is a system without information (Behrenshausen, 2016, pp. 30–76). Decreasing such entropy is one definition of communication: when communication occurs, it is capable of reducing entropy (Cannizzaro, 2016). Furthermore, there is an assumption that communication channels are always noisy, and *minimising* - rather than entirely eliminating - such noise is key for successful information transmission. In these systems, information involves the act of selection among various probabilities to reduce uncertainty, which is in itself a process marked by lots of indeterminacies (Cannizzaro, 2016). Thus, although uncertainty is not a property of information as such, it can be said that it is a property of its existence. Put differently, information in itself does not engender uncertainty, yet uncertainty is intrinsic to its conceptualisation and to its ontological makeup. This is perfectly put by one author, who argues "…information is carved from that entropic space" (Wicken, 1987, pp. 180–181).

2. The entropic space of cybersecurity

> "The corollary of constant change is ignorance. This is not often talked about: we computer experts barely know what we are doing. We're good at fussing and figuring out. We function well in a sea of unknowns. Our experience has only prepared us to deal with confusion. A programmer who denies this is probably lying…"(Ullman, 1997, p. 110).

The theoretical link between information and entropy, as well as its reflection in the operation of information and communication systems, similarly unfolds in cybersecurity. Cybersecurity too is carved from an entropic space, where uncertainty is ontological and marks a default state. These uncertainties have far reaching implications on the sort of policies implemented to secure against cyber threats and importantly, on the span of the *possible* in cybersecurity. The entropic space of cybersecurity redefines the temporality of uncertainty as theorised by the security-risk literature. That is, the

uncertainties of cybersecurity are not necessarily future-oriented or concerned with future unknowns (for example: Stockdale 2015); they are also linked to the past and the present. To illustrate this point, four examples will be discussed to show some facets of the entropic space of cybersecurity, in which different types of uncertainties and temporalities come together.

2.1. Vulnerability analysis

All networks, processes, operating systems, applications, and even devices in information systems operate through lines of codes written by programmers and software vendors. A security vulnerability is an error or a bug in coding, design, or modelling that can be exploited for attacking the system or network. Bugs are either introduced intentionally for malicious use, often called 'backdoors', or unintentionally as part of unplanned implementation or design errors. They vary in their severity and exploitability; not all bugs are exploitable and thus not all necessarily qualify as *vulnerabilities*. Some may give the attackers limited privileges on the system and others may allow for full remote control of the compromised target (Ablon & Bogart, 2017, pp. 1–2).

Unknown vulnerabilities are sometimes called 'zero-day vulnerabilities' or simply 'zero-days' for short. They are the ones that are unknown to the software vendors and for which no patch (fix) is available. Hence the name 'zero-day', which refers to the number of days the vulnerability was known to the target before it is exploited. These are the most difficult to detect and thus difficult to defend against. Because of that, a large market for zero-days is becoming very popular, in which governments and several other entities, and even individuals, participate.[28] These markets are primarily 'information markets', since they sell knowledge about the potential results of exploiting specific vulnerabilities - knowledge that the

[28] The markets of vulnerabilities and zero-day exploits can be classified into: white, grey, and black markets. White markets are usually the bug bounty programs run by many companies such as Google, Facebook, and Microsoft that bug hunters participate in with the responsibility to disclose found bugs to those companies. Grey markets are the ones that the intelligence agencies and governments participate in for either offensive or defensive purposes. Black markets are used solely by criminals for malicious use (Libicki et al., 2015, pp. 41–59)

vendor/user/target does not possess. As said by a zero-day vulnerability seller and noted by one study “we don’t sell weapons, we sell information” (Fidler, 2016, p. 280).

According to the DHS, 90 percent of all reported cyber incidents result from the exploitation of bugs (errors) in software coding (Department of Homeland Security, n.d.). Any single software contains millions of coding lines, in which errors are mostly inevitable. Consequently, it is widely acknowledged by most cybersecurity actors that all software would always have bugs of some sort. Some can stop the system from working, interrupt connectivity, or cause irregularities in the operation of certain devices. Others, however, are security vulnerabilities that can be exploited for hostile cyber operations that affect the confidentiality, integrity, and availability of information (Winkler & Gomes, 2016, p. 43). According to one study, before testing, there is an estimate of 20 bugs in every 1000 lines of coding; a number that can decrease by only one or two after testing (Libicki et al., 2015, p. 42). This inevitability of bugs has always been emphasised by almost all software programmers and engineers. They acknowledge that ‘there will always be another bug’ in every software, considering the complexity of information systems. It is even argued by some experts that errors are more prevalent and more problematic in software design than in any other technology, and that no matter how skilful the people performing software reviews are, some bugs will remain undiscovered. This creates a belief that bugs and the uncertainties they produce are ‘endemic to programming’ and that they are the ‘natural hazards’ of information systems (Nissenbaum, 1997, pp. 51–52).

Inevitable, undiscoverable vulnerabilities mean inevitable uncertainties and a large number of unknowns and *unknowables*. It is almost impossible to know beforehand how a certain software would react with the hardware it is installed on or with other programs on the system (Ormes & Herr, 2016, pp. 5–6). Furthermore, even in the case of known vulnerabilities for which patches are available, there is no guarantee that a patch will solve the problem. In many cases, a patch can contain more security holes that are not discoverable unless applied or tested on the system. The unpredictability of how the system will react to the applied patch and how the elements of that system will interact with it adds another level of uncertainty that challenges human control (Libicki et al., 2015, pp. 41–59).

2.2. Intrusion detection

Intrusion detection systems (IDSs) refer to processes through which malicious activities on the system are detected by analysing the possible signs of incidents that violate the system's security policy and standard practices. Intrusion prevention systems (IPSs) involve a similar process, but one that does not stop at detection. An IPS seeks to prevent the intrusion from succeeding or spreading. It can do so by stopping the intrusion itself and terminating the connection used in the attack, and thus blocking access to the target, or by changing the environment of the system configuration and removing/changing the malicious content of the attack (Scarfone & Mell, 2010, p. 177,178).[29]

Unlike the military sector in which the first steps of an attack may be detectable, the non-physical elements of information – which will be discussed further in Chapter 6 – can make a cyber intrusion invisible to the target for a long period of time. One report indicated that security alerts are generated for only 9% of recorded cyber incidents and that 53% of attacks infiltrate unnoticed (FireEye, 2012, p. 6). Additionally, data shows that the average number of days to identify breach incidents was 206 in 2019; rising from 197 in 2018 and 191 in 2017 (IBM Security, 2019, p. 49). It is also mostly other entities - particularly the FBI in the US case - that notify the victims that their systems have been compromised (Protecting America From Cyber Attacks 2015, p.8). This is strongly related to the inherent multiplicity of information and its emergent properties. Since complex information systems are diverse and constantly changing, it is challenging to keep a static image of the topology of networks. Given this complexity, the data produced by intrusion detection systems is often ambiguous. It is common for attacks to be mistaken for errors or over-load signals and vice versa. This is because the existence of anomalies is a fundamental characteristic of certain systems (Lazarevic et al., 2005, p.25). In consequence, based on a survey conducted in 2016, of all the malware

[29] A very important example for detection and prevention systems is the EINSTEIN program run by the DHS. EINSTEIN is a system that aims at detecting and blocking attacks at the federal level and providing information to the DHS for accurate situational awareness for public and private partners. The first EINSTEIN was launched in 2003 with the aim of recording the network traffic in all federal civilian agencies in the executive branch for it to be analysed and for malicious activities to be identified. EINSTEIN 2 used signature-based methods to issue alerts on potential attacks. EINSTEIN 3 accelerated (E3A) was developed in 2012 not just for detection but for actively stopping the detected attacks (*EINSTEIN*, n.d.).

alerts that private companies investigate, 40 percent are false positives: indicating a threat that does not exist (Ponemon Institute, 2016). This happens despite the continuous progress in advanced intrusion detection systems.

2.3. Attribution and damage analysis

Another major source of uncertainty in cybersecurity is the problem of attribution. Attribution refers to the process of identifying the source of the attack, the identity of the attacker, and their motives. In fact, there are many technical barriers related to the nature of the internet as a packet-switching network that impede attribution and forensic analysis. Firstly, cyber incidents can be initiated by botnets, or compromised devices that are centrally controlled by the attacker or 'the botnet operator'. This means that the attack is distributed among different nodes of thousands of machines with multiple IP addresses, and thus making it difficult to correlate the malicious packets to a single source (Boebert, 2010).

Secondly, the use of proxies is another source of complication because it changes packets' IP addresses and provides anonymity over the internet for privacy purposes or otherwise. For example, big corporations sometimes use Network Address Translation (NAT), a technology that reduces the number of IP addresses shown publicly. This technology would hence establish a link between any potential intrusion analysis with the institution itself rather than a certain node inside it. Onion routing is another example of a method used for maintaining communication anonymity by hiding the IP address of the sender. The onion router operates through a layered cryptographic system that encrypts the packet and its content from a hop (i.e., onion router) to another, keeping the sender anonymous. Thirdly, ISPs use dynamic IP addresses, meaning that a new IP address will be assigned to the user every time they connect to the internet. This means that the packets a certain user sends and receives may have different IP addresses over time (Boebert, 2010).

Fourthly, there is the problem of what a study referred to as 'the dilemma of interpretation' or knowing the real intentions of the intruder in this environment of uncertainty. In the traditional military sector, an invasion of troops is often interpreted as an offensive attack and a breach of sovereignty even if the intruder's intention was

enhancing their defence. Yet, in cybersecurity, a system intrusion can be done for the mere purpose of intelligence gathering, even among friendly nations, without damaging the system or resulting in any kind of harm. This leaves the targeted state with a dilemma of whether to interpret this as an intelligence collection, contingency planning, or as a preparation for a cyber attack. This is what the study called the security dilemma of cybersecurity that is arguably more complicated than the security dilemma of conventional sectors (Buchanan, 2016). This does not mean that attribution is not technically possible, it rather shows the severity of the uncertainties that overshadow attribution as one part of cybersecurity's threat logics and policy response. This is also important considering that sometimes even the main target of the attack is not known in the very early stages, particularly if the attack spreads across a large number of systems.

Another level of uncertainty can be seen in the process of damage analysis following a cyber incident. Even after detection, and notwithstanding attribution, it is difficult to determine with great certainty the full extent of the resulting damage. To date, there is no agreed-upon protocol for defining and measuring cyber damage; most of the available figures are inaccurate estimates. Consequently, if multiple companies were targeted by the same attack, each might have its own, different estimates of the damage scale and resulting losses. This all makes it very difficult to predict an attack on a particular target in the future, or to anticipate the full magnitude of the resulting damage or costs. Since the data available is not enough, quantifying cyber risk to make generalisable statistics remains very problematic. As argued in a congressional hearing: "A locksmith can tell you how long a safe can resist an attack with certain kinds of tools. A computer scientist can't do the same" (Cybersecurity – Getting It Right, 2003, p18)

2.4. Lack of awareness and technical knowledge

It is not just the absence of information that creates uncertainties in the infosphere; it is also the absence of *technical knowledge* and *awareness* even when information is available, which is sometimes referred to in cybersecurity discourses as the 'knowledge gap'. This aspect can be framed within the subjective property of information mentioned in the previous chapter. Even when information is available, it might not be informative for everyone. In cybersecurity, its informative quality is bound by the

technical nature and complexity of information systems. Given the complexity and indeterminacy of such systems, understanding many cybersecurity problems requires a certain level of awareness and expertise that may not be available outside the circle of cybersecurity experts. This is one explanation why the majority of cyber attacks target known vulnerabilities for which patches are already available.

In a survey of over 3000 security experts in nine countries, including the USA, respondents indicated that 60 percent of system breaches in 2019 were linked to known vulnerabilities for which patches were available (Ponemon Institute, 2019, p.5). In fact, many known vulnerabilities go unpatched because the users or operators of the system are either unaware of them, unaware of the patching methods, or struggling to keep up with the great number of patches that are issued monthly. It is common that users ignore patches or run outdated software even in cases of critical vulnerabilities; not knowing the possible cascading effects this may have on the security of everyone. Hence, discovering vulnerabilities and issuing patches is never the end of the road in cybersecurity.

Again, the nondeterministic nature of information systems is one factor that complicates the patching process. Patching is an error-prone process and one that is never fully controllable by humans. It is difficult to predict how the system's elements are going to react to the applied patches. In some cases, applying a patch may result in even more security holes or lead to disabling the system altogether. This problem intensifies in the case of Industrial Control Systems (ICS) through which critical information infrastructure are operated. On the ICS vendors side, there is reluctance to issue patches straight away following the knowledge of certain vulnerabilities, because multiple tests and validations have to be performed first to see how the software operation would react to the patch. On the users' side, there is a need to do similar testing for the patch on the ICS-specific environment to minimise the chance of unintended consequences. This is a time-consuming process, especially that the system would need to be taken down completely for the tests to be done and the patches to be applied. That is why patching a system, particularly ICS, may happen long time – sometimes years – after the vulnerability is discovered (Lee, 2016, pp. 34–35). It can be thus argued that the more complex and vital the system is, the more challenging the

process of patching will be. According to one security expert working in the communication sector:

> "The composition of systems, the components of complex systems working together properly is a very, very difficult and unsolved problem…It is not that the administrators are irresponsible, or that the vendors haven't supplied good tools, it is that we don't know how to do it easily, reliably and without breaking something else" (Cybersecurity – Getting It Right, 2003, pp 43,44).

Furthermore, technical knowledge about patching and system configuration is usually lacking in the case of ordinary users, who are targeted the most by hostile cyber incidents. The fact that users sometimes cannot differentiate between secure and unsecure software diminishes their power to influence the market of cybersecurity or to push for more secure software by-design. This indirectly encourages the 'fix it later' culture that drives software vendors to introduce buggy software in the market, and then issue incremental patches gradually; meanwhile subjecting software to possible exploitation of potential vulnerabilities (Chong, 2016, pp. 73–74). This knowledge gap does not only exist between ordinary and skilled users, but also between local and federal governments on one side, and the public and private sector on the other side. A federal executive once noted in a congressional hearing in 2005 that when they were communicating patching information with town supervisors, one replied saying: "I don't understand what you mean by patching. When I hear the word, I look for duct tape" (The Future of Cyber and Telecommunications Security at DHS, 2005, p60).

These are just some of the many examples of the protracted entropic space of cybersecurity, co-produced by the peculiarities of information. It is a space in which uncertainty cannot be simply reduced to a human discourse, empirical non-knowledge, or to a particular future temporality. It is *ontological uncertainty* that is intrinsic to the information systems that cybersecurity aims to protect and that is pervasive across the past, the present, and the future. This is not a transformation from security to risk that follows Ulrich Beck's argument on the emergence of a 'risk society' in the second modernity, in which the unknown, incalculable, and uncontrollable dangers are massively increasing (Beck 1992). It is also not a transition from the semantic field of security to that of risk as suggested by risk studies that discuss modern conceptualization of security (Kessler and Daase 2008). It is a recognition that

cybersecurity is *born* a risk society as such due to its informational ontology. This is a security environment that the concept of entropy – defined as uncertainty – directly captures. Meanwhile, there is a lot more that entropy can add to the theorisation of cybersecurity, its evolutionary processes, and its essence. This can be made clearer by exploring another meaning for entropy as defined in physics: entropy as disorder.

3. Entropy as disorder and the essence of cybersecurity

Another way entropy appeared in the information theory literature was in Wiener's cybernetics (Wiener, 1948, 1988). Wiener assumed that there is a natural connection between information and entropy, considering that information is the measure of the system's organisation, while entropy is the measure of its *disorganisation*. Thus, unlike Shannon who viewed information as positive entropy, information to Wiener is the inverse of entropy, or negative entropy. This is an idea he derived from physics and the second law of thermodynamics. In physics, entropy represents the assumption that matter and energy are always changing and in every change they lose part of their structure, hence of their information. Any physical change of matter-energy produces a certain loss of order or information, and entropy is the measure of that lost information. This is part of a metaphysical view of the universe that sees time as moving in one direction: towards more loss of information and order, which defines the 'ultimate fate of every physical entity' (Bynum, 2008, p.17).

Physical entropy explains the natural tendency of ice to melt for example, and for hot things to eventually cool and lose their heat, unless acted upon by an external force. Even when entropy seems to be decreasing in parts of a system, it must be increasing in others. So, for instance, if a fridge is cooling and experiencing a decline in entropy, it is because heat is coming out of it and consequently raising the entropy of its surrounding. Thereby, it is assumed that "the entropy of the universe never goes down" (Davies, 2019, p.32). From a thermodynamics perspective, information processing of all types, be it encoding, transmission, decoding, etc., leads to energy dispersion and increases entropy (Li and Du, 2017, pp. 6–8). This is how many scholarly contributions connect information theory and physics (Davies, 2019, pp. 27–66), as in the work of Rolf William Landauer (Landauer, 1991, 1999).

3.1. Entropy as a security analogy

Entropy as disorder can serve as an informative analogy to think about cybersecurity. *Firstly*, the analogy of entropy can help in understanding how some cyber insecurities are not just accepted, but often also embraced as a natural product of complex information systems. When Wiener conceptualized information as negative entropy, he did not mean that entropy itself is negative. To him, entropy demonstrates reality's natural gravitation towards disorganization and chaos (Wiener 1948, 1988). Similarly, the mathematician Warren Weaver distinguished between what he called 'spurious uncertainty' that results from the influence of noise in information communication, and 'desirable uncertainty' that reflects the sender's 'freedom of choice' (Weaver 1949, 13). Even when viewed negatively as a problem of communication, noise remains integral to the existence of information.

In cybersecurity, it is widely believed among many actors that "complexity is the worst enemy of security" and that "everything about complexity leads towards lower security" (Overview of the Cyber Problem, 2003, p. 11). The complex operation of information systems can engender an understanding of absolute security as something that contradicts the very essence of information being dynamic and complex. As put by a security expert: "So I don't believe you can ever have a dynamic, effective, productive system and be 100 percent secure. It would violate the reason why you built it" (Cyber Insecurity, 2007, p. 55). Again, here, complexity - and in turn insecurity - is ontological. It does not necessarily reflect a human perception or choice of 'embracing risks' and 'thriving on uncertainties' for commercial or economic gains as part of risk governance (Amoore 2013, 24).

Ontological uncertainties that are normalized, or even embraced, in cybersecurity can be explained by Frederick P. Brooks' distinction between 'accidental' and 'essential' complexity in software engineering - in line with Weaver's distinction between spurious and desirable uncertainty. For Brooks, the complexity of software systems and digital computers is incomparable to any other artefact, because of the large numbers of states they can have and the non-linear interactions among their elements. These complexities are not accidental; they are *essential* to the existence of software. Though many methods have been developed to handle accidental complexities, there is

'no silver bullet' for dealing with essential complexities (Brooks, 1987). Likewise, as argued by an adviser in a risk and insurance company speaking about cybersecurity, "…there is no silver bullet and that there is always going to be some residual risk, despite how strong your practices are" (The Role of Cyber Insurance in Risk Management, 2016, p. 37). In this way, cybersecurity becomes inherently a kind of entropic security based on an understanding that cyber threats are intrinsic to the very makeup of the systems that need protection.

Secondly, the analogy of entropy adds an important temporal dimension to the conceptualisation of security. Thermodynamics entropy is connected to a particular view of progress that distinguishes the past from the future, referred to as 'the arrow of time'. It is an assumption that certain physical phenomena are irreversible. Melting ice cubes is an example of a spontaneous phenomenon for which reversibility - i.e., water turning into ice - requires an external source of energy (Kisak, 2015). This temporal aspect of entropy and its arrow of time is evident in cybersecurity. For example, data shows that in the period between 2014 and 2019, the likelihood of a data breach grew by 31 percent; malicious and criminal attacks increased by 21 percent; and the average total cost of a data breach increased by 12 percent (IBM Security, 2019). As a result, many actors believe that cyber dependency and the complexity of information systems are unavoidable, and mostly irreversible. Many discourses frame the cyber threat around the idea that cyber dependence 'will continue to increase' (The Department of Defense, 2006, p.9), and that 'Complexity is something we can't change' (Overview of the Cyber Problem, 2003, p. 11). Accordingly, the future of cybersecurity is conceived as essentially more threatening than the present. Just like the one-directional physical entropy, cyber threats are seen as always evolving, ever-increasing, and becoming more serious every day. As expressed by a representative from the DHS describing the cybersecurity challenge: "the train has left the station" (Cybersecurity, 2010, p. 40).

It follows that being 'secure' is perceived by most actors as more of a *process* than a *goal* or a *state* per se. Secure is the application of enough security measures that cope with the ever-increasing cyber threats, which do not necessarily eliminate them. That being the case, normative adjectives are often attached to cybersecurity, such as 'good security', 'weak security', 'agile security', 'bad security', etc., that seem counter-

intuitive to the semantically positive notion of security. Security in this way becomes a non-binary concept that breaks the distinctions between 'secure' and 'insecure'. This processual, temporal nature of entropic security is best exemplified in statements like "cybersecurity is a journey and not a destination" that is repeated by the government (Protecting Cyberspace, 2012, p. 21) and the private sector alike (Securing America's Future, 2012, p. 43). Entropic security is a process, not an end goal or a status, because absolute security is unachievable.

Thirdly, entropy is additive, and therefore is a signification of complex interdependencies. The entropy of any certain system is calculated by summing up the entropy of each of its parts. This implies an intrinsic connection between all parts of the system and its overall thermodynamic properties. An air conditioner that is decreasing the entropy of a room by cooling it down is actually dispersing hot air that increases the overall environment's entropy (Kisak, 2015, pp. 17-24). The same logic applies to cybersecurity. As entropic security, cybersecurity is constituted by every single user of digital technologies, from individual citizens to corporations and governments. This creates an understanding that "cyber security is only as strong as its weakest link" (Protecting Cyberspace as a National Asset, 2010, p. 17), since an attack against one may affect the security of the rest. As one study put it, "Everybody is your neighbor on the Internet" and calculating one's risk has to consider that of others (Aycock, 2006, p. 3). Due to this interdependency, end-users are sometimes blamed for not updating their systems regularly, not necessarily for the sake of their own security, but for the negative implications of that on the security of the state (The White House, 2003, pp. 7–8).

By extension, even if entropy appears to be decreasing in one part of the system, it is increasing in others, as explained earlier in the fridge and air conditioner examples. This idea captures a very complex paradox in cybersecurity. Although in other security fields, such as economic or military security, more development can be linked to increasing security, this is not the case in cybersecurity. As noted by some actors, "cyberspace is becoming less secure even as security technologies improve" (Overview of the Cyber Problem, 2003, p. 11). There is a general belief that the more cyber dependent the state is, the more inevitably threatened it becomes. As argued in a congressional hearing, "the United States is at risk of becoming a victim of its own

success" (America is Under Cyber Attack, 2012, p.39). This growing insecurity does not just contradict with the development of security technologies, but also with the application of more security measures and more investment in cybersecurity. It is estimated that the global cybersecurity market has grown to $173 billion in 2020 from $88 billion in 2012, despite the simultaneous exponential rise in cyber threats (Columbus, 2020).

Finally, it can be argued that entropy is both a product of and a contributor to complexity. The physicist Boltzmann argued that entropy is proportional to the number of microstates in a system, or to the possible ways the different parts of the system can be distinguished (Kafri and Kafri 2013). This idea links entropy and complexity with multiplicity. Complex systems are generally non-linear; resulting in random outcomes. From a thermodynamic perspective, more randomness means higher entropy and vice versa. Likewise, cybersecurity as entropic security is complex and non-linear. The inherent multiplicity of information and the large number of sub systems that are connected to one another engenders non-linearity and a more entropic security environment. That is, entropy (defined as disorder) as a security analogy can help us understand the security implications of the complexities and interdependencies that characterize cybersecurity. This entropic nature is already acknowledged by the majority of cybersecurity actors, even if they do not use the term 'entropy' as such.

3.2. From absolute security to negentropy

Thus far, the chapter has made the case for the relevance of the concept of entropy for understanding the intrinsic uncertainties of cybersecurity and its disorderly nature. But how can entropy describe processes in the opposite direction; ones that aim at increasing order and organization? Assuming that cybersecurity is entropic does not deny the existence of a wide range of cybersecurity defence measures that target cyber threats/risks. It also does not dismiss the possibility of achieving progress. But such processes have their own peculiarities, and there remain many useful insights that the analogy of entropy can add in this respect.

In general terms, the assumption that the entropy of the universe is always increasing may seem to contradict humans' and modern sciences' strive for more order

and organization (Arnheim, 2010, p. 8). However, physicists would argue that the existence of entropy does not negate the possibility of *negentropy*: the increase in order and organization, i.e., negative entropy. In local systems (e.g., the fridge), negentropy and increasing order is always possible, which purportedly goes against the second law of thermodynamics. In global systems (e.g., the universe), however, the second law still holds. As put by Wiener: "There are local and temporary islands of decreasing entropy in a world in which the entropy as a whole tends to increase, and the existence of these islands enables some of us to assert the existence of progress" (Wiener, 1988, p.36). This means that the different parts of the system can experience negentropy even if the entropy of the entire system is rising.

This argument can be broadened to apply not just on parts of a system, but to the universe as a whole. From a cosmological point of view, some predict that the entropy of the universe will keep increasing until it reaches the maximum point of heat death. Others contend that if the physics conceptualization of entropy is acknowledged, more technology would mean more entropy. This is framed as 'the diminishing returns of technology' or the assumption that rather than solving our problems, technological developments decrease the overall amount of available energy in the world. This could also apply to industrial capitalism and modes of production that lead to overpopulation, pollution, and other negative implications that signify the demise of energy in the universe (Best, 1991; Rifkin & Howard, 1989).

Nonetheless, this view is challenged by other scholars who argue that the continuing expansion of the world is pushing the maximum point of entropy further, making it unlikely for heat death to occur. And this is how life continues to maintain its existence: through the force of negentropy (Kisak, 2015). This debate is connected to a more general one on the relationship between order and chaos. For instance, chaos theory argues for the non-linearity of complex, dynamic systems. Such systems would constantly produce randomness due to the inability to predict their future by observing their 'initial condition'. However, many scholars believe that chaos is not necessarily the opposite of order. They talk about the possibility of order and regularities emerging out of chaos and irregularities; i.e., 'irregular regularities' (Best, 1991, p. 203). This is what Toffler argued in the forward of a book named *Order out of Chaos*, speaking about how

entropy can be the creator of order, even in a spontaneous manner (Prigogine & Stengers, 2018).

Many scholars contend that evolution, biological reproduction, and processes of acquiring knowledge show a lot of negentropy (Sonne, 1985). Similarly, instead of viewing uncertainty antagonistically, it is sometimes approached positively as a possible driver for creativity and freedom, particularly in certain fields like arts and academic research (Smithson, 2012). According to Wiener, machines, just like humans, can exert such 'anti-entropic processes' (Wiener, 1988, p. 32). Floridi also assumes that informational entities are capable of decreasing the entropy of the universe, or at least resisting it (Floridi, 2013). Some even talk about what they call 'extropy', which is introduced as a post-humanist or even trans-humanist idea that technology will change human existence in an opposite way to the chaos that entropy suggests (Pepperell, 1995).

Negentropy that can increase in local parts of the system due to the existence of an external force, despite the increasing entropy of the whole, is analogous to cybersecurity. Even though the overall cybersecurity statistics all over the world show rising insecurity every year, there are always areas of improvement in specific fields, industries, organizations, or periods of time. As an example, though the total global average cost of system breaches has been increasing over the years, the year 2017 witnessed a considerable drop in costs. Likewise, though the overall breaches are increasing in number, a system glitch as a root cause for those breaches has been decreasing since 2015 (IBM Security, 2019). The inevitability of cyber insecurity makes such numbers look good in security evaluation even if the overall picture is worse. This is because, as argued by Chandler, failure is intrinsic to complex, non-linear systems – ones that informational systems resemble. 'Failing better' thus becomes a more achievable target than success (Chandler, 2014, pp. 1-14). This also reflects the nature of the processes of information that, as argued by Malaspina, represents a 'controlled way of falling', 'recuperated disorganizations', or 'repeated cycles of acquisition and loss of equilibrium' (Malaspina 2018, 73).

Hence, instead of defence strategies, cybersecurity measures are better theorised as *anti-entropic practices*. Nonaction means insecurity because entropy is the

default state. Cybersecurity interventions thus seek to resist the non-human force of entropy and increase negentropy in individual systems, even when the overall cyber insecurity is rising. And just like life is pushing the point of heat death further, cyber defence measures as anti-entropic practices are processes aiming at the avoidance of absolute cyber insecurity rather than achieving absolute security. Importantly, framing cybersecurity measures as anti-entropic aiming at negentropy considers the fact that they are not always directed towards a particular threat or a constitutive causality, but against the entropic force of increasing insecurity.

Given this, cybersecurity as entropic security explains the dominant discourse adopted by many actors that the essence of cybersecurity is the reduction of risks, threats, and vulnerabilities rather than their elimination. Such belief is not exclusive to the private sector as it might seem. As an example, it was explicitly mentioned in the US Presidential Policy Directive in 2013 that: “The terms "secure" and "security" refer to *reducing* [emphasis added] the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters” (The White House, 2013). A cybersecurity policy document issued by the DHS also defined the state of critical infrastructure’s security by that in which the owners and operators of such systems ‘manage risks’ and sustain ‘adequate security’ (Department of Homeland Security, 2011, p. 11). This results in an assumption that there is no ‘fool proof security’ (Cyber Security – 2010, p. 9), and that the occurrence of more cyber attacks is ‘not a matter of if, but when’ (DHS Cybersecurity, 2013, p.55).

Furthermore, similar to what Wiener described as ‘temporary islands of decreasing entropy’ (Wiener, 1988, p.36), the state of security in cybersecurity can be as temporary. The multiplicity and transformational capacity of information results in an understanding of cybersecurity as a ‘moving target’ or ‘a snapshot of a moment in time’ (Cyber Insecurity, 2007, p. 55), given its speed of change and dynamism. It is also argued that “cyberspace is the most rapidly evolving technology space in human history” (Oversight of Executive Order 13636 and Development of the Cybersecurity Framework, 2013, p42), accompanied by rapidly changing threat environment. This ‘kaleidoscopic change’ is seen as the only constant in information environments since the development of the first internet, ARPANET, making it difficult to catch up with every next

vulnerability or threat (Emerging Cyber Threats to the United States, 2016, p. 35). For example, a system that is updated and patched, can still have hundreds of unknown vulnerabilities, and a detected malware can change its signature making its first discovery ineffective. Therefore, patching is not entirely controllable by humans. A system that is updated today and cleaned of all vulnerabilities, can have hundreds of vulnerabilities that the user did not know about a day after. And even when a single component of an information system is presumably secure, there is no guarantee that it will remain as such when interacting with other components in an information system or infrastructure.

Hence, cybersecurity as entropic security is measured by the relative future improvement to the conditions of the present and the past. It is not totally fixed to the logics of defence against a present and urgent threat as securitization theory suggests, but rather aims at making systems relatively more secure in the future. This creates an understanding of the essence of security in cybersecurity as the management of risks and reduction of uncertainties, which in turn overshadows the ability of a human actor to take the emergency measures that securitization assumes is a precondition for security. Entropic security, thus, does not entirely subscribe to traditional logics used to distinguish between both risk and security in the literature. This can be made clearer by investigating the kind of policies and practices put forward to achieve cybersecurity in such an entropic space.

3.3. Anti-entropic practices in the infosphere

> **“**Are we doing everything we can? Of course not. Because everything we can doesn’t make any sense to do.” Bruce Schneier (Overview of the Cyber Problem, 2003, p40)

The entropy of information systems imposes conditions that enable, shape, and/or limit the kind of discourses that actors construct to securitize cybersecurity, and the sort of policies, strategies, and practices introduced to manage cyber risk/threats. All strategies of intervention proposed in cybersecurity assume a high level of uncertainty. As shown previously, the uncertainties of cybersecurity are not limited to the future. Uncertainties are invasive in thinking about both the present and past threats. Hence, the traditional distinction between uncertainty as incomplete, incalculable knowledge and risk as

measurable uncertainties does not necessarily hold in cybersecurity. Uncertainty lies at the centre of every single strategy applied to achieve cybersecurity; something that is evident in both the practice and discursive levels.

Before a cyber incident takes place, several long-term precautionary measures are usually proposed in order to reduce the potential threat/hazard and its damaging consequences. Although the risk literature assumes that precaution implies the possibility of prevention (Aradau, 2016), in cybersecurity this possibility is perceived differently. Cybersecurity as entropic security implies that cyber threats are generally continuous. Intrusions happen in massive numbers, and not all have the same level of criticality. There is a general perception of the need for risk prioritisation, which means that prevention would be possible for only a few incidents, but not all. Prevention appears more when the object of inquiry is CNI, which many argue should be approached with 'zero-tolerance'.

Importantly, prevention in cybersecurity is not necessarily about stopping one big incident, crises, or disaster. It is mainly about the prevention of cascading effects, attack spread, or stopping as many incidents as possible so that the overall threat is reduced but not necessarily eliminated. Again, making such practises anti-entropic rather than strictly defensive and aiming at negentropy rather than absolute security. Consequently, given this entropic nature of cybersecurity and the fact that most incidents happen with little to no warning, response is considered the core of cybersecurity policies and strategies. If most attacks cannot be predicted or prevented, the best that can be done is responding to them, by stopping them, limiting their damaging implications, and recovering from their consequences

3.3.1. Vulnerability reduction

As stated earlier, vulnerabilities are seen as a by-product of complexity in information systems. The more complex systems are, the faster they change, the more vulnerabilities they produce, referred to as 'complexity induced vulnerability' or 'negative technological synergy' (Hellström, 2007, pp. 417–418). Therefore, the proposed policies/strategies to deal with vulnerabilities always aim at their assessment, reduction, mitigation, and management, but not necessarily their elimination or total prevention.

To that end, proposed and implemented practices include manufacturing secure software ('secure by design' or 'secure out of the box') by automating coding, improving training for code developers, and implementing robust quality assurance that involves external certification and third-party reviews. They also include measures to ensure secure software deployment by developing easy-to-deploy, use, and configure products.

Yet, just like physical negentropy that can only succeed in individual systems, there is a high level of risk acceptance and prioritisation in choosing the targets of cybersecurity measures. As an example, many software vendors postpone security measures for after the software is released by issuing patches, instead of spending more time creating secure software from the start. Some companies launch bug bounty programs later to encourage researchers and white-hat hackers to discover vulnerabilities in their systems before they get exploited so that they fix them. This can be described as a postponed precautionary measure or as explained by chief technology officer in McAffee "It would be like taking a decongestant or a pain reliever when you have a cold, rather than eating healthy and exercising and building your immunity" (America is Under Cyber Attack: Why Urgent Action is Needed, 2012, p31).

3.3.2. Modelling, simulations, and exercises

Another anti-entropic method to manage the uncertainty and unpredictability of the infosphere, and to prepare for a cyber attack, is the performance of modelling, simulations, and exercises. These methods go back to the 1970s, when penetration testing was used to ensure the functionality of the system throughout the process of software and hardware development. They can be considered a form of 'anticipatory security' to 'inhabit the future', implying that vulnerability and failure are inevitable. Such method is particularly important in cybersecurity since a lot of the threat scenarios, especially the ones associated with major destructions, are either few or non-existent (Stevens, 2015, pp. 149–179). These practices imply the impossibility of prevention, and thus aim at managing the future threats by simulating them for better response when

an attack takes place. It operates under a worst-case-scenario assumption; i.e., preparing for the worst because it cannot be prevented.[30]

3.3.3. Prevention through access control

Access control is inherently an anti-entropic practice rather than one that simply defends against threats. It refers to a number of methods used to prevent unauthorised access to certain information systems, and to ensure that only authorised users can use them. It is commonly stated as part of the preparedness strategy to prevent, limit, and later identify cyber attacks. It is done through authentication by granting access to particular users; using unique identifiers (usernames, biometrics, etc.) to identify those users; validating the users' identity; and finally logging files and records to associate actions to particular users for analysis (Kim & Solomon, 2016, pp. 136–154). Besides, there are always continuous calls for improving encryption and the use of VPNs, firewalls, and antivirus software. However, the multiplicity of information and the huge number of diverse nodes in every system that resembles entropy's microstates, limit the utility of such measures. The more microstates, the higher the entropy and vice versa. As stated in Congress: "We are moving more towards a motel rather than a hotel model. In the hotel, there are one or two entrances and everyone is walking past the front desk. In the motel, every room has got its own door to the outside. It is a lot harder to secure that, and we are moving more towards that ladder" (Cybersecurity – Getting It Right, 2003, p35).

3.3.4. Deterrence and pre-emption

Although deterrence seems like an imposed analogy on cybersecurity that does not really work, it is still sometimes used as part of cybersecurity discourses, particularly in

[30] There are many examples for such simulations. For instance, since February 2006, the DHS has been conducting an exercise series in cooperation with the private sector and international partners called Cyber Storm (I, II, III, IV, V, and VI) which is considered the biggest government-sponsored exercise to-date. It aims at examining the entity's capability to 'prepare for, protect from, and respond to cyber attacks' potential effects', in addition to enhancing information-sharing for better situational awareness during attacks (Cyber Storm, n.d.). Similar to Cyber Storm are Blue Cascades, Black Ice, and Silent Horizon (Arquilla, 2009, p. 212).[30] There are also multiple red teams, blue team, and war games exercises performed by other agencies like the DoD. As an example, the National Cyber Range program run by the DoD conducts network testing and cyber capabilities' assessment testing periodically. And in an attempt to transfer the results to public, a televised simulation of a cyber attack called Cyber Shockwave wargame was conducted in 2010.

that of the military. Many studies have argued against the applicability of deterrence to cybersecurity, particularly given the uncertainties of attribution. However, Joseph Nye stated four main ways through which deterrence and dissuasion can take place in cybersecurity. The first is deterrence by punishment, or the use of retaliatory measures that do not have to be restricted to cyber. This is the type of deterrence in which the uncertainties of attribution play a major role. This is because an attack needs to be attributed to a certain source for punishment to be possible. The second is deterrence by denial, by improving cyber defences and building resilience. The third is entanglement, by investing in more interdependencies that raise the cost of the attack. And finally deterrence by norms, or the 'reputational costs' that can be imposed on an attacker in a way that harms their soft power (Nye, 2017). Stevens also discussed this normative aspect of deterrence as a way to change states' behaviour in cyberspace and deter adversaries, away from the traditional conceptualisation of military power (Stevens, 2012).

Among these four methods, the first two are the dominant ones in cyber deterrence discourses. Deterrence by punishment is especially mentioned when discussing cyber crimes and the fact that the absence of strong punishments does not provide adequate deterrence to stop cyber criminals. Strong defence and resilience are also portrayed as critical steps towards deterring the enemy. Yet, added to these two, offensive cyber operations are sometimes proposed as a necessary intervention to dissuade attackers, based on perceptions like 'the best defence is a good offense'. In practice, it is now common that states conduct operations by exploiting vulnerabilities in the target system and then characterising them as defence operations, if direct damage was not inflicted. The DoD in its cyber strategy of 2015 mentioned that it may perform cyber operations for the sake of deterrence and defeating adversaries (The Department of Defense, 2015). This is sometimes framed as 'active cyber defence', which may include non-disruptive practices like maintaining a presence on the adversary's network for information collection, or disruptive ones like 'hacking back' to recover stolen data for instance (Healey, 2019; Pattison, 2020) . However, pre-emptive measures in cybersecurity are still bound by its chronic uncertainties. This is because vulnerabilities may be patched and thus hindering the attempts to exploit them; exploits

may result in unintended consequences; or a targeted system may prove resilient to exploitation (Valeriano et al., 2018, p. 7).

3.3.5. Intrusion detection and prevention

IDSs and IPSs take place under a high level of uncertainty. As explained earlier, it is impossible for such processes to provide a completely accurate image about a certain system. In addition, if they are not 'rapid' and 'timely', detection and prevention's usefulness will be limited. This is again another example for how prevention has completely different logics in cybersecurity. The fact that intrusion prevention has to be preceded by detection means that the intrusion or at least its first steps have to occur first for them to be stopped or prevented. Hence, prevention inherently aims at stopping an intrusion that has already taken place in order to limit its progression or its damaging consequences, rather than preventing its occurrence. A successful prevention is therefore one that *quickly* detects an intrusion and *mitigates* its harm, not necessarily one that stops the intrusion from happening in the first place.

3.3.6. Resilience

In the risk literature, some deal with resilience as a response strategy to disaster or crises (Krieger, 2016), while others associate it with the epistemic regime of novelty and surprises (Aradau, 2014). It is sometimes defined as the ability of the system to 'bounce back' to a 'normal' status quo that needs to be preserved (Krieger, 2016; Petersen, 2016). In cybersecurity, resilience is an overarching concept that spans various logics and temporalities. It is proposed as both part of the preparedness and response strategies. It is the ability of the system to overcome intrusions or minimise the scale of their consequences, as per measures taken *before* an attack takes place. It is the survivability and adaptability of the system *during* an attack and its capacity to function properly and survive on redundancy. It is also system's ability to recover the consequences of the attack *after* it occurs. Moreover, due to the entropic nature of cybersecurity, resilience is not only fixed to disasters or crises and is not limited to novelty and surprises. Besides, given the parallels of the arrow of time and irreversibility in physical entropy, resilience as an anti-entropic process does not imply a 'normal state' that needs to be preserved, because the cyber threat is perceived as continuous in which

the ‘normal’ does not really exist. That is, the present is not fully secure, so bouncing back to it is not a target per se; rather, it is negentropy that is achievable.

Conclusion

This chapter focused on the definition of entropy as uncertainty and disorder to outline the first logic that governs cybersecurity as entropic security, which is the logic of negentropy (negative entropy). On one hand, it harnessed insights from information theory’s understanding of entropy to theorise the intrinsic uncertainties of cybersecurity. On the other hand, physical entropy – defined as disorder in cybernetics and thermodynamics – was used as an analogy to describe the disordered nature of cybersecurity and add a temporal aspect to the analysis. The result is a theorisation of cybersecurity as entropic security that is carved out of an entropic space through anti-entropic processes aiming at negentropy.

Entropy has always been an integral part of information theory and of Shannon’s theory of communication. Defined as uncertainty, the chapter demonstrated how entropy is the default state that communication in essence tries to minimise. Entropy as a security analogy has the capacity to capture the peculiarities of uncertainties and disorders in cybersecurity in multiple ways. Firstly, it shows how such uncertainties are ontological, and therefore cannot be reduced to an empirical challenge of ‘not knowing’. Such uncertainties exist regardless of human’s perception and even with the existence of knowledge about threats. Because of their ontological nature, uncertainties in cybersecurity are also *not necessarily* future-oriented; they span the past, the present, and the future. Secondly, and by extension, entropy is a signification of uncertainties that are essential to the operation of information systems, and hence are partially embraced as a natural product of complexity. Thirdly, the uncertainties and disorders that entropy represents have a particular temporal nature that adds a processual conceptualisation to cybersecurity. Lastly, entropy reflects a theorisation of uncertainty that is connected to complex interdependencies among information systems. As shown in the chapter, such an understanding of uncertainties and disorders is already acknowledged by most cybersecurity actors - even without coining the term ‘entropy’ as such. In this way, entropic security adds an inductive conceptual framework

to study existing understandings of the field that cannot be easily captured by the paradigms of security and risk.

Due to the complexity of information systems, and the big number of coding lines required for the operation of any software, bugs are mostly inevitable. Even when vulnerability analysis is effective, there will always be another unknown bug that could be exploited in a cyber incident. Moreover, applying a patch may result in more security holes or to system malfunction, and it is usually difficult to predict the result. In addition, intrusions may stay invisible to the target for a long time and intrusion detection systems may be overwhelmed with false negatives and false positives. Related to this is the problem of attributing attacks to a certain source and accurately measuring the damage inflicted. The use of botnets, proxies, NAT, onion routing, and dynamic IP addresses are examples of factors that pose technical barriers to attribution. Finally, the technical nature of information systems requires a certain level of awareness or expertise to understand their security issues and fix them properly. This level may not be available to ordinary, non-expert users: the largest pole of targets.

Operating in such an entropic space, cybersecurity becomes a disordered field analogous to entropy in the field of thermodynamics. Just like the natural tendency of matter-energy to decay, cybersecurity has a tendency towards increasing disorder, due to the complexity and dynamism of information systems. For that reason, the proportionality of increasing complexity and increasing insecurity is evident in many cybersecurity discourses. Besides, a similar arrow of time to that of entropy can be found in thinking about cyber dependency and increasing future threats; both are seen as irreversible. Entropic security is thus less about the state of being secure and more about fighting the entropic forces of insecurity. Additionally, entropic security is additive, in which the insecurity of the part contributes to the insecurity of the whole. Yet, paradoxically, the same as physical entropy, collective cyber insecurity may be increasing even if the security of individual systems is improving and if the state of the technology is progressing.

Accordingly, in cybersecurity, defence is reflected in anti-entropic processes that aim at achieving negentropy. Negentropy in cybersecurity is achieved in two ways. The first is decreasing the entropy of particular systems. Since securing everything is not

possible, a risk-based prioritisation of the targets that receive resources and attention should be adopted. The second is shifting the point of absolute cyber insecurity further away, rather than seeking absolute cyber security. This negentropy has an inherent temporary nature, since cybersecurity is a moving target and information systems are essentially dynamic. Nonaction would mean insecurity because entropy is a default state, unless external force is applied. External forces or anti-entropic practices in cybersecurity include: vulnerability reduction, modelling and simulations, deterrence and pre-emption, intrusion detection and prevention, and resilience. They all reflect an understanding that even though prevention is important, what is more feasible is the quick detection of intrusions, mitigation of the resulting damage, and resilience in the form of the survivability of the targeted vital systems.

CHAPTER (5)
THE NON-ANTHROPOCENTRIC INFORMATIONAL AGENT: FROM EMERGENCY TO EMERGENCE

> "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 (America is Under Cyber Attack: Why Urgent Action Is Needed, 2012, p.45)

Introduction

Technologies and socio-technical structures are often instrumentalised, and their agency is reduced to the passive mediation of human subjectivity and the immaterial representation of human desires. They are frequently viewed in utopian terms when they obey human's orders and perform the tasks they are designed for, and in dystopian terms when they do not (Miccoli, 2017; Schandorf & Karatzogianni, 2018). Contrary to such widespread views, this chapter argues that information has generative and agential properties that go beyond mere instrumentalization in the construction of security. It focuses specifically on the syntactic elements of information, i.e., codes/software, that fundamentally distinguish cyber threats from conventional ones. In so doing, the chapter investigates agency as an intrinsic property of the existence and operation of codes/software. It explores how, even if initially given their agency by humans, codes/software can subsequently change such agency in execution and also lend agential roles back to both humans and material objects. With application to cybersecurity, the chapter argues that actancy as an intrinsic property of syntactic information challenges the idea of human control and intentionality imbedded in the logics of enmity and emergency in the securitization literature.

Using the second manifestation of entropy as randomness, this chapter introduces 'emergence' as a non-linear logic that captures the agential capacities of digital information and the uncertainties they engender in co-producing entropic security. As will be explained further, emergence is a key concept in complexity theory and the study of self-organising systems that is closely linked to entropy. Emergence illuminates the inherent unpredictability of complex informational systems and the

elements of novelty associated with their operations. Throughout the chapter, the complexities of codes/software, their self-organising capacities, and autonomous properties will be analysed to produce an understanding of cybersecurity as *emergent security*. As will be shown, the *logic of emergence* and *emergent security* challenge the idea of human control in cybersecurity in two ways: by undermining the centrality of human intentionality as a basis for constructing enmity, and by acknowledging the role of the informational non-human in co-producing the agency of subjects and objects of cybersecurity.

To illustrate this argument, the chapter is divided into three sections. The first section starts with an exploration of the centrality of agency in theorising for information and its ontology. Focusing in particular on syntactic information, this section examines the peculiar conceptualisation of agency in technical literature, such as software studies and computer science, to distinguish it from the agency of ordinary matter. The second section analyses the agential capacities of codes/software, of which malware as the ultimate cyber weapon is a prominent example. Two main aspects of this agency are demonstrated: elements of autonomy and unpredictability in the operation of codes/software; as well as codes/software's ability to grant agency back to both humans and material objects. Based on an understanding of the peculiar agential capacities of codes/software, the third section conceptualises cybersecurity as emergent security, in which digital information influences human actancy and agency. It analyses this logic of emergence in light of the construction of enmity and the co-production of subjects and objects in cybersecurity discourses and practices.

1. An informational account of agency

> "It is from this rich and complex ferment of information that the concept of agency emerges." (Davies, 2019, p. 2)

In popular discourse, information is sometimes seen as an important signifier of reality. For example, strategies to protect personal information or intellectual property rights see it as a valuable object that represents something *about* reality. From this viewpoint, agency is that of the human subject and their ability to protect and control information. In other modes of thinking, information is perceived as having an 'a-signifying modality'. It is a non-representational force that performs operations and make interventions in

order to *shape* reality. It does not merely describe; it engenders representations. Taking this argument further, some scholarly accounts of information regard it as *reality per se*. This 'cosmic fundamentality' is ascribed to information given its ability to establish order and organise matter through processes of formalisation and encoding. This is a perception of agency beyond human subjectivity, which was common in theories of information that emerged after WWII (Behrenshausen, 2016).

In fact, the idea of agency has always been central to the theorisation of information, even if not uttered as such. In one of its commonly used definitions, information is conceptualised as 'the difference that makes a difference' or the 'distinction that makes a difference', in relation to the Latin origin of the word 'informare' meaning to 'shape' or 'form'. This definition indicates that information always has a purpose and seeks to achieve a particular change or transformation (Burgin, 2010, p. 102). Just like energy heats up matter, information can also be added to matter and change it or give it form and structure. For example, to build a house, it is not enough to have physical materials such as lumber, bricks, or pipes. In themselves, such objects lack form. They need information or the 'appropriate relata' to be encoded into them to form a building. Building the house with a specific form signifies information that changes the space-time relationships among the used materials. This means, it is information that brought the house into existence, not just matter or energy (Bynum, 2016, p. 207). Therefore, some theorists argue that what distinguishes our planet is the concentration of information intrinsic to its existence. Even if other parts of the universe have more matter or energy than Earth, none has more information. It is not the singularity of matter or energy that makes Earth special; it is physical order signified in information (Hidalgo, 2015, pp. 8–9). Consequently, information has a strong relationship with causation. Some studies contend that all causal links are inherently *information*. This is because the idea of causation itself is about transferring a quantity of information between two or more states of a particular system (Illari & Russo, 2016).

This capacity of information to *do* things, be it *order*, *change*, or *causation* is the basis of many informational approaches to cosmology and evolution. According to such approaches, evolution is a complex process of information exchange (Gleick, 2011, p. 12), in which information specifies *what* things should do (Lloyd, 2006). If the question

of life is in essence a question of physics, then it is ultimately about information that physical systems possess and the transition in the informational structure of matter (Walker, 2014, p. 425). In the same vein, information is thought to be the force that bridges the gap between biology, as a science concerned with the living, and physics, with its focus on the 'non-life'. The same way physics is sometimes understood as an evolution of information, biology can be also expressed in informational terms. For example, cells gather information, molecules communicate it, and brains can be seen as information-processing systems, or a digital computer per se (Davies, 2019). It is thus information, not matter or energy, that is the primary entity of change and the core of agency in the world, by combining life and non-life (McMullin, 2010).

The argument that information has agency, and one that is peculiar when compared with matter or energy, can be made clearer by looking at how ICTs, digital information, and software engineering literatures define the concept of *agency*. As mentioned in Chapter 3, many of the new materialism literatures derived their main ideas and assumptions about the agency of non-human things from cybernetics. Cybernetics introduced a behaviouristic conceptualisation of agency by focusing on the external, goal-oriented, and purposive behaviour of entities, rather than their internal properties. It considered how such entities interact with their environment and adapt to changes (Behrenshausen, 2016). Alan Turing's famous paper titled 'can a machine think?', published in 1956, posed a question that is still under discussion to this day (Turing, 1956). Whether a computer/software has consciousness, can actually think, or even has emotional intelligence remains an open question that reflects the increasingly blurred lines between human and non-human agency in informational settings (Davies, 2019, p. 186).

If information in general is the difference that makes a difference, software as a particular digital pattern can be seen as an 'organised array of differences' (Suber, 1988). Although not all codes/software can be described as 'intelligent' agents in the same manner as AI, they nevertheless remain purposeful. For that reason, agency has always been a significant concept in the study of information systems. This agency is usually defined either as part of situational theories, in which the informational agent reacts to the environment without reasoning, or deliberative theories, in which agents

possess goals and act deliberately to achieve them (Gregor & Hart, 2005, pp. 165–167). One study compared human and hardware/software agents by arguing that both can act like contracting parties. The same as a human can be hired to perform a certain task to other humans, a hardware/software does tasks on behalf of an individual who cannot do them due to lack of skills, time, or knowledge. A certain level of intelligence is usually required to perform such tasks (Brenner et al., 2012, pp. 19–34).

Technical conceptualisation of agency and agents, particularly in the computer science literature, often goes beyond the ability to simply *do* or *act*, towards human-like characteristics that ordinary matter hardly possess. Among the most important of these attributes is *autonomy.* Traditionally, autonomous agency was considered as one characteristic of living beings, through which they maintain their survival. Yet, the evolution of information systems has shown that autonomy cannot be exclusive to living beings or humans. In some instances, autonomous agency is defined in computer science literature as an 'autocatalytic system' that can detect, measure, and constrain energy. This demands nuanced intelligent choices, or the ability to choose among various courses of behaviour in a way that is sensitive to the surrounding environment. The mere existence of multiple choices though does not signify agency, and this distinguishes information systems from ordinary matter. For example, a vertically-balanced pencil that can fall in any direction and end up falling in one does not have autonomous agency. The position it ultimately took is not a result of free choice to achieve particular interests (Grisogono, 2017, pp. 86–89). Autonomous agency thus requires an element of rationality, or the existence of desires on the part of the agent and an ability to act on best interest. Rational agents according to computational and logical theories are 'practical reasoning systems' capable of making intelligent choices (van der Hoek & Wooldridge, 2003, p. 135).

In addition to intelligent choices, autonomy in this literature comes with two other meanings. The first signifies self-governance or the ability of the system to behave with little to no human intervention or commands. It can control its own behaviour and manage its state without necessarily needing a human operator. Alternatively, autonomy may refer to the system's independence from the process of its production and development. This happens when an information system deviates from the human

intentionality embedded in its design and ends up being used in ways not envisioned by its creators. It is a re-attribution of agency from the designer to the machine itself (Rose & Truex, 2000). This is the argument made in Chapter 2, which explained the unplanned paths that computing and internetworking technologies have taken, away from their initial purposes dictated by humans.

Another agential property that many studies mention is *reactivity*, or the ability of the system to react to its environment, interact with other human and non-human agents, and adapt its behaviour in response. This is also linked to the agent's *proactivity*, and being able to take initiatives, instead of just reacting to changes in the external environment (Wooldridge & Jennings, 1995). Proactive behaviour is primarily goal-oriented and requires a minimum degree of intelligence that allows the informational agent to understand its internal and external environment, and to adapt its behaviour based on such knowledge. It should have an inferential capability through which it uses existing knowledge to work on abstract tasks (Bradshaw, 1997). In addition, it should be mobile and able to navigate in different systems and networks flexibly, while possessing human-like traits, such as reliability and trustworthiness. Nonetheless, these capabilities are not necessarily enjoyed by all information agents. They vary in their level of complexities; the more complex they are, the more of these properties they enjoy and vice versa (Brenner et al., 2012, pp. 19–34).

The criteria against which the agential capacities of informational agents are measured in those disciplines is one important manifestation of how their agency is fundamentally different than the rest of *things*. For many computer science scholars, a powerful conceptualisation of agency is one in which the properties of informational agents are "conceptualised or implemented using concepts that are more usually applied to humans" (Wooldridge & Jennings, 1995, p. 117). For AI, moreover, agents that cannot enjoy human characteristics such as cognitive, or even emotional, functions are fundamentally weak (Bradshaw, 1997, pp. 3–40). As summarised by one study: "Agents are unlike other artefacts of society in that they have some level of intelligence, some form of self-initiated, self-determined goals" (D. A. Norman, 1997, p. 54). This is one reason why this literature uses the concept of *agents* rather than *objects* in talking about information systems. They see objects as entities that do not have choices of

action and cannot make decisions, while *informational* agents *do* and *can* (Agent-Based Software Development, 2004, pp. 2–5).

The massive development of ICTs strengthens those perceptions of an informational autonomous agency that stands against humans and challenges their dominance. Although the process of automation started long before the development of computers, it was computing technologies that presented a real potentiality of resembling human's autonomous agency. This starts with the ordinary user's interaction with a software whose operation they do not fully understand, and one they do not know how to fix when buggy or infected by malware. Nowadays, the more intelligent and powerful a piece of software is, the more likely for it *not* to follow human-written instructions and to produce unintended consequences (Bradshaw, 1997). Besides, in interacting with the internet, the user appears like a posthuman subject that has little control or knowledge of the systems and the structures they are tangled in with every decision they make (Starosielski, 2015, p. 67). For instance, the decentralised nature of packet-switching (explained in Chapter 2), which forms the core of the internet infrastructure, gives self-organising routers the ability to choose the paths that data packets take. It is decided based on the distance between the source and destination, bandwidth, number of hops or intermediate links on the network, and several other factors that as users we are neither aware of or informed about (Misra & Goswami, 2017).

Another way of examining this informational agency is through a focus on codes/software, which constitute a defining element of cybersecurity threats. As David Berry argues – who is one important scholar in the field of software studies – we are now living in a code-mediated world, in which computational ideas and concepts are not just important, but also *ontological*. Such ideas help us understand the world in a same way that evolution once did (M. Berry, 2012). That is why one study has even regarded information technologies as 'technologies of cognition', which enable humans to think about and change reality in different ways through cognitive means (Kallinikos, 2010, pp. 1–11). Codes/software function within computational ecologies and a habitus that combine human and non-human actors. And although their agency is initially prescribed by humans, it is humans who thereafter try to develop an understanding of their actions

(M. Berry, 2012). This is a process of 'softwarisation' that modern societies are undergoing, in which we think about our lives and world in digital terms and establish identities that are influenced by our computational thinking (Berry, 2014, pp. 89–120).

Having software everywhere actually means *information is everywhere*, by granting a wide variety of objects informational capabilities to gather and process information. This creates what one author called 'a regime of ambient informatics' or 'everyware', in which human life is organised around information processing and its possibilities (Greenfield, 2010). In turning our world into a programmable space of rules, databases, and algorithms, codes/software seems as if they are 'alive'. Yet, codes/software do all their complex processes without people noticing, creating a 'technological unconscious'. Notwithstanding these pervasive influences, codes/software's agency is arguably not yet adequately theorised. That is because many studies focus on the technologies enabled by codes/software, rather than on the power of codes/software as such (Kitchin, 2011). This is a gap that the next section addresses.

2. The agential capacities of codes/software

> "…software is somewhat excessive and vexed. It overflows its own context and creates new contexts. In many instances software is so complicated, so distributed and convoluted in architecture that it defeats comparison with any other technical object." (MacKenzie, 2006, p. 17)

In popular discourse, terms like codes, software, and algorithms are sometimes used interchangeably as if they all refer to the same thing. For analytical purposes, however, it is useful to examine how each of these terms is technically defined. Generally, there are two types of codes. The first is 'source code', which is a textual artefact written by programmers using programming languages, that specify a certain set of instructions that digital devices have to follow to perform their designated functions. These codes are then combined in a form that computers can understand, and thus transformed into 'executable code'. Software, on the other side, are commercial applications produced by software engineering that transform static codes into processual programs, and in turn act as mediators between codes and real-world execution (D. Berry, 2011, pp. 1–33).

As normal users of information technology, we do not interact with codes as an internal, static element of computing systems; rather we interact with software and applications as the external, dynamic element. Codes may be embedded in objects, such as DVDs or computer chips, in infrastructure (like mobile or radio networks), and in processes of information transfer (Kitchin & Dodge, 2005). Codes cannot operate without algorithms; all kinds of codes involve a certain kind of 'algorithms and data structures'. Algorithms set clear instructions on how a software can operate in order for certain outputs to be produced. They are primarily the ideas that codes aim to execute. In software, agency is 'contested in and through algorithms'. This is because algorithms influence every step in software operations, which involves several selections of alternative sets of actions and thus produce agency (MacKenzie, 2006).

What is more, codes also embody a high level of complexity. They can be both a solution to a problem when they are produced by software programmers, or the problem itself, when they change themselves in their operation or embody errors that can be exploited in cyber incidents. They are rule-governed but also adapt with the peculiarities of different computing environments. Due to their complexity, codes are sometimes difficult to understand by a single programmer, and in operation, they sometimes seem like they are re-writing themselves. They can also be considered as 'concealed social orders' as MacKenzie argues (MacKenzie, 2003). On one side, they are designed to control the complexity of the world, but in doing so, they shape our understanding of this complexity and instantiate their own complexities (MacKenzie, 2003). As Leach argues in discussing the agency of machines, sometimes technological artefacts work in harmony with humans, but in other cases, they are stubborn, non-cooperative, and do not meet the expectations of the human creators (Leach, 2020, p.12). Likewise, in the following points, the section presents two ways codes and software can be agential: by granting agency to both humans and non-humans, and by operating autonomously outside the span of human control.

2.1. Agency generation and distribution

Studying the actions of codes/software and their operation is ultimately a study of agency. As MacKenzie argues, 'code is agency-saturated' (MacKenzie, 2006, p. 16). Power is integral to the logic of bits in general. The very idea of binary codes is based on

an understanding of something as 'permitted or not permitted' (Thrift & French, 2002). Even if it is primarily a textual entity, code is more than a 'medium of description'. Importantly, it is a 'medium of execution'. This executability and inherent causal power of codes/software is a main property that distinguishes their agency from that of other artefacts (Colburn, 1999). Speaking of agency here means an investigation of what codes/software *do* rather than what their properties are.

Codes/software are structured as a distribution of agency which different entities compete for, including programmers, users, or codes themselves. Although 'art-like objects' usually have a human recipient, it is not necessarily the case for codes/software. Sometimes the recipients of codes/software are other machines or software, which in turn can generate codes (MacKenzie, 2006). In cybersecurity, specifically, a malicious software (malware) is targeted towards particular vulnerabilities (exploitable coding errors) in the adversary's system, not humans. Additionally, though they inhabit micro-spaces, codes/software are agents for the 'automatic production of space', which is essentially informationalised (Thrift & French, 2002). They play an important role in constructing spatiality in the modern world by controlling, producing, and managing many essential elements of life, be they communications, travel, work, etc. (Kitchin & Dodge, 2005). In cybersecurity, as argued by Balzacq and Dunn Cavelty, malware is capable of co-constructing spatiality by circulating within multiple spaces, that cross sovereign boundaries (Balzacq & Dunn Cavelty, 2016). Codes/software in general create computational ecologies in which humans and non-humans exist. Such ecologies engender 'new social ontologies' manifested, for example, in the role social media is currently playing in shaping people's lives. And hence, in many ways, codes/software stand between us and our experience of the world (D. M. Berry, 2012).

On one side, codes/software are transforming material objects, increasing their affordances, and stretching their physical limitations. Equipment we use, appliances, medical devices, etc., are all now given the capacity to perform tasks that were not possible before - all thanks to codes/software. Additionally, codes/software can make objects addressable, through bar codes, magnetic strips, chips, etc. They transform non-digital objects into machine-readable ones, and thus give them an ontological and epistemological unique status by making them traceable across space and time (Kitchin

& Dodge, 2011). They create new experiences of spatiality, particularly when coded objects replace non-digital ones entirely. For instance, a supermarket where coded systems fail, ceases to function as such because products will not be scanned. Similarly, trains that operate through coded infrastructures are no longer a viable mean of transportation if this infrastructure crashes (Kitchin & Dodge, 2005). That is, codes/software alter the capacities of traditional material objects, increase their technicity and affordance, and make them 'addressable, aware, and active' (Kitchin & Dodge, 2011, p. 47).

On the other hand, software and its coded objects, infrastructure, and the processes it enables also influence human agency by shaping, regulating, augmenting, and facilitating their activities. Humans can now process larger amounts of information than ever before, perform complex tasks efficiently, manage systems remotely, engage in new labour practices, etc. (Kitchin & Dodge, 2011). There is always an increasing desire to delegate more to codes/software and to go even further by creating interpersonal relationships between people and their devices. For example, with the development of digital personal assistants, like 'Siri' and 'Cortana', there is an expectation that technology will figure out our needs without us saying anything (Willson, 2018). This demands a study of the co-evolution of humans and digital objects to explore how just as humans are the creators of the digital, the digital is also influencing their knowledge practices and their agency at large (Adams & Thompson, 2016).

Furthermore, instead of instrumentalising codes/software and studying the extent to which they mirror human intentionality, we should consider elements of contingency in their performance (Rammert, 2012, p. 103). Computers can repeatedly refuse to follow users' requests by crashing, not opening a file, failing to save it, etc.; and it is almost always the human who is forced to try to think the same way as a machine to compel it to work in their favour. Humans are capable of adapting to the 'stupidities' of a machine much faster than a machine can, because it takes time for updates to be released and for bugs to be fixed. Through such contingencies, codes/software are forcing humans to adjust their behaviour to the demands of the machine (Goffey, 2017). Accordingly, it can be argued that the agency of codes/software

is never passive. They define the relationships between humans and digital objects and thereby construct regimes and hierarchies of knowledge and power (Kitchin, 2018).

Acknowledging the blurring lines between the 'who' and the 'what' in cybersecurity, as well as the distributed agency among humans and non-humans, raises multiple ethical questions, particularly on the issue of responsibility. If both human practices and the digital are agential, where is the line of responsibility? (Adams & Thompson, 2016). For this reason, several ethical aspects are now arising with the widespread use of AI and the consequences of the autonomous decisions it makes on equality and social justice. There is a growing acknowledgment of the biases that exist in many algorithms, based on race, gender, or social class; ranging from those responsible for evaluating job applicants or granting people loans, to those used in predictive justice and predictive policing. There is also an increasing concern about the use of autonomous weapon systems in warfare, enabled by AI, often called 'killer robots'. This includes the use of drones and anti-missile defence systems that algorithmically analyse sensor data and make decisions with varying degrees of human intervention. Many movements have already emerged to try and ban the evolution of such systems, in order not to give a non-human system an unsupervised power to make autonomous decisions to kill (Dunn Cavelty et al., 2017; Leese, 2019).

This human vs non-human responsibility dilemma intensifies due to the secrecy associated with algorithms, or what is referred to as 'black-box machine learning'. This secrecy allows algorithms to take important decisions in the absence of a thorough understanding from the users' part on how they actually work (Knight, 2017a, 2017b). The resulting questions of responsibility and accountability challenge the liberal-modernist understanding of humans as the sole agency that produces clear causalities based on intentional decision-making (Hoijtink & Leese, 2019, p. 3). It is thus no surprise that we find an increasing number of literatures talking about the role of codes, not just humans, in producing and reinforcing inequalities (Graham, 2005), perpetuating racism (Sandvig et al., 2016), and other forms of discrimination (Noble, 2018).

The use of AI and machine learning is quite prevalent in cybersecurity practices too. It is estimated that the AI market in cybersecurity will increase to $34.8 billion in 2025 from $1 billion in 2016. DARPA has also introduced a research programme in 2019

titled ‘Guaranteeing AI Robustness against Deception’ in order to advance deception-resistant machine learning systems that could defend against AI attacks (Taddeo et al., 2019, p. 557-558). This is not new; as explained by Stevens, using algorithms as a method of intelligence gathering for cybersecurity goes back to the 1990s (Stevens, 2020). Nowadays, malware, vulnerability, and intrusion detection processes are moving towards more automation. The USA has recently established the Joint Artificial Intelligence Centre, as part of the DoD, with cyber defence as a key aim. AI adds an operational advantage to cybersecurity strategies since it is capable of overcoming the limited cognitive abilities of humans to handle huge amounts of data. This creates new epistemic assemblages in cyber defence that combine humans, machines, and algorithms. In these assemblages, threat intelligence becomes a process that is not only performed by humans, but is rather one in which the non-human AI produce information that shapes security decision-making (Stevens, 2020).

However, the complexity, uncertainty, and lack of transparency associated with anomaly-based AI technologies in cybersecurity raise questions about agency and decision-making between the human and the algorithm (Stevens, 2020). Additionally, because AI systems are inherently dynamic, understanding their operation and explaining their outcomes is not an easy task. That is why, when AI systems are attacked, detection becomes difficult, because reverse-engineering their operation to understand their behaviour is quite challenging. This makes it difficult to know whether the outcome of such behaviour is a result of an attack or not (Taddeo et al., 2019, p. 558). Not only is AI growing in use in defence practices, but also in offence. With increasing AI capabilities that do not require a lot of human labour or intelligence gathering, the costs of cyber operations are being lowered. Experts predict that new type of cyber incidents are likely to appear in the future given that AI is capable of transcending what humans may consider impractical, such as labour-intensive spear phishing operation (Brundage et al., 2018).

2.2. Autonomy, uncontrollability, and unpredictability

Codes as textual objects are distinguished from normal language by their ‘executability’. They do not depend on externalities and do not require the same level of mediation as language. Even if written by humans, once embedded in a digital machine, codes start

operating automatically, telling that machine what to do or not to do, sometimes beyond human control. That is, the machine can be considered the 'final arbiter' in operating codes, not the human (Frabetti, 2015, pp. 45–46). In many tasks, starting from simply logging into the internet, codes/software act autonomously and reacts to inputs and outputs automatically, often with no direct human intervention (Kitchin & Dodge, 2011). Machines are now automatically exchanging data, using electronic sensors, updating themselves, producing predictions and warnings, controlling traffic lights, authorising payment cards, opening and closing doors, etc. (D. Berry, 2011). Starting from the year 2008, the number of 'things' on the internet even exceeded that of humans on Earth; a trend that amplified with the advent of the internet of things (Hansen, 2017, p. 37).

Computer-mediated information processing embodies some form of intelligence and is capable of interfering in many human tasks such as memory and cognition. They are also more malleable, flexible, adaptable, and interactive to the outside world than other technologies and 'material artefacts' (Kallinikos, 2010). Now, algorithms and AI are taking decisions on behalf of humans in many fields, with little to no communication on how and why they chose a particular course of action. Humans are sometimes faced with a condition in which they have to either trust the machine and follow its choices, or not use it at all. For example, when cars apply brakes automatically or change the seat position because they decided that an accident will take place, the driver is not consulted on those choices (D. Norman, 2009, pp. 11–42).

Instead of humans being in absolute control of the digital, they are now constantly tracked by machines and sensors, that are collecting data about them, sometimes without their knowledge or permission (D. Norman, 2009, pp. 11–42). The rise of web beacons/bugs is one obvious example in this regard. These are automated agents for data collection, composed of algorithms that are presented in the form of small one-pixel graphical images embedded on websites and browsers – so small that users cannot see. These beacons are capable of constantly collecting data about users, influencing their behaviour, and tampering with their actions online. And although many mechanisms are being developed to allow users to know who is tracking their data,

these web beacons are growing more complex and difficult to understand, even on the part of programmers (D. M. Berry, 2014, pp. 121–148).

This autonomy of codes/software often makes them unpredictable, and ultimately escapes the span of human control. Their inherent unpredictability already starts with the way they are produced. Codes/software are not developed by a single person but are usually engineered within big projects in which many programmers with varying levels of skills and knowledge participate. This process results in a very complex piece of software that no one single programmer can claim they fully understand (Kitchin & Dodge, 2011). The more a software remains 'alive', the larger the number of programmers involved in its development and maintenance, and the more difficult it is for a single programmer to fully understand its complex operation. Further, in most cases, software is engineered through a process of trial and error. They are left to run and have a life of their own, while being tested and improved in the process. That is why, software is mainly *engineered* rather than *designed*, since it does not always follow what programmers dictate. In such case, programmers almost have an 'ignorant expertise' in dealing with codes/software they helped producing (Thrift & French, 2002).

Hence, although source code can be considered a human bid to control the digital, codes maintain sovereignty over execution through self-enforceability. Their operation is never linear; they usually incur self-modification and deviation from the source code in execution. This deviation is also common due to bugs (errors) that are likely to occur regardless of how efficient code-writing is (Chun, 2011). This is what one author described as 'code drift' to explain the many unplanned consequences, fluctuations, and transformations that occur in the operation of codes/software. It can be argued thus that albeit the illusion of control, information systems are evolving as 'code drifters' (Kroker, 2014, pp. 49–59). Added to this, programming is done by standardised, formalised software-enabled languages that facilitate the process of writing code. This involves a lot of abstractions that hide details that may seem unnecessary for the programming process. Although these abstractions make the job of programmers a lot easier and enable people to code even if they do not possess sufficient technical capacities, they also reduce their knowledge of and power over the codes they write. As argued by one study, automatic programming "is both an

acquisition of greater control and freedom, and a fundamental loss of them" (Chun, 2011, pp. 45–46).

This tendency is magnified when it comes to normal users who are neither given the access to such codes, nor do they have the required knowledge to understand them. Ordinary users normally have no comprehension of internal codes and algorithmic processes beyond the graphical interfaces they interact with. Such interfaces give the human user an illusion of control and an imaginary of a 'sovereign executive', when in fact they are perpetuating users' ignorance (Chun, 2011). The ignorance on the part of users is influenced by two main principles in the design of digital objects: encapsulation and exceptional handling. Encapsulation refers to the way through which programmers hide code implementation from users so that they prevent code tampering that may cause errors. Exceptional handling refers to the way machines are programmed to deal with surprises and problems without necessarily consulting the user or informing them of the problem. Although both are meant to facilitate users experience in dealing with digital objects, but they also significantly decrease their knowledge of the system (Goffey, 2017).

It can be argued, therefore, that codes/software are in constant state of emergence. They are designed to interact with their environment, with little to no intervention from humans. For instance, the algorithms of page ranking on Google, or post rating on Facebook, interact with different users differently, based on their own individual interests. They use non-fixed codes designed to evolve by themselves through a process of independent learning while interacting with the user. And in some cases, algorithms are built to be random and unpredictable. One example is the algorithm used in autocomplete in Google search that produces different results when the same letters are typed in different contexts (Kitchin, 2018). As opposed to rule-based algorithms in which humans specify clear instructions to be followed for producing a certain output, machine-learning algorithms give the machine a certain set of data, accompanied by some feedback, and then leave it to operate independently to determine the best way to reach an output. Although machine-learning algorithms have the advantage of solving many problems that humans cannot possibly write instructions for, they also make it

almost impossible even for the most skilled of programmers to understand the steps they took to reach a solution (Fry, 2018, pp. 12–13).

Beyond that, codes/software also operate under different temporalities that are much quicker than that of a human. We usually only notice codes/software exist when they slow down, stop working, or when there is a glitch (error) in the system. This is what Berry described as 'the glitch ontology' (D. M. Berry, 2014, pp. 89–120). In interacting with software, the user cannot possibly know what their actions will result in or if the result is what they intended. Also, information representation is hardly a reflection of users' command; users only see the surface of what a device allows them to see. The computational device is in itself a mediator between objects and their representation. Anything can be changed, altered, and manipulated in many ways by codes/software before being represented to the user. For example, using a microscope to see a microbe, there is first a conversion of the analogue microbe into a digital image saved in the memory of the computer as numbers or bits. In processing this image, the computer's software can manipulate it in different ways, like changing its size, colour combinations, etc. Then the processed representation is introduced to the user after transforming the binary digits to an image that they can see. The user's control over this process of transformation is very limited (D. Berry, 2011).

Finally, the autonomy of codes is revealed when they are used maliciously. Several unintended political and technical consequences that transcend the control of the initiator may result from self-replicating malwares. They can spread to un-targeted systems, they can be discovered due to an error in coding, and they can cause an over-reaction from governments or media that was not initially intended. In ANT terms, malwares can be approached as mediators with 'transformative agency' that is detached from the initiator's intent. Assuming that objects also enact spaces, malware is co-constitutive of the 'space' in cyberspace, meaning that cyber incidents should be analysed within 'the spaces they build themselves' by spreading between devices in completely unplanned ways by their initiators (Balzacq & Dunn Cavelty, 2016). This argument has far reaching implications on security and the assumptions of human control imbedded in its logics, as will be explained next.

3. The logic of emergence and human control in entropic security

As explained in more detail in Chapter 3, the logic of emergency in securitization theory embodies an implicit assumption of human control of security environments. It is humans who construct security threats as existential and they are the ones who implement exceptional, emergency measures in response. As argued by critical security scholars, this logic is intrinsically linked to enmity and direct causal relations to perceived threats. Here, constructing enmity is assumed to be a human choice with the purpose of invoking security. In addition to its implicit statist underpinnings,[31] this assumption by the theory remains problematic because of its anthropocentrism. Assuming that emergency measures are integral to security construction means that their introduction and implementation is always a possibility. It implies that it is up to humans' desires and intentionality to propose and implement such measures, subject to the approval of human audience. This becomes problematic if the above-mentioned agential capacities of codes/software are considered in studying cybersecurity, particularly the agency of malwares.

Malwares - commonly also referred to as 'cyber weapons' - are special kinds of codes/software. Cyber incidents caused by malwares are major challenges to ideas of control upon which cybernetics and computing technologies were based. It is the dystopia of the promises of 'cybernated' economies, cyborgs, and cyberspace as a new frontier parallel to reality. Now, control over machines can be taken from humans, systems can be attacked and controlled distantly, and several damages can result in the form of data loss, abuse, denial of services, or even damages to machines (Rid, 2016). Malwares represent the uncontrollable forces that challenge the idea of user's control over a system as a function of its security. The relative unpredictability of malwares can defy human control, even if operating through rationally pre-defined codes and algorithms (Parikka, 2007).

[31] The theory defined the securitizing 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. 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 securitization theory retains a state-centric perception of security environments.

The most peculiar property of viruses and worms is not their maliciousness, because they are not malicious per se, but rather their ability to copy themselves automatically, described as 'self-reproducing automata' (Parikka, 2017, pp. 173–228). And while viruses require human action to activate them, like clicking a link or opening a file, worms even have the capacity to self-propagate. Malwares are also capable of performing multiple self-preservation techniques that complicate security measures. For example, they can do what is known as stealthing, through which they hide their presence and make it difficult to detect them. This can be done by slowing down their operation or presenting a fake clean image of an infected file to an anti-virus program. Polymorphism is another self-preservation technique, by which malwares change their base code dynamically every time they run, whilst having the same functionality. A step further to polymorphism is metamorphism, which refers to malwares changing their functionality as they propagate across different systems (Skoudis & Zeltser, 2004, pp. 64–68). In short, malwares are inherently active; they are constantly doing something or spreading somewhere, 'almost like living' (Parikka, 2017, pp. 173–228).

The agency of information in general, and of codes/software and malwares in particular, play an important role in changing the logics of security beyond the assumptions of the Copenhagen School. Here, the thesis proposes the *logic of emergence* as an alternative way of theorising cybersecurity, and as the second logic in the trilogy that constitute entropic security. Emergence is a key concept in complexity theory, which is also linked to cybernetics, computer science, and chaos theory. In one definition, complexity theory is conceptualised as 'a science of emergence' (Waldrop, 1993, p. 88). The key assumption behind emergence is that a complex system will necessarily produce new, unexpected properties and will end up behaving in an unpredictable way (Mason, 2009, pp. 32–35). As a result of interactions among its diverse parts, the properties of such systems will change dynamically in a non-linear process, producing *emergent* rather than *resultant* behaviour. Emergence, non-linearity, and non-equilibrium are characteristics of self-organising and complex adaptive systems, in which outputs cannot be simply predicted based on inputs or analysing the individual parts of the system. The interactions that take place autonomously in these systems lead to emergence (Bousquet & Curtis, 2011).

As explained in the previous chapter, entropy as uncertainty is strongly connected to the concept of emergence. In some definitions, entropy and its time irreversibility per se is even described as 'an emergent quality of the system' (Standish, 2001, p. 5). Generally speaking, if entropy increases in the system, this results in increasing randomness and unpredictability, hence increasing *emergence* (J. J. Johnson et al., 2013). This notion of emergence is capable of countering the reductive assumptions of 'ontological individualism' and ideas about humans as the sole agents in the world (Bousquet & Curtis, 2011, p. 52). It is a statement against an in-control human with a full capacity to understand and predict surrounding environments. In that sense, emergence is seen as *ontological*; it is 'real' and does not have to be perceived as such to exist. It is an ontological phenomenon that is fundamental to the operation of self-organising, complex systems (Morçöl, 2013, p. 67). Accordingly, a shift towards nondeterministic self-organisation theories has been taking place in many fields. These theories study the fluctuations in complex systems and the difficulties of predicting their future state. In such case, the system does not undergo a mechanical transformation that connects causes and effects. The system chooses one among various alternative ways of reactions, without relying on specific structural instructions outside it (Hofkirchner, 2011).

Emergence has a number of characteristics that can be employed in theorising cybersecurity as *emergent security*. Firstly, emergence is characterised by *novelty.* New features can appear as a result of dynamic changes, which cannot be simply predicted from existing properties of a system. Again, this is connected to non-linearity and unpredictability (Corning, 2002, pp. 7–18). Secondly, emergence is contextual and relational. Emergent properties in every system are unique to its particular context and to its interactions with multiple agents (Mason, 2009, pp. 32–35). Thirdly, emergence is related to holism: the overall operation of a system is not identical to the behaviour of its self-organising parts. Put differently, the whole cannot be reduced to its parts; i.e., 'the whole is bigger than its parts' (Humphreys, 2016, pp. 26–35). Emergent systems are not centralised, and their parts are not necessarily working towards achieving a particular, unified goal. They rather adapt and interact with the dynamic changes in their

environments, producing emergent results for the entire system (Corning, 2002, pp. 7–18).

Information is entirely connected to the idea of self-organisation as shown earlier. Information systems are inherently 'self-organising agent-based systems' that act as autonomous agents. They are capable of collecting information and act upon it to pursue a certain set of goals, producing a wide range of future possibilities that cannot be easily predicted (J. Johnson, 2006). Therefore, information should be seen as generative of non-formalised 'self-determined processes' in complex systems (Hofkirchner, 2011). For that reason, the operation of information technologies and information-processing systems can be only described probabilistically, since it is impossible to accurately predict their future behaviour (Keyes, 1977).

Complex, dynamic, and decentralised information systems with emergent behaviour produce complex, dynamic, and decentralised *security* with emergent properties. The elements of autonomy and unpredictability in the operation of codes/software as described earlier generate a logic of emergence in cybersecurity. To be clear, this does not entirely invalidate human control in cybersecurity. Rather, it suggests that the construction of security in cybersecurity is not always subject to the sole agency of humans and their intentionality. The elements of novelty, unpredictability, contextuality, and decentralisation associated with emergence can be found in the production of enmity and the subjects and objects of cybersecurity, as will be explained in the next two subsections.

3.1. Enmity and the attribution dilemma

CSS contend that enmity is embedded in securitization theory's logics of emergency and exceptionality (Aradau, 2004; Williams, 2003). The theory implicitly assumes that for security to take place, an enemy has to be established, with a direct causal relation to the perceived harms, and towards which extraordinary measures are directed. This threat-defence logic that lies at the centre of the theory suggests that security can only take place within antagonistic, friend-enemy relations (Trombetta, 2008, p. 139). Nevertheless, such an assumption is not as straightforward when applied to cybersecurity, because the establishment of this direct causation is bound by the agency

of codes/software. This is particularly evident if we look at cybersecurity policies and practices and not just speech acts, and if the scope of the analysis includes non-state actors.

If we examine the development of cybersecurity discourses in the USA in 2003, particularly those of the federal government, we find that attribution was not initially used in constructing the cyber threat. 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 a particular enemy. However, this situation has been changing gradually ever since to one in which attribution sometimes form the core of the cyber threat perception. A strong emphasis on nation-states as a threat source is often made, namely Russia, China, Iran, and North Korea. Arguments by the intelligence agencies that those states have been conducting cyber espionage against the USA and planting malware in the American infrastructure in preparation for a potential future attack are used in support of this threat perception. The construction of futuristic threat scenarios becomes easier when threat attribution with traditional enemies is invoked as a facilitating condition for securitization. Such discourses transfer fears from conventional security fields to cybersecurity, in a way that makes it less questionable talking about future cyber threats and the need for more security.

Despite that, enmity is less evident in approaching the day-to-day cyber threats/incidents that do *not* involve governments and that do *not* necessarily get media attention. If we focus more on *mundane* cybersecurity, we find a conflict of understanding to the role of threat and attack attribution among various actors.[32] Although the publicly published reports on attack attribution by the private sector exceed those of the government (Rid & Buchanan, 2015, p. 28), it is the government and some think tanks that focus more on this *threat* attribution. More specifically, intelligence communities are generally more concerned with attributing cyber threats to a particular enemy than private operators and defenders of information systems, or entities like the DHS that has the main responsibility for protecting the government's

[32] 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 the future threat/hazard and a particular source.

'cyberspace'. For instance, the DHS has repeatedly asserted that its role is not to establish attribution and that this is left to other entities, like the intelligence agencies. As argued by a representative of a network security company: "intelligence and law enforcement entities often prioritize attack attribution, while almost no emphasis is placed on attribution by those defending systems" (Reviewing the Federal Cybersecurity Mission, 2009, p27). The technologies and threat mitigation policies developed for cyber defence are also primarily focused on the tools that adversaries use in hostile cyber operations, rather than determining who this adversary actually is (America is Under Cyber Attack, 2012, p9).

Establishing an enemy in cybersecurity is a complicated process that does not just reflect the agency of humans, but also that of codes/software. Enmity in cybersecurity, just as complexity is described by one of its early writers, "arises out of the combined agencies, but in a form which does not display the agents in action" (Lewes, 1875, p. 368). Elements of novelty, non-linearity, contextuality, and decentralisation are manifested in the construction of enmity in multiple ways. Firstly, the agency of malwares conditions the centrality of human intents in constructing threats. Hostile intents and aggressors' capabilities are not the only deciding factors for the occurrence and success of a cyber incident. There are also other material elements related to digital information that shape the potentiality of incidents, including system vulnerabilities and dependencies (Friis & ReichBorn-Kjennerud, 2016). Vulnerabilities are essentially contextual: they vary across different systems. No attack can take place unless an exploitable vulnerability is identified in the targeted system. Here, the process of defence will primarily focus on fixing those vulnerabilities, regardless of the human enemy. Besides, the implications of cyber incidents are mainly linked to the level of the target's dependency on information systems. The less cyber dependent the target is, the less effective an attack against it would be, making the impact of such an attack relational too. That is why, it is argued that in cybersecurity, "offensive capacity correlates with defensive vulnerability" (Schutte, 2012, p. 8). Hence, human intentionality is not enough.

Secondly, cybersecurity is characterised by a high level of asymmetries between actors and their capabilities that often render any attribution-specific defence

strategy insufficient. This, in turn, puts more emphasis on codes/software than human aggressors. It is coding vulnerabilities and exploits used to target them that lie at the core of defence as anti-entropic policy practice, even when enmity is more discursively prevalent.[33] Also, as explained in the previous chapter, the entropic nature of cybersecurity is in itself a threat, even in the absence of a clearly identified enemy. This can be contrasted with the logic of threats and vulnerabilities in military security as presented by securitization theory. The theory argues that in military security: "The absolute capabilities of potential attackers determine the nature and extent of military threats" (Buzan et al., 1998, p. 58). However, as argued by one study, "Whereas defenders in the physical domain can reasonably assume that pretty criminals do not have nuclear weapons and that foreign military powers will not rob the local McDonald's, this same categorical logic does not hold true in cyberspace" (Rivera & Hare, 2014, p. 104). Attack sophistication is not necessarily an evidence for state-sponsorship. For instance, 'heavyweight code-breaking' does not require states' capabilities; it can be performed by renting bots (compromised computers that are controlled remotely, often without their owners' knowledge) (Libicki, 2009). Added to that, defining cyber capabilities is often more of a matter of speculation than knowledge. Unlike military arms, the non-physicality of cyber offensive tools makes them almost unobservable, unquantifiable, and in most cases, unrecognisable before an attack actually takes place (Schutte, 2012, p. 8).

Thirdly, the agential capacities of codes/software challenge attack attribution even further, making it primarily a process driven by profound uncertainties. For instance, malwares may take control of a user's computer without their knowledge, creating a network of devices that work together to orchestrate an attack in a way that crosses geographical limits. The malware moves between devices across borders, scanning for the targeted vulnerability without consulting the attacker on the devices it affects. This makes it difficult to know if a certain device is acting as a bot or not and to determine who is controlling it, particularly given the irrelevance of geographical proximity as an element of attribution (Singer & Friedman, 2014). This also means that

[33] This argument particularly refers to passive defence, or the one that happens *after* an incident takes place, in contrast to active defence as mentioned in the previous chapter, which takes pre-emptive actions by intruding in the adversaries' systems.

any system can be hijacked by a third party to implant attacks, and thus challenging the accuracy of 'to whose benefit' strategy in attribution. Moreover, packets used in an attack can be changed multiple times before reaching the target, and they can operate through a bot that erases the original address. Even when those packets are traced to a certain country, this does not in itself prove a government's involvement. It could be any politician, separate organisation, or even an individual.

Accordingly, attribution is not necessarily part of an immediate response to counter a cyber attack. Although attribution can be fundamental for cyber deterrence as a defence strategy if it involves retaliatory action, since one needs to know the target they are retaliating against (Iasiello, 2014) - an argument which still can be challenged (Hare, 2012) - yet the same logic does not necessarily apply to other forms of anti-entropic practices in cybersecurity. The immediate enemy in cyber defence is the code, not the human. As argued in a congressional hearing, "Regardless of whether the hacker was a terrorist, a nation-state, a cyber criminal, or hacktivist, the impact of a devastating cyber attack would be the same" (Promoting and Incentivizing Cybersecurity Best Practices, 2015, p2). Defence that is immediate in the face of a certain cyber attack does not always involve or necessitate attribution. It is mainly targeted at the threat itself in the form of the vulnerability and the malware targeting it, not necessarily the human attacker.

However, saying that attribution and enmity are less central in immediate cyber defence strategies, does not mean that they are completely irrelevant. In fact, attribution remains as political a process as it is technical, and plays an important role in operations characterised as 'active cyber defence' that were explained in the previous chapters. In recent years, the line between offensive and defensive cyber operations is being blurred. Even in some academic literature, some categorise cyber operations by differentiating between attacks, exploitation, and defensive operations (Brantly, 2014; Mazanec & Thayer, 2015). Such 'defensive operations' involve the use of malware against the target for intelligence purposes. Thus, by calling them 'defensive', they are becoming increasingly normalised. For example, a former assistant secretary of Homeland Security once acknowledged that many 'friendly' nations maintain an existence on the US network for information collection (Cybersecurity: Developing a

National Strategy, 2009, p30). In addition, a representative in Congress quoted the director of DARPA saying: ‘‘From a technology perspective, defense and offense are indistinguishable’’ (Wassenaar: Cybersecurity and Export Controls, 2016, p87). Drawing the line between the offensive and defensive therefore becomes often a significant political rather than a technical act.

That is, on the practice-level and in immediate policies directed at defending against a hostile cyber operation, the logic of enmity is not as central. The emergent properties of information systems condition enmity, particularly in everyday cybersecurity that does not necessarily get publicised. Yet, the story can be slightly different if one looks solely at the government discourse, especially that of the military and the intelligence. Much of the emphasis on enmity in the cyber threat perception is driven by territorial understandings 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 ‘foreign attacks’ are important examples. But if we broaden the analysis to include private actors and defence measures in practice, the enemy is no longer just a human attacker or a particular actor; the enemy also becomes the vulnerability and the malware: codes/software.

3.2. The subjects and objects of cyber incidents

Another way the agency of information challenges the idea of control embedded in the logic of emergency and gives rise to a logic of emergence can be seen in how malwares co-constitute actancy. Cybersecurity is distinguished by its multi-stakeholder nature. It is co-constituted by every single user of digital technologies, from individual citizens to corporations and governments. However, the identification of the actors of interest in a certain incident and those entitled with taking the necessary measures to counter an ongoing cyber incident or attack is not always pre-defined and can have an emergent nature. Furthermore, choosing security *objects* in a single incident may not also be entirely controlled by the attacker. The subjects and objects of cybersecurity, together with the resulting consequences of a cyber incident, are co-produced by the agency of malwares *in addition to* that of humans. Therefore, they are characterised by their inherent novelty, unpredictability, non-linearity, and contextuality.

Firstly, if all software contains bugs, a malware is distinct given its self-replication property, which intensifies its potential buggy nature. Bugs are even more likely to appear in malwares because they do not go through the same testing processes of normal software. And since they do not operate in controlled environments, it becomes difficult to overrule the bugs they may contain during propagation, and therefore increasing the chances of unintended consequences. For instance, a malware may unintentionally eat up computer resources in the process of replication due to the automatic creation of multiple copies of itself. Furthermore, it is very difficult for the attacker to maintain control over the propagation of the malware once deployed, or to accurately predict its behaviour. It can always affect unintended systems resulting in unintended consequences and various degrees of damage. Not knowing strictly which systems the malware will propagate to beforehand, in most cases, limits the attacker's ability to test its compatibility with such systems (Cobb & Lee, 2014). If the malware is incompatible with the system it is trying to attack, it will behave in a way that is emergent and unplanned by the attacker. There are many examples for such operability problems that existed on a large-scale. The Morris worm in 1988 contained a bug in its code that led to a total paralysis of ARPANET and the infection of 6000 machines. The Slammer worm in 2003 increased network traffic by 25% causing internet blackouts in several countries (Inoperable Computers and System Networks, n.d.).

Secondly, even if the propagation is meant to be limited, in practice, that might not be possible, particularly that attacks can hardly be stopped once started. To reach its target faster, the attack needs to spread widely and to propagate fast among non-target systems. In performing the task of target selection, a specific algorithm is used to either simply choose random IP addresses to infect, or target neighbouring devices on the same local network as the victim. Once on the target's system, those algorithms can also choose other targets from email address books, DNS server, among other ways (Panagiotis, 2006). This relative independence of malwares from their human initiator is one reason why some scholars criticise the use of cyber attacks by states as a purportedly more ethical choice than military attacks. They argue that the unintended and uncontrollable potential implications of cyber attacks on civilian targets make the argument about their ethical use obsolete (Rowe, 2017, pp. 40–41). For the same

reasons, some argue that the collateral damages in cyber attacks are even much higher than military attacks (Hirsch, 2018).

There are numerous examples that demonstrate the inaccuracy of cyber targeting that lead to unintended consequences. The NotPetya ransomware of 2017 is thought to have been targeted at companies in Ukraine. However, the target verification mechanisms of the ransomware did not work properly, and it ended up infecting a large number of targets far away from Ukraine and in several parts of Western Europe. Another example is an attack that exploited a vulnerability in a software called CCleaner. Due to an error in coding, the attack ended up infecting targets in Slovakia instead of its initial target: South Korea (Hirsch, 2018, pp. 281–283).

But perhaps the most notable example in this regard is the Stuxnet worm that, as widely believed now, was designed by the US and the Israeli governments to target the Iranian nuclear centrifuges in 2010. The worm was imbedded on the targeted system initially using a USB stick, before it started propagating. Stuxnet spread to multiple other unintended targets outside Iran, including Germany, China, and even the USA itself. This happened despite the high level of sophistication of this worm, which many believe was designed over many years. It is thought to have included some methods of limitation that the developers used to curb its wide proliferation. But these anti-propagation measures and complex design did not stop it from producing unintended consequences (Keizer, 2010). Though it had a specific target, it transmitted to more than 100,000 computers in various locations in its original propagation (Hirsch, 2018, p. 283). The spokesman of Chevon, an American multinational energy corporation that was hit by Stuxnet, reportedly said upon discovering the malware in the company's systems: "I don't think the U.S. government even realized how far it had spread…I think the downside of what they did is going to be far worse than what they actually accomplished" (King, 2012).

Hence, one could argue that although the humans behind cyber incidents can choose which software/hardware vulnerability to exploit, and in turn which private actor would need to issue patches to stop the attack, a lot is left for the agency of malwares. Even with the existence of targeting mechanisms, the malware per se co-determines which systems gets infected at the end-users side during its propagation. By

propagating across machines, malwares create a network of cybersecurity actors who are then required to take steps to stop the attack, such as updating their systems to apply the necessary patches. By doing so, malwares contribute to emergent, contextual actancy in every single incident.

For instance, in 2017, the WannaCry ransomware exploited a vulnerability in the Microsoft operating system that allowed for remote execution of a code that encrypts files in the infected systems. The choice of the infected targets depended entirely on the agency of the malware during self-propagation, by scanning unpatched systems and deploying itself. It reportedly infected more than 230,000 systems in 150 countries, among which was the National Health Service (NHS) in the UK (Cooper, 2018). By infecting its systems, the malware put the NHS under the spotlight as a major cybersecurity actor. Much of the blame was directed towards the entity for not updating its systems to apply the patch issued by Microsoft before the attack ('NHS Trusts "at Fault" Over Cyber-Attack', 2017). This does not only apply to big entities, but also to individual users who become influential actors when a particular attack takes place and infects their machines. One congressman even considered 'untrained users' as threatening as malicious insiders and outside hackers, because they do not take the necessary measures to secure their systems, and consequently affect the security of everyone (Hacking the Homeland, 2007, p.5).

These agential capacities of syntactic information - in co-constructing enmity and the subject/objects of cybersecurity - thus undermine the idea of an in-control securitizing actor who manages the cybersecurity environment and has the capacity to implement extraordinary measures. It is a demonstration of the power of codes/software in co-producing actancy and agency in cybersecurity, which in turn becomes *emergent security*. Furthermore, the malleability and dynamism of digital information creates a liability and responsibility dilemma in cybersecurity that resembles Beck's argument on the second modernity and its 'highly differentiated division of labour' that results in a 'general complicity' and lack of responsibility. As he said, "Everyone is cause and effect, and thus non-cause" (Beck, 1992, p. 33). But this dilemma in cybersecurity is not specifically just a result of modernity. Rather, as argued in this chapter, it is primarily co-produced by the agency of codes/software.

Conclusion

This chapter discussed the agential capacities of codes/software as one peculiar property of information and analysed the implications of such agency on cybersecurity construction. Instead of instrumentalising information technologies or analysing them as a mere capability that influence power relations among actors in international politics; the chapter focused on the agency of information in and of itself. It interrogated the ontology of codes/software, their intrinsic actancy, and how they influence the agency of other human and non-human agents. This property of digital information has significant ramifications for the logics of enmity and emergency measures as introduced by the Copenhagen School and as widely applied by the cyber securitization literature.

Contrary to underlying assumptions of human control that are embedded in securitization theory's logic of emergency, this chapter proposed *emergence* as an alternative logic of security. Theorising cybersecurity as entropic security that is co-governed by the logic of emergence acknowledges the self-organising, dynamic, and complex nature of digital information systems and their role in co-producing discourses, policies, and logics of cybersecurity. The chapter argued that the non-linearity and unpredictability produced by such properties can challenge conventional ideas about enmity and the construction of subjects and objects of security. This necessarily produces a kind of security that is in itself non-linear and emergent; i.e., *entropic*. Therefore, a shift towards the logic of emergence can deal with the anthropocentric limitation of securitization and present a non-binary framework in which the agency of human and non-human actors can be studied.

In the literature on information theory and the philosophy of information, information is frequently conceptually approached as agential in nature. Information is taken to be the source of order, change, and causation, and therefore seen as even more fundamental to the ontology of our world than matter or energy. Applied to digital information, the technical conceptualisation of agency is always linked to what are traditionally regarded as human capacities. This includes elements of autonomy, goal-oriented behaviour, reactivity, proactivity, adaptability, among others. And although not all informational agents possess all of these capabilities, many of them do with varying

degrees, ranging from normal software to AI. All these properties that were once exclusive to humans can now be acquired by non-anthropocentric informational agents.

Codes/software assume a central position in cybersecurity, given their role as the ultimate cyber 'weapon' in the form of malwares, and as the embodiment of vulnerabilities that these malwares target. Even if initially given their agency by humans, codes/software can change their agency in execution and lend agential roles both to humans and material objects. They create digital habitus that humans find themselves having to comply with in many cases, and grant technicity and affordance to matter in ways that may stretch its physical properties. They construct spatiality in the modern world and create computational ecologies in which other agents exist. They also enjoy an autonomous status in their operation, such as in machine-learning algorithms or self-replicating malwares, that increases the scope of the unpredictable and the uncontrollable for the human actor. Web beacons that collect information without users' knowledge, the *ignorant expertise* of programmers in dealing with complex codes, encapsulation in software designing, and the malleability of codes in operation are all important examples of this autonomy and unpredictability.

This agency of codes/software has the capacity to generate a different logic of enmity than the one suggested by securitization theory and to co-constitute human actancy in cybersecurity. The logics of emergency, exceptionality, and enmity are based on an assumption of human control of security environments and a belief in the significance of intentionality. However, the agency of self-replicating malwares that propagate beyond the aggressor's control, the use of bots in attacks without users' knowledge, the packets that change multiple times before reaching the target, and many other factors make it difficult to establish attribution in cybersecurity. Also, in direct cyber defence in the face of an incident, it is usually the code that is the threat, not the human enemy. This complicates the logic of enmity and undermines its centrality in practices of cybersecurity, even if it is more prevalent on the discursive level, particularly in relation to the military and intelligence communities. Furthermore, even when human aggressors make the initial choice of targets, the agency of malwares can still co-constitute human actancy by determining which other targets are affected by attacks and therefore which actors are important in the line of defence. Accordingly,

the logic of emergence becomes a more accurate description of the way threats, actancy, and many practices unfold in cybersecurity - given its intrinsic relation to the agency of information - than the supposedly humanly constructed logic of exceptionality and emergency.

CHAPTER (6)
THE COMPLEX (NON-)PHYSICALITY OF INFORMATION: THE EXISTENTIAL, THE MUNDANE, AND THE LOGIC OF NOISE

> "In cyberspace national boundaries have little meaning. Information flows continuously and seamlessly across political, ethnic, and religious divides. Even the infrastructure that makes up cyberspace - software and hardware - is global in its design and development. Because of the global nature of cyberspace, the vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them." (The White House, 2003, p. 7)

Introduction

'Cyberspace' is frequently regarded as a 'unique' space given its virtual nature. As a 'virtual' space, cyberspace arguably transcends many of the constraints of the material or physical world. Communications that travel across borders in no time, virtual memories, virtual reality, virtual books, online shopping, and several other forms of virtualisation of life all make the argument of the 'immateriality' seem straightforward and intuitive. In fact, since the massive development of ICTs in the 1990s, many voices started to highlight the transformative influences of information by emphasising its immaterial nature (Mihalache, 2002). For many scholars, cyberspace represented 'the substitution of bits for atoms' and an information society that 'dematerialised nature' and transcended material objects by presenting on-screen equivalents (Dourish, 2017). Further, the so-called 'cyber-weapons', which are primarily codes/software, are also sometimes portrayed as peculiar because of their purportedly non-physical nature. As argued by Dipert, "Cyberattack technology is more like an idea than like a physical thing" (Dipert, 2010, p. 404).

Although this immateriality aspect cannot be denied, there is also much more to information processes and operations than the immaterial and the virtual. That is to say, cybersecurity is different not simply as a virtual or immaterial sector, but because it embodies a complex relationship between this arguable virtuality *and* the physical as an intrinsic characteristic of information. This chapter, therefore, takes the common conceptualisation of cyberspace as a combination of a physical and a virtual layer further, by analysing the co-constitutive influences of both informational layers on the logics of cybersecurity. This is done by focusing specifically on the logic of *existentiality*

and problematising it both in the securitization theory's framework and in its application on cybersecurity.

According to securitization theory, to qualify as security, a threat has to be directed against the *survival* of a referent object. This chapter, by contrast, argues that the peculiar (non-)physicality of information reduces the question of survival to be just *another* discourse in the construction of cyber threats, rather than a defining logic. The (non-)physicality of information, the chapter contends, adds another important logic that contributes to the construction of urgency without existentiality, which the thesis calls 'the logic of noise'. Noise as a security logic is based on information theory's bid to maximise the amount of information by minimising entropy – defined as noise – in the transmission channel or medium. As a problem of communication in information theory, entropy as noise is not dealt with in existential terms. It is rather approached as *mundane* and *routine* disruption that tamper with information, but do not necessarily destroy it. Similarly, the chapter presents the logic of noise as an important security logic in cybersecurity that evokes urgency without existentiality and therefore highlights the significance of the mundane as opposed to the existential. Such a logic is co-constituted by the simultaneous physicality and non-physicality of information, rather than simply mirroring human intentionality.

To corroborate these arguments, the chapter proceeds in three sections. The first section starts with situating the argument on the (non-)physicality of information within the philosophical debate on its (im)materiality. It then moves to an analysis of the physical infrastructure of digital information and how its affordance is determined by the intangible codes/software. Likewise, it discusses the various physical articulations of the intangible elements of information representation and software operation and their constant interaction with digital matter. The second section investigates the co-constitutive influences of the (non-)physicality of information in relation to general geopolitical security considerations. It deals particularly with the geolocation of data centres, data routing, cables construction, and software and hardware manufacturing. The third section moves from general security considerations towards a specific focus on the logic of existentiality as theorised by securitization theory and other security literature. It explains why existentiality in the infosphere is reduced to the physical; how

it is not a pre-condition for perceived urgency; and develops an understanding of cyber threats through the logic of noise.

1. Information, matter, and the (non-)physical

The relationship between information and physicality has been subject to much philosophical debate. Many information theorists approach information materialistically, assuming that information requires a medium to represent it - 'no information without representation' - and that representation is necessarily tied to physical implementation. Written text exists as shapes on a paper or a screen, spoken ones exist as acoustic waveforms, and in a technical context, they are stored as symbols in a computer or transferred through electromagnetic waves. Even ideas in a person's mind occur through neurons in their brains. Thus, the physical medium supports information and its very existence (Battail, 2013, pp. 11–17). Consequently, since information cannot be 'physically disembodied', they argue that it is a physical entity per se (For example: Landauer, 1991, 1999).

The assumptions that 'information is physical' (Landauer, 1991, 1999), and that 'computers are physical systems' (Lloyd, 2000), are strongly connected to the emergence of information physics in the late 20th century. Building on Shannon's theory and the need for minimising the amount of energy used in transmitting information, information physics dealt with information as a 'physical quantity' or as a 'measure of interaction between physical systems' (Fradkov, 2007, p. 6). It is a physical phenomenon because all information processes, such as storing, transmitting, or processing data, involve varying levels of energy consumption and transduction, and are constantly influenced by thermodynamics and the laws of physics. These laws define what is informationally possible for devices used in information processing and set the boundaries of their development. Although modern electronic information systems are designed to consume less energy, all information processes generate heat at every stage of transmission, encoding, and decoding (Karnani et al., 2009). Even the erasure of bits of information generates heat. Thermodynamics also influence the development of modern computers and laptops. The smaller a computer gets, the smaller the size of its microprocessor, the more difficult it is for heat to be released from it (Lutz & Ciliberto, 2015). That is why, it is argued that information theory and thermodynamics

complement each other in their search for the best ways to utilise information within the available resources and energy levels, and that physical materiality is essential to computation theory (Floridi, 2010, pp. 60–72).

Nonetheless, physical representation does not necessarily impose physicality as an ontological property on information. For some theorists, information is an abstract rather than a concrete entity. The fact that it has to be written down, transferred, and processed by physical medium does not mean that the pieces being written, transferred, or processed are physical as such. Although these theorists do not necessarily conceptualise information as non-physical, they distinguish between the ontology of concrete tokens and that of abstract information (Timpson, 2013, pp. 67–71). They argue that although the existence of information requires this physical medium, it does not necessarily depend on it. It is true that information requires a medium to exist, but it can exist on *any* medium. In this view, information is characterised by its invariance to the physical medium that carries or represents it.

In addition, it is argued that being physically inscribed in matter does not mean that information is itself a physical entity, since the properties of the medium cannot be considered properties of information per se. Information has properties that cannot be possessed by matter or physical objects. For example, information is sharable and does not lose any of its parts when copied, unlike matter. It is also characterised by its proliferation capacity: it can exist in multiple mediums simultaneously without increasing in number (Battail, 2013, pp. 11–17). Even the simple idea that information is transportable and can travel at the speed of light - or even faster as argued by quantum mechanics - could be used to argue against its physicality (Burgin, 2010). It is a position that is best summarised in how one study defined information as a 'non-physical emergent of particular physical processes' (Lombardi & López, 2017, p. 53).

Applied to digital information, it is argued that bits have a specific type of materiality that does not resemble that of the figures, letters, or sounds that are encoded in them. This is what one study called 'bare materiality'. Their materiality is not experienced by humans nor represented to them; it is rather directed to digital machines and systems. The semiotic relation between bits and humans occurs only after bits are decoded back to the original figures encoded in them. And although those

encoded figures have a time and space-bound materiality, bits exist in a more abstract domain. They are designed and implemented in a way that allows them to isolate themselves from physical variables, like temperature and vibration, and only focus on the relevant material properties like data storage. By doing this, bits are subordinating matter and material properties to their logic (Evens, 2015, pp. 5–30).

This paradox of the (non-)physicality of information is evident in everyday interaction with ICTs. The digital is made of binary codes embedded in machines and are not visible to human beings. Codes/software hide their complexity in user-friendly interfaces, fuelling the deterministic views that the digital is necessarily immaterial, which one author described as 'digital mysticism' (Boomen, 2009, p. 8). Although people can touch screens and keyboards, they cannot touch codes and data. Additionally, codes are not written to be read or understood by humans, but by other digital machines. To the average user, they seem as placeless entities, detached from the physical world. The electromagnetic medium that carries information appears to users as a 'stampable mass', or a formless entity that can carry any electronic signal regardless of its content. Unlike regular mass that people touch and have bodily experience with, people move in 'cyberspace' without an actual physical experience of space (Eldred, 2013).

In short, it is clear that the answer to the question 'is information physical?' is not an easy one, and actually, it should not be. Picking one side of the debate would be a reductionist view to the complex ontology of information, specifically in its digital form. Instead, this chapter argues that the property that makes information so peculiar is its *simultaneous* physicality and non-physicality. Unlike many of the aforementioned contributions, this chapter therefore does not use the binary division between hardware as physical/material and codes/software as non-physical/immaterial in the analysis. Rather, it analyses how hardware, which is the obvious physical, is given meaning and functions by codes/software; and in the meantime, the way codes/software as the obvious non-physical have their own material representations.

1.1. Digital information infrastructure

The materiality of information infrastructure is a very direct form of materialism. This infrastructure is usually referred to as the physical layer of cyberspace. In the computing

and networking technologies, there are several manifestations of this materiality in different types of hardware, starting from the computer itself and its material parts, such as the central processing unit (CPU), hard disk, screen, keyboard, etc. There are many physical considerations that affect their operation, most importantly degradation. All these objects have a physical lifetime and specific capacities that can degrade over time or become technologically obsolete (Harvey & Weatherburn, 2018). Moreover, for networks to function they also require computer *servers*, which are high-end computers that perform functions for other computers (the clients) on a network. Networks also require internetworking devices such as *hubs* and *switches* that connect multiple client computers and allow them to communicate and share data. Similarly, a *router* (gateway) connects one network to another by routing data packets between them (Hallberg, 2009, pp. 32–36).

Another fundamental material part of the networking infrastructure are *cables*; usually called the backbone of networking. There are different types of cables; the most common of which are copper cables, also known as 'twisted pair'. Those cables contain multiple copper wires twisted together in a plastic insulator. When computers communicate in binary digits of zeros and ones, the wires transmit data as an electric current by changing voltages between two ranges, and thus the receiving system translates those two ranges into zeros and ones. There are various types of cables that differ according to the speed by which they transfer data and how resistant they are to outside interreference. The most expensive and sophisticated type of network cables are fiber-optic cables. Those are made of extremely thin and tiny glass tubes that use pulses of light rather than electric voltages to transmit data. Since they do not require electricity, they are not subject to electrical interference (Evans & Schneider, 2008, pp. 6–11).

When a user searches something on Google, for instance, the signals take a long route on physical devices, including routers, switches, cables stations, and undersea cables until they reach Google's data centre, and take a similar route back to the user. So, despite the wireless experience at the user's end and the illusion of immateriality, it is in the last stages of transmission between their computer and their home router is the signal finally set free from the materialities of the grid (Starosielski,

2015b, pp. 53–54). For that reason, it is sometimes argued that digital communications are no more than “magnetic flux on a disk, electrical currents, photons in optical cable” (Straube, 2017, p. 159). Some even believe that codes are no more than ‘signifiers of voltage differences’, which means that basically, ‘there is no software’ (Kittler, 1995).

Nevertheless, this physical infrastructure is not disembodied from codes/software. For any object to become computational, it has to include computer codes to dictate the functions that it should perform. In digital technology, codes/software are the forces that allow the physical to work by defining what it can possibly do and enable it to overcome its physical limitations. Everything that happens in the physical is a result of encoded bits. That is, the affordance of computational objects, or digital *matter*, is defined by codes and protocols that in themselves are not physical or tangible (D. Berry, 2011, p. 15). These codes do not necessarily exist within the physical digital objects, they can instead interact with it externally. For instance, a DVD or credit card have no embedded codes, but if they do not interact with software to give them meaning, they will remain as mere plastic (Kitchin & Dodge, 2011, pp. 5–6). Berry argues, therefore, that code is a ‘super medium’, or the element of information systems that that provides coherence among its different parts (D. Berry, 2011, p. 10).

To conclude, the components of information systems infrastructure are material, yet *differently material*. They combine both physical materials, such as glass, plastic, silicon, and also intangible bits and electronic voltages (Bratteteig, 2010). The indispensable interaction with the intangible is what makes digital matter peculiar and different from matter in other security sectors. Digital matter is inherently informational, or ‘information all the way down’ (Dembski, 2016, pp. 97–102). However, this materiality of infrastructure does not just exist, it is also co-constitutive. It is obvious how a degrading hardware or broken cables can impact information operations. Most importantly, however, the material has the power to enable and/or constrain the virtual and its non-physical articulations, as will be shown next.

1.2. Information representation and software operation

> “Nonetheless, the materiality of software is without a doubt *differently* material, more *tenuously* material, almost less *materially material*.” (D. M. Berry, 2012, p. 381)

The materiality/physicality of bits as such is a debatable issue in the fields of media studies, software studies, and the philosophy of information. Their intangibility has led many scholars to view them as inherently immaterial, even if they have material *properties*. This arguable immateriality is claimed to be the defining feature of the 'information age' and its metaphysical promises in popular thought about liberating humans from the constraints of matter. In this view, the peculiarity of digital information is linked to its ability to avoid the boundaries of degradation that characterise physical matter. By entering the information age, they argue, the world has transformed 'from atoms to bits'. Through what is called 'the method of abstraction', bits are capable of transmitting across various media, regardless of their physical properties. Put differently, 'bits are bits' notwithstanding the physical medium of storage or transmission (Blanchette, 2011).

Nevertheless, there is more to codes/software than being just an abstract artefact or a 'technology without matter' (Kallinikos, 2012, p. 77). Although codes/software are 'born digital', they are still bound by the physical and have their own physical representations (Dourish, 2017). Codes/software are not simply an abstract 'self-contained language' separated from the material world. Rather, they are constantly and dynamically engaging with the physical in diverse forms of materiality (Zhu & Knoespe, 2007). Bits and codes are both 'logical and material' (Blanchette, 2011, p. 1042); they materialise in devices that operate within their structures, and as such represent an assemblage that combines the 'computational and the human' (D. Berry, 2011, p. 10).

One important example of the influences of digital matter on the non-physical aspects of information is evident in the process of developing software and programming. Although the computing infrastructure was designed to transcend differences in physical computational resources, the historical development of this physical infrastructure has always had an impact on what is technologically possible in developing software. The transformation from wired to wireless communications for instance, or from desktop storage to cloud computing, had massive impact on software development. Computation is not just a method of abstraction to transcend physical material differences, but also a continuous trade-off process to make the best out of the

limited material resources of storage, power, and connectivity. Efficient abstractions require a consideration of the 'politics of resource allocation' (Blanchette, 2011).

Programming is another aspect of software development where the impact of the physical can be detected. To begin with, the process of writing codes passes with various forms of materiality when they are written as text on paper, compiled in hardware, tested by humans, and distributed through physical medium (D. Berry, 2011). Codes also depend on the practitioners' experiences and the 'vernacular meaning' they give to them based on their embodied, real-world experiences. In its simplest form, computer commands like 'print' or 'copy' have a connection with natural vocabularies that are rooted in our experience of the physical world (Zhu & Knoespe, 2007). The interaction of codes with natural language can also be seen in the constraints of syntax in programming, such as punctuation, since the slightest mistakes can cause various errors. Added to this is the limited vocabulary of microprocessors that requires conformity between software and hardware, that is why for example some software are designed only for Mac and cannot be run on Windows and vice versa (D. Berry, 2011).

It is not just programming and software development that is influenced by the physical; such influences can be also traced on the operational level. Bits are not bits regardless of the media that stores and transmits them as Shannon's theory of information proposed. Bits are constantly communicating with the material, not just in the obvious implications of hardware design, but also software, and thus they can be considered as 'material objects' per se (Dourish, 2016). Although computers theoretically can only do what a program tells them to do, there are still other important material aspects in the execution of any task that programs do not specify. They include the network type, the computer's processing speed and memory size, the program's size, and the required memory capacity to execute it. These material characteristics influence the program execution and information representation and can even cause the program to stop working. The gap between the annotation in a program and the actual execution is where the materialities of information can be found, or where the 'lie of virtuality' exists (Dourish, 2017).

Another manifestation of the deep connection between information representation and the material world is the problem of trade-off. For example,

computers are supposedly capable of eliminating noise by using error-correction codes and thus mitigating physical constraints such as the network's bandwidth. However, error-correction codes increase data expansion and processing load, and in turn reduces capacity. Therefore, error-correction becomes a trade-off problem that involves various material constraints. Another example in networking is packet switching. Data travels throughout the network by being divided into packets that compete for limited processing bandwidth and thus impact applications like voice, streaming, and video by causing latency. These are all materially shaped trade-off processes (Blanchette, 2011).

Even in applications like emulation that is seen as 'doubling the virtuality' of the virtual space, various materialisation can be pinpointed. In computing technologies, emulation is the way through which software is used in new devices to simulate older ones. For example, if a certain software used to work on an older version of a device and is no longer supported by the newer versions, emulation can create a simulated platform of the old device so that the software runs on the new hardware. This is similar to other forms of virtualisation, such as virtual books, virtual memory, and virtual reality. Although this may give an image of a completely virtual setting, there are multiple materialities that control it. In fact, rather than virtualising the old device, emulation actually rematerializes it using a host platform to bring it into action, and therefore remains constrained by the material properties of the present host and the absent emulated device. In this case, the differences in processors and capacities can obstruct the functioning of certain instructions in a program, resulting in errors or any form of performance reduction (Dourish, 2017).

Consequently, dealing with software as necessarily immaterial, or portraying digitality and materiality as two opposing categories, becomes obsolete. Such an argument overlooks the various material considerations that affect the 'virtual' representations and operations. Analytically, it thus makes more sense not to use the term 'digital' to refer only to the non-physical or the physical components of cyberspace. Instead, 'digital information' should be used as an overarching term that showcases the complex (non-)physicality of digital artefacts, whether in the form of physical infrastructure, or intangible codes/software. It follows that what makes digital

information *different* is not the immateriality of its intangible elements, but rather the peculiar interactions between its tangible and intangible ones.

2. The geopolitical contexts of information systems: sovereignty, privacy, and security

The co-constitutive influences of the (non-)physicality of information on security can be further observed in studying the geopolitical contexts in which digital information systems operate. Such contexts create peculiar questions about sovereignty, privacy, and security that users are often entangled in, with little choice from their side. As will be shown next, every action that human users take on the internet can have various security implications connected to the geopolitics of information operation, that users are mostly unaware of. This unawareness extends to the location where their data is stored, the routes that their data packets take over the internet, the geolocation of the cables that carry them, and the manufacturing origin of the devices and software they are using.

On one side, digital information transcends the physical limitations of territories and distances. Through ICTs, one can cross borders by sending and receiving information from almost anywhere in the world. Geographical distance and proximity do not affect the speed or quality of the transmitted information. Besides, digital information is peculiar in its ability to exist in multiple places simultaneously. This makes geographical location as a mean of identifying data ownership obsolete. As stated by a data expert and outlined by one study: “Sometimes the answer to the question ‘where’s my email?’ is more quantum than Newtonian” (Blum, 2012, p. 240) – a statement that points out the fact that a single piece of information can exist in multiple places at the same time.

For instance, to speed up the process of retrieving data on the internet, some data may be replicated and stored in what is called ‘edge caches’, which exist in closer locations to the user. This facilitates content retrieval by shortening the distance between the user and the server. The decision on what data is most in-demand and needs to be stored in cache is one that the ‘cache network’ strategically and autonomously takes. In addition, in order not to waste resources and increase efficiency, data may be replicated in multiple servers in different regions. Copying data in several

locations is also done to account for emergencies, like natural disasters, technical failure, or accidental loss that might affect any single data centre (Reisman, 2017). Another well-known practice in data storage as part of the cloud architecture is called 'sharding'. In this process, data stored in the cloud is divided into tiny portions, or shards, each stored in a different location across different regions (J. F. Hill & Noyes, 2019, p. 200).

On the other hand, however, this purportedly 'space-less', 'immaterial', or 'transcendental' experiences of digital information is made possible by a massive physical infrastructure, with the influence of various geopolitical realities. These elements of materiality engender numerous security considerations that users mostly neither choose nor are aware of. In the following points, this argument is unpacked by analysing the geolocation of cloud data centres, data routing, cables construction, and software and hardware manufacturing. This analysis aims to support the two arguments that have been brought forward so far in this chapter: that information is simultaneously physical and non-physical, and that this (non-)physicality is co-constitutive of peculiar security questions.

2.1. Data centres

Data centres are the core of cloud computing. Although cloud computing gives the user an impression that their data is stored in a virtual place, it is massively physical. All the data in the cloud are actually stored in data centres and servers that have physical existence and that require a huge amount of energy to be run and cooled down.[34] A data centre is a facility that stores all the components of a computer system and its storage in a particular entity. They are a collection of cables, computers, routers, pipes, wires, hard drives, etc. These centres are not just material because of their physical representation, but also for the various geopolitical considerations they produce. When a user or entity in a certain country store their data in a cloud, or use it in accessing their emails, the data is not stored in a virtual, parallel space. Rather, it is stored in physical

[34] In some estimates, one data centre can use the same amount of power required for a medium-size town, or even more, making the cloud hold the fifth place in world electricity demand. And because of the energy waste they produce, many companies are now trying to apply less-energy intensive strategies, by relying on hydropower and renewable energy as part of 'greening' cloud infrastructure (Vonderau & Holt, 2015).

data centres that exist within certain territories that cloud providers choose based on IT costs, taxation policies, energy prices, etc. (Albeshri et al., 2014).

The management of data centres engenders various security concerns over data privacy and state sovereignty. Having citizens' data stored outside the borders of the state raises questions about legal jurisdiction over this data and the extraterritoriality of that state's laws and regulations. A famous example here is the legal battle between the USA and Microsoft in 2014, when the government demanded access to the emails of an American citizen that were stored on Microsoft's data centre in Ireland (Daskal, 2018).[35] Had the data centres been in the USA, this legal controversy would not have taken place because the centres would lie under the US jurisdiction. Likewise, if the US government were able to force Microsoft to hand in the data it requested, it would have been a breach of the Irish data privacy. As said by a witness from Microsoft in a congressional hearing, explaining why non-American cloud users could be discouraged from using their services: "So I should use a local provider, right? Because if I use your cloud service, you are a global company; you are headquartered in the United States. You are just going to give all our data to the U.S. Government" (Protecting America from Cyber Attacks, 2015, p24).

For these reasons, many states perform data localisation or data territorialisation practices. This is done in the form of regulations demanding the storage of citizens' data on data centres located within their borders (Baur-Ahrens, 2017). Many forms of data localisation laws are already implemented in several countries with varying degrees, including Canada, Iran, Brazil, Australia, China, Russia, among others (Fraser, 2016). And following the Snowden revelations, several countries in Europe started calling for a 'European cloud infrastructure'. In Germany, for instance, Deutsche Telekom - its biggest telecommunication corporation - called for storing all citizens' emails locally in a campaign titled 'E-mail made in Germany' (Baur-Ahrens, 2017). Yet, data localisation can also have negative implications on citizens' privacy and their personal data security. The local storage of data may be a barrier towards the

[35] This legal battle continued until the CLOUD Act was passed by the Congress and signed in 2018. The act allows the government to compel American technological companies to provide it with data it requests, even if it is stored on foreign soil, subject to data sharing agreements between the USA and foreign governments (Daskal, 2018).

implementation of international security standards for data protection, which global companies have to abide by given the competitive environments they operate in (Fraser, 2016, p. 363).

2.2. Data routing

The internet infrastructure is not fixed and linear as telephone systems; it is composed of a wide range of scattered, non-hierarchal nodes and hubs. Instead of relying on a centralised entity, the functionality of communications on the internet is managed by self-organising end hosts. This flexibility is meant to secure communications against disruptions resulting from targeting a central hub (Baur-Ahrens, 2017, pp. 38–40). When data transfers over a network, it is divided into packets, and each packet takes a certain route, until they are re-assembled at their destination. The path the packets take is not a decision that the user make, nor is the user mostly aware of. Rather, it is decided by the router itself according to the distance between the source and destination, bandwidth, number of hops on the network, and several other factors to ensure the efficiency of delivery (Misra & Goswami, 2017).

Routing is an aspect of the internet architecture that is highly influenced by several geopolitical considerations. The fact that the network traffic inside a country may leave its borders even if the sender and receiver are based locally raises questions of security, sovereignty, and privacy. That is why, some countries have called for having a ‘national internet’ or ‘domestic internet’, by trying to localise data routing that takes place on their territories. China and Russia are among the countries that implement certain aspects of national routing. Additionally, in 2013, Deutsche Telekom also campaigned for a ‘German internet’, alongside the previously mentioned campaign for localising data storage. But since these attempts were not conforming with European laws, the campaign shifted to calling for ‘Schengen routing’ or making sure that communications sent within the Schengen area do not get transferred through foreign territories (Heumann, 2017).

2.3. Undersea fiber-optic cables

Although the current age is marked by increased ‘wirelessnes’ among a wide range of devices, these wireless connections are supported by a huge infrastructure of cable

systems, under soil or under sea. Fiber-optic cables in specific appeared to be more cost-efficient and better in capacity than satellites since the 1990s (Starosielski, 2015a). Right now, most of the internet that travels across the ocean is transmitted via cables, not satellites. The undersea fiber-optic cables are responsible for transporting 99 percent of digital communications across the ocean, that is why they are considered the backbone of the internet (Chesnoy, 2015). And given the decentralisation of data routing, even if the sender and receiver of the data exist within the same state, the data packets might be transferred through cables outside its borders.

The geolocation of cables raises similar security and privacy concerns to routing and data centres, since their location can make the data passing thorough them susceptible to surveillance. The documents released by Edward Snowden revealed that the NSA and the GCHQ (the British intelligence organisation) were wiretapping the data flowing in fiber-optic cables between Google and Yahoo data centres, as part of a project they called 'MUSCULAR' (Gellman & Soltani, 2013; Rushe et al., 2013). As a result, several new cable projects in Europe, Asia, and the Middle East were proposed to route networks away from cables located in the USA (Starosielski, 2015b). However, the challenge remains that the distribution of cable infrastructure is both centralised and limited in terms of available paths. For instance, there are only 45 cables that provide external links from the USA to the outside world. This is considered a big number compared to other countries that have five or less external links. This concentration can be explained by the low financial incentives to diversify location, in addition to security considerations linked to scarcity of safe location for cable extensions (Starosielski, 2015a).

2.4. Hardware and software manufacturing

Hardware and software are not merely technical products detached from their socio-political context; and one key aspect of this context is geopolitical. Where software and hardware are produced, and the nationality of the companies that manufacture them, is an important cybersecurity consideration. As mentioned in the 2011 defence strategy for operating in cyberspace by the DoD, ICTs products are manufactured and assembled in different places, and can be maliciously tampered "at points of design, manufacture, service, distribution, and disposal" (The Department of Defense, 2011, p. 3). This has

been an issue of concern to the US government for a very long time. For example, in 2003, the NSA information assurance director stated that the USA should manufacture the software used in CNIs locally, in order not to risk it being compromised by foreign nations (Cybersecurity – Getting It Right, 2003, p22).

Several cases demonstrate the criticality of this issue. For instance, the leaked Snowden files revealed that the NSA and GCHQ exerted pressure on private companies for surveillance purposes, including Microsoft, Apple, Facebook, Google, among others. This was done through court orders, withholding licenses, or hacking into their systems (Deibert, 2015, p. 11). These measures altered the software or hardware of targets' devices, a process they called 'interdiction' (Biham et al., 2016, p. 777); weakened encryption by utilising supercomputers capable of cracking encryption algorithms; and enforced 'backdoor' access to software (Harding, 2014, p. 259). This is similar to the backlash faced by Huawei and ZTE, forcing them to exit the US market, amidst fears by the US lawmakers that the Chinese government is embedding backdoors in their products (J. Hill, 2014).[36] Most recently, the DHS took the decision to stop using the Russian antivirus software, Kaspersky Lab, and ordered all government agencies to follow suit, claiming that it is linked to the Russian intelligence. In fact, even before this decision, the Russian origin of the company has always created such concerns (Rosenberg & Nixon, 2017).

This analysis shows that the materiality of the geographical context in which information flows matters for security. This is particularly important given the imbalance in the distribution and control over the physical infrastructure mentioned earlier. For example, data shows that around half of a 2.5 billion analysed internet traffic goes through at least one member of the Five Eyes intelligence alliance: the USA, the UK, Australia, Canada, and New Zealand. This means that with the right technology, those countries can spy on a huge number of data. In addition, the majority of technology companies that most people around the world use, like Google, Apple, and Facebook, are all based in the USA, which makes them compliant to the US law (Buchanan, 2020, p. 19). Although information has the capacity to break the boundaries of physical

[36] In the same vein, a news report was published in October 2018 claiming that China inserted a backdoor in servers' chips used by around 30 U.S. companies and government entities, including Amazon and Apple, during the manufacturing process in China (Robertson & Riley, 2018).

matter, therefore, it still remains simultaneously physical. This peculiar (non-) physicality, moreover, is co-constitutive of cybersecurity logic(s). Specifically, this property of information poses challenges to the logic of existentiality as introduced by securitization theory and applied by the cyber securitization literature – this will be further explained in the next section.

3. The (non-)physical between existentiality and noise

> "Noise, beyond the reference to unwanted sound, thus reveals itself to be conceptually polymorphous because it has never been about types, classes or measures of phenomena that qualify noise as a particular type of disturbance, but about the relation between contingency and control." (Malaspina, 2018, p. 203)

Existentiality holds a central position in the securitization theory's conceptualisation of security. It is an indispensable quality of the threats that security aims to survive against. It is also intrinsic to the conceptualisation of the referent objects of security. The theory defines referent objects as "things that are seen to be existentially threatened and that have a legitimate claim to survival" (Buzan et al., 1998, p. 36). What cannot be existentially threatened, or perceived as such, cannot be considered a referent object of security. So, for example, firms in a liberal economy cannot be considered referent objects since they are not expected to last forever and therefore cannot securitize their survival (Buzan et al., 1998, pp. 103–104). There is a general agreement in CSS that security is always about the existential and the exceptional and thus has to be rejected. Even scholars like Floyd, who did not necessarily reject security but argued instead for a 'just securitization theory', accepted existentiality as a given. She asserted that the 'moral rightness of securitization' will be achieved if threats are 'objectively existential', by establishing causal relations with a particular intentional aggressor. And thus, immigration, for example, cannot be constructed as an existential threat because the intentionality of harm is not achieved (Floyd, 2011, 2015).

Whether digital information can be existentially threatened or constructed as such is an important question that the cyber securitization literature did not engage with. Most of these literatures focused on studying cyber threat representations, without examining whether they match any criteria for existentiality and whether

existentiality is in itself an applicable logic to cybersecurity to begin with. The different conclusions they reached about the state of cyber securitization are mainly centred around the application of extraordinary measures. Whereas, most of them implicitly considered it enough for the threat to be presented as *serious* to qualify as *existential*. This can be partially explained by this literature's preoccupation with state and political discourses, in which claims of existentiality are usually made. Most importantly, it can be also explained by their focus on human discourses without considering the role of the non-human referent object in shaping/limiting what is possible in constructing cybersecurity.

Acknowledging the agency of information and the co-constitutive influences of its (non-) physicality shows that existentiality is just *another* discourse in cybersecurity. It is not the only reason for threats to register in the cybersecurity debate, nor is it a precondition for perceived *urgency*. This argument goes contrary to securitization theory and its assumption that existentiality and questions of survival are intrinsic to security and essential legitimisers to urgency and immediacy. Such understanding is either applied by those who accept the theory or contested by those who reject the concept of security entirely and introduce alternative approaches instead, such as emancipation or risk - as explained in Chapter 3. Accordingly, this chapter introduces another important logic that help in understanding the complex construction of the cyber threat by acknowledging the agency of information, which is that of 'noise'.

Noise as disruption or interference in signal transmission lies at the core of Shannon's information theory, as one key definition of entropy. Shannon regarded noise as a key problem in information communication, albeit one that is not existential in nature. To understand this point, we need to first interrogate the meaning of existentiality as such. Wæver states that an existential threat is one that targets the 'essential being' of the referent object, not one that simply results in varying degrees of harm (Wæver, 2009, pp. 22–23) . Constructing a threat as existential is like saying: "If we do not tackle this problem, everything else will be irrelevant (because we will not be here or will not be free to deal with it in our own way)" (Buzan et al., 1998, p. 24). Noise as a challenge in information theory, on the contrary, does not meet this criterion of existentiality.

In information theory, noise is portrayed negatively as the 'parasite' of communication, yet one whose existence does not threaten the *survival* of information. It is a threat for information, though not an *existential* one. Shannon's theory aimed at maximising the amount of information in a transmission channel *despite* the existence of noise, which means that information and noise exist simultaneously. To develop 'noise tolerance', Shannon introduced methods such as redundancy and error-correction (Fresco & Wolf, 2016, pp. 80–82). Coding theories also try to encode information in the transformation process in such a way that allows the retrieval process to take place despite noise (Piccinini & Scarantino, 2016, p. 27).

That is, noise is less than existential. It is not a destructive phenomenon in communication channels (Krapp, 2011, p. xii). Information does exist despite the disruption caused by noise. Moreover, even if viewed negatively as a problem, noise remains integral to the existence of information. As put by Malaspina, "…the creation of information can only occur on the basis of noise" (Malaspina, 2018, p. 75). Noise is sometimes considered as a precondition for complexity and a reflection of the variety of a system. Hence, it is an essential concept in complexity theory and computer science, in which the idea of creating order out of entropy - defined as noise or disorder - is explored. It is therefore normal for information to exist with 'recuperated disorganisations' and fluctuations between stability and 'loss of equilibrium' (Malaspina, 2018, p. 73). Constraining noise and contingency are key goals for every information system, but the existence of both does not in itself threaten the existence of information.

Noise can be used analogically as a logic of security to help understand the complexity of cyber threats, as opposed to the centrality of the existential. The majority of cyber threats in the documents analysed in the thesis are viewed as *disruptive* rather than destructive. This marks a belief that the cyber threats we should be concerned about are not necessarily the ones that disable the target, but rather the ones that manipulate it 'in a very unintended fashion' (Securing Critical Infrastructure in the Age of Stuxnet, 2010, p45). When disruption is portrayed as the consequence of a cyber threat, several referent objects that intersect with other security sectors are drawn into the discourse. Links to the economic sector are established when cyber threats are seen

as harmful to ‘economic competitiveness’, ‘business opportunities’, ‘innovation’, ‘customers’ confidence’, the state’s ‘global competitive advantage or leadership’, etc. Intersection with the military security are found when the cyber threat is viewed as a challenge not to the survivability of armed forces per se, but to their operations and communications, defence and emergency capabilities, and their ability to use cyberspace as a force-multiplier. Added to that, cyber threats are sometimes portrayed as a security challenge for ‘internet openness’ or ‘cyberspace openness’, which in turn affect the privacy and civil liberties of individuals. All such threats are mainly interpreted in disruptive rather than destructive terms.

Just like noise is perceived as an intrinsic part of information systems but one that has to be battled, the disruptive implications of cyber threats are viewed negatively yet not existentially. They are often characterised as ‘catastrophic’, ‘debilitating’, ‘massive’, ‘critical’ to the economy and the society, even if they do not necessarily threaten their survival. Here, urgency and immediacy in constructing the cyber threat is often focused on an assumption 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). Complexity is perceived as both a defining feature of the technology and of its attack tools, including malwares. Increasing complexity and dependency widens the attack surface and renders the implications of a cyber attack more severe. This is seen as one factor that contributes to shifting the offence-defence balance towards the offence advantage. Additionally, urgency is evoked when past cyber attacks are mentioned, with the acknowledgment that they had disruptive rather than destructive ramifications; mainly financial losses and operational dysfunctions.

This does not mean, however, that cybersecurity discourses are not full of futuristic disaster scenarios about potential destruction. Although advocated mainly by the intelligence community, analogies of ‘cyber Pearl Harbour’ and ‘cyber 9/11’ are widely adopted by many other actors who present the cyber threat in destructive terms, even if not part of the official strategy of the state. For example, the NSA director’s statement that a cyber Pearl Harbor ‘is not a question of if but when’ is highly referenced in many statements by MPs, security experts, and private corporations (America is

Under Cyber Attack: Why Urgent Action Is Needed, 2012, p.46). Yet, discourses of cyber destruction are not dominant, and are usually marked by wide uncertainties: the destruction is often perceived as *potential* or *possible* but not *certain*. It is primarily in the defence and intelligence community discourses that more assertions are used. But if the analysis is widened to include private actors, the story becomes totally different.

Here, the analogy of noise becomes relevant in recognising the significance of *mundane cybersecurity*. There is no doubt that some cybersecurity discourses match securitization theory's existentiality assumption. High-profile cyber incidents that are widely publicised, such as Stuxnet, WannaCry, Notpetya, and others, are sometimes used a basis for an argument about survival. However, the cybersecurity challenge cannot be reduced to the threat of one big incident, crises, or disaster that matches securitization theory's existentiality assumption. Unlike the scenarios long imagined by many academics and cyber strategists talking about the potentiality of cyber wars that resemble that of a nuclear catastrophe, none of that has actually taken place. Instead, cyber incidents are becoming the 'new normal of geopolitics'; i.e., as mundane as noise in the operation of information systems. They are happening on daily basis in a persistent, albeit non-destructive manner. They destabilise world politics, without needing to be apocalyptic (Buchanan, 2020, p. 3).

In fact, 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 majority of concerned actors. This does not mean that the cyber threat is not sometimes hyped or exaggerated, since these two qualities are not essentially linked to existentiality and survival. But why so? Explaining why and to what extent existentiality may or may not register in the cyber threat perception should not be reduced to the thoughts, interests, and intentions of the human securitizing actors. There is much more that the properties of information can say about existentiality in cybersecurity, particularly its complex physicality and non-physicality.

3.1. The physical and the logic of existentiality

> "Sort of imagine Bin Laden sitting in his cave plotting the next attack against America, and he is not going to say, ''I know, let's disrupt their chat rooms.'' He is not going to say that. He is going to say, ''Let's kill a

> lot of people, let's cause mayhem, let's cause terror.'' The Internet is important, but it is—it doesn't put bloody bodies on the front page of a paper, which if you are a terrorist is what you want to do." Bruce Schneier (Overview of the Cyber Problem, 2003, p44)

In debating whether information should be theorised as a physical or a non-physical entity, some information theorists resort to existentiality for an answer. They explore the physicality/non-physicality of information by exploring a philosophical question: can information be destroyed? For instance, some contend that the destruction of a physical media carrying information, such as books or CDs, does not mean the destruction of information per se (Ben-Naim, 2008, pp. 122–128). This is used as an argument for the non-physicality of information since it exists in a 'spatiotemporal organisation' of energy and mass that means it cannot be destroyed (Tse, 2013, pp. 122–123). Likewise, the non-physical aspects of digital information arguably condition the perception of existentiality and reduce it to the physical. That is, when the cyber threat is presented in existential terms, it is usually associated with the *physical* elements of information systems and attacks that could result in physical consequences. This goes against securitization theory's assumption that survival is not necessarily tied to the concrete or physical, because in cybersecurity *it mostly is*.

Existential threats in cybersecurity are mostly connected to the fear of potential physical damages resulting from a cyber attack. That is why whenever the cyber danger is discursively aggravated, the physical is brought into the argument: "the cyber world and the physical world is here" (America is Under Cyber Attack, 2012, p38). This emphasis on the destructive physical implications of cyber attacks is the closest to the existentiality assumption, particularly if the target is CNIs.[37] Given their interconnection with medical systems, power plants, and the emergency response capabilities of the state, cyber attacks on CNIs are usually constructed as existential threats because they will necessarily result in *physical damage*. As a result, CNIs security is granted more importance than individual or corporate cybersecurity: "The risks to that infrastructure

[37] In the cybersecurity strategy of 2003, critical national infrastructures were defined as the "public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping" (The White House, 2003).

are greater than the sum of the risks to the individual companies" (Overview of the Cyber Problem, 2003, p13). When attacking CNIs is discussed, it is usually accompanied by several scenarios of physical damage such as planes crashing, lethal clouds emitting from chemical plants, exploding pipelines, total national blackouts, etc. Here, the existential threat is either the direct physical damage to the infrastructure, or the indirect one in the form of potential loss of life.

Furthermore, not only do the physical elements of information systems allow for the existentiality assumption to feature in cybersecurity discourses, they also take away the existential quality from the non-physical. In such discourses - in which the physical damage resulting from a cyber attack is considered possible in the future - identity theft, espionage, and attacks that lead to the disruption of services or loss of data are not seen as existential enough, since they are not physically destructive. This argument can be summarised in the following quote:

> "Many of us recognize the average cyberattack such as a worm or virus is a nuisance, one that irritates us, slows down our computers or prevents us from e-mailing. Yet deliberate cyberattacks have the potential to do physical harm in the form of attacks on cybersystems controlling critical infrastructures" (H.R. 285: Department of Homeland Security Cybersecurity Enhancement Act of 2005, 2005, p2).

Nonetheless, discourses that emphasise this logic of existentiality are still not dominant outside the scope of the military and the NSA, and primarily talk about the *potential* rather than the *certain*. One obvious reason for this is the fact that such attacks have not taken place before, or at least in the same scale mentioned in such existentiality-induced discourses. Most importantly, as argued by Rid, the violence resulting from a cyber attack is inherently both *indirect* and *less physical* than conventional forms of violence. The tools of cyber attack, commonly referred to as 'cyber weapons', are generally not lethal and rely on 'weaponizing the target' and utilising its energy instead of inheriting the violent nature themselves. Put differently, codes are bound by their indirect nature as a medium of presumed violence and do not have an inherent 'explosive charge' (Rid, 2013, pp. 139–140). The indirect nature of the majority of cyber attacks and the non-physicality of their consequences challenge the existentiality logic.

For instance, it is widely believed by many actors in the USA that there are two types of entities in the modern time: those who know they are hacked and their security is compromised and those who do not – with particular reference to the Chinese government as the hacker. This is not usually represented as an existential threat as such. Yet, if the same argument was to be made in the military sector, the claim of existentiality would be more straightforward. Moreover, there is also a belief that most states maintain a presence on other governments' networks for espionage purposes, in which malwares are used to breach the systems. Due to the immateriality of the informational targets and the tools used in those operations, the existentiality claim cannot be easily established. As put by a representative in Congress: "You know, we talk about the analogy, agents of a foreign power caught with paper files walking out with classified or nonclassified information, it will be all over the papers. But yet in the virtual world, that is happening and no one seems to know or really pay attention to it" (America is Under Cyber Attack, 2012, p45).

Hence, even when existentiality is in question in cybersecurity discourses, it is usually connected to high-profile hostile operations that are widely publicised in the media. However, cybersecurity is not just about these attacks. At the heart of cybersecurity lie the less-than high-profile, mundane incidents that take place on daily basis across the world, targeting a wide range of entities and individual users. These threats are closer to the logic of noise than existentiality. In turn, the anti-entropic policies implemented to defend against them – such as patching, intrusion detection, and the rest of practices mentioned in detail in Chapter 4 - resembles what Huysmans called 'little security nothings' (Huysmans, 2011). This is a kind of security that is not centred on the exceptional, but one that extends to the banal, everyday, and routine practices.

3.2. The non-physical and the logic of noise

If the physicality of digital information co-produces existentiality perceptions, the non-physical limit them and open the door for noise instead. This can be explained by three main reasons. The first is the *invisibility of cyber insecurity and the absence of adequate imagery*. Whereas the physical bring the 'cyber' closer to our 'real-world' experiences and imagination of danger, the non-physical makes it hard to visualise the consequences

of cyber threats. In security studies, there is a growing body of research on the role of visuality in constructing security as a part of a field known as visual security studies (Vuori & Saugmann, 2018), together with a growing use of visual methods in CSS in general (Andersen et al., 2014).

Visual security studies illuminate many peculiar characteristics to visuality in securitization that cannot be easily utilised in cybersecurity. For example, Hansen argues that images prompt instant emotive reactions that go far beyond the kind of reactions people have towards texts or words. Images of violence, for instance, can have powerful emotional impact on the observer that is incomparable to speaking about it (Hansen, 2011, pp. 54–58). In addition, images have a 'special affinity to reality' and are capable of creating a sense of authenticity. This is driven from an assumption that what the camera captures is an objective reality. There is also a strong link between images and temporality. Images preserve memories. By simply looking at it, an image has the power to instantly connect the observer to particular historical phases or memories that evoke certain emotions. Some images may even turn into icons that have a specific interpretation in the viewers' minds (Brink, 2000).

However, visuality and imagery in cybersecurity are conditioned by the non-physical aspects of digital information. Cyberspace is "an invisible battle ground" (Securing the Modern Electric Grid from Physical and Cyber Attacks, 2009, p21). We cannot possibly visualise a phishing campaign or have an imagery of the aftermath of data being stolen. As explained by the director of the National Cybersecurity and Communications Integration Centre in the DHS: "…if I told you there was a Category 4 hurricane that hit the Gulf Coast you would go, ''Oh, that is bad.'' Category 1? It is bad, but 4 is worse….What is that in cyber? How do we get that imagery?" (Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure, 2013, p28). It is not just the absence of previous experience of cyber destruction that leads to a situation that "people are much more afraid of bombs and anthrax than they are of viruses and worms" (H.R. 285: Department of Homeland Security Cybersecurity Enhancement Act of 2005, 2005, p12). Rather, it is also the inherent invisibility of cyber insecurity. The fact that when a cyber attack takes place "There are no burning buildings or collapsing structures" (Overview of the Cyber

Problem, 2003, p6) makes existentiality hardly imaginable. This is also arguably one reason why people care less about their digital privacy than they would in a non-digital context. Digital surveillance is intangible, cannot be seen, and therefore hardly felt, which gives an illusion of privacy (Mitnick, 2019).

Secondly, information is innately replicable and therefore possibly retrievable. Unlike atoms, bits are persistent by default (Boyd, 2010, pp. 45–48). The non-physical aspects of bits makes it easy for digital data to be duplicated and copied and impossible to distinguish a copy from an original (Masur, 2018, p. 16). In addition, as stated earlier, there is always a possibility that data exists in multiple places, so an attack on one does not mean necessarily its complete loss. And if spied on and breached by cyber attacks, like espionage, data can still remain intact and unharmed. Stealing military, commercial, or personal information do not necessarily affect the survival of the state, the private sector, any individual, or the stolen data itself. Similarly, denying customers/citizens access to certain services through DDoS attacks, for instance, does not in the majority of cases threaten the essential being of anyone. For instance, speaking of the danger of a data breach, a representative in Congress said that breaching valuable information can be 'inconvenient' for people and 'expensive' for banks and cause 'worry' and 'confusion' for all; arguments that do not speak existentiality or survival (Data Breach on the Rise, 2014, p176). This does not mean, however, that data is never lost; because it can be and is. But this replicability and retrievability property makes its complete annihilation in case of an attack *possible* rather than *inevitable*. That is why, it is often argued that the majority of data loss due to failure of software or hardware, human errors, or malware are recoverable (Reuvid, 2006, p. 156).

Thirdly, the universality of computing devices makes them inter-changeable and can weaken the logic of existentiality. As stated earlier, one property of codes/software is that they are not tied to a particular material substrate/entity/configuration. If a computer gets hacked, in most of the times the user can re-install a new operating system and still use it. And if it happens to stop working due to this attack, they can re-install their backed-up data on a different device and still have the same experience. The same applies to software; their existentiality is hardly ever a question in the case of a cyber attack. When a software is attacked, it remains

operable after patching and does not cease to exist. It can be re-designed, re-written, re-tested, or debugged, but is not destroyed due to an attack. Though software is not eternal, it may cease to exist due to the development of new technologies that make it obsolete, its incompatibility with new devices, or several other reasons, but not as a direct result of a cyber attack. Here, the cyber attack is the noise that threatens the system but does not necessarily challenge its existence.

Conclusion

This chapter focused on the third property of information that the thesis argues is co-constitutive of cyber (in)security, which is its simultaneous physicality and non-physicality. Against the seemingly intuitive arguments that 'cyberspace' and digital information are essentially peculiar because of their 'immateriality', the chapter showed that their peculiarity actually stems from a complex interaction between their *simultaneously* physical and non-physical nature. This (non-)physicality co-produces several security conditions that human actors may involuntarily be tangled in. It also co-constructs a different conceptualisation of existentiality and urgency in cybersecurity and opens the way towards an analogical interpretation of cyber threats through the logic of noise.

On one hand, the infrastructure of digital information is a clear signification for materiality. Information cannot exist without representation, and this representation is always through a physical medium. Computers and their components, hubs and switches, cables, and the rest of internetworking infrastructure is key for digital information processes. Yet, digital matter is not just *another* type of matter, because it is inherently informational. The physicality of digital matter is not disembodied from the intangible or the 'virtual'. Its affordance, functions, and capacities are dictated by codes/software. On the other hand, codes/software have their material articulations and are constantly interacting with the physical world. These interactions are manifested in the process of software development, programming, code-writing, and in software operation. Bits are not bits regardless of the medium as some argue, and both their operation and the way they are experienced by the end-user are affected by the physical properties of the infrastructure.

The entanglement of the physical and non-physical is evident in the geopolitical context of digital information operation. Digital information is characterised by its divisibility and mobility and is peculiar in its ability to exist in multiple places at the same time. This does not mean, however, that 'cyberspace' is placeless or borderless. The geolocation of data centres and undersea fiber-optic cables, the paths that data routing take, as well as the geographical origin of hardware and software manufacturing are all demonstrations of the argued (non-)physicality of digital information. This, in turn, creates various security considerations and privacy concerns that users mostly neither choose nor are aware of, with every simple action they make online.

In addition to the general security considerations regarding privacy and sovereignty, this (non-)physicality of digital information reduces existentiality to being just *another* discourse in the construction of cyber threats, that is limited to the physical. If not existential, the cyber threat is constructed as urgent and imminent through what the thesis calls the logic of noise. Viewed as disruption to communication channels in information theory, noise can be used analogically to understand the complexity of cyber threats in a space between contingency and control. The same as noise is seen as a 'normal' characteristic of information operation, but one that needs to be minimised and challenged, cyber threats are often viewed as a disruptive yet integral aspect of the everyday functioning of systems. Reasons include the absence of an imagery for the non-physical, the innate replicability of digital data, the universality of computing devices, the invisibility of attacks and uncertainties about the scope of damages, and the indirect nature of cyber violence. It is the physical that can bring existentiality to the analysis, particularly in regard to the security of CNIs.

CHAPTER (7)
CONCLUSION

Cybersecurity has been transforming the security agenda of nations and non-state actors around the world since the 1990s, though it has not had the same transformative impact on theories and conceptual frameworks of security in International Relations. The policy-oriented nature of cybersecurity as a field of research posed a theoretical challenge to Security Studies, albeit one that has been approached mostly as a challenge of inclusion rather than as one of deeper transformation. A prominent example in this regard are the cyber securitization literatures and their bid to include cybersecurity as a sixth sector in the framework of the Copenhagen School's securitization theory. Such attempts have certainly produced important insights on the discursive particularities of cybersecurity; but they have also stopped short of investigating the materiality of this cybersecurity field and how it can transform the meanings and logic(s) of security beyond those of securitization.

Against that background, this thesis has advanced an alternative theorisation of cybersecurity that acknowledges its peculiarity and inherent multi-disciplinarity, in a way that does not simply bind it to the existing logics of other security fields. The thesis is thus a study of the ontology and materiality of cybersecurity as such, not just of how human actors perceive it or discursively construct it. It does not assume that the ambiguity of cybersecurity can be overcome only through empirical analysis. Instead, it problematises the very being of the 'cyber' as an essential constructing force of its security. This is cybersecurity as an infosphere rather than a discursively-constructed security sector as theorised by the cyber securitization literature. The peculiarity of cybersecurity as an infosphere is not reduced to its novelty as just one additional sector that we can test the assumptions of existing theories on. It is different because it challenges such assumptions and produces different security logics that should be theorised for differently. This is what the thesis does by exploring the informational ontology of cybersecurity and the implications it has on our theoretical understanding of security.

Combining theoretical approaches from the philosophy of information, information theory, cybernetics, software studies, new materialism, and risk studies, the

thesis conceptualised cybersecurity as *entropic security* that is governed by the logics of *negentropy*, *emergence*, and *noise*. This conceptualisation is based on three core assumptions that were fleshed out across different chapters: the field of cybersecurity has an informational ontology; information is a peculiar non-human entity; and thus, it follows that the field of cybersecurity is equally peculiar in relation to other existing security sectors and should be studied through a different theoretical framework.

By way of extension, the theoretical exploration of cybersecurity developed here is based on three main pillars. Firstly, it is one that adopts a non-anthropocentric conceptualisation of agency. This means it approaches information as a vital, active force in the co-production of the security of the 'cyber', and also of the development of its technologies. It transcends the question of whether actancy in cybersecurity is a function of state or non-state actors, towards a study of the materiality of the non-human informational agent. Secondly, securitizing the infosphere entails a deeper theoretical analysis of the referent object of cybersecurity that is not exclusively tied to humans and their interests. Beyond listing a group of referent objects of relevance to human life, the thesis investigated information as the ultimate referent object of cybersecurity and explored the different forms of materialities it possesses. Thirdly, security in the infosphere does not follow the fixed security logics assumed by the Copenhagen School (and its critiques). It challenges existing understandings of existentiality, exceptionality, and emergency measures and transcends the traditional binary divisions between security and risk.

1. The matter and materialities of cybersecurity

Investigating the informational ontology of cybersecurity in this thesis is ultimately a study of materiality. Three forms of materiality were analysed in the thesis. Firstly, the thesis approached *materiality as intrinsic properties* of information, both as an overarching assumption for the whole thesis and also as a central idea in Chapter 4. By this the thesis means the peculiar properties that are inherent to the existence of information, and not necessarily ascribed to it by humans and their discursive utterances. In Chapter 4, the thesis examined the intrinsic uncertainties and tendency towards disorder that characterise information systems and how they co-shape the essence of 'security' in cybersecurity, through the logic of negentropy. The second form

of materiality in the thesis is *materiality as agency*. Again, this is an organising idea for the whole thesis in shifting the focus from human actors to information and analysing its role in co-constructing cybersecurity. Chapter 5 in particular focused on the peculiar agential capacities of syntactic information (codes/software) and their influence in co-producing the logic of emergence. Finally, the thesis approached *materiality as physicality* in discussing the ontological status of information as compared to matter. Particular focus on this question of physicality was given in Chapter 6, by examining the complex (non-)physicality of information and its generative influence on the logic of noise and mundane cybersecurity. Though the analysis of these three forms of materiality may intersect with other informational fields, like information security, it remains cybersecurity-specific. Accordingly, those three chapters (4-6) started with a general theoretical exploration of theories of information, followed by an application on digital informational systems, and ultimately establishing a connection between these theoretical arguments and the empirical analysis of cybersecurity in practice.

First, the thesis examined information as a complex entity that is ontologically linked to uncertainty. In part, the complexity of information is a product of its multiplicity and transformational capacity. In operation, information is capable of transforming itself, its environment, and other agents' perceptions of it. This transformational capacity produces complexity and also variety, hence the definition of information as 'reflected variety'. Most importantly, the complexity of information is a result of the indeterminacies associated with its operation. As shown in Chapter 4, entropy – defined as uncertainty or disorder – has been integral to the conceptualisation of information, as part of the development of information theory. Mostly, information has been defined through entropy: either as its inverse or its synonym. In communication contexts, the mathematical theory of information assumed that indeterminacy is the default state that information transmission seeks to minimise. And because information and communication systems interact with thermodynamic subsystems, the probability of noise is always high. As a result, the outcomes that an information system produces are best described as *emergent* rather than *resultant*.

This creates many uncertainties in the security management of digital information systems. It is impossible to know all the vulnerabilities that exist in a system

beforehand. Many bugs appear in a later stage of software operation or are discovered only once they are exploited in a hostile cyber operation. Even patching those vulnerabilities is an unpredictable process, as it is difficult to know how the patch would react with the system before its actual application. Intrusion detection is also made difficult by the innate multiplicity of information and the difficulty of keeping a static image of a system with a large number of attack targets. Attribution and damage analysis are other processes marked by vast uncertainties, due to the use of botnets, proxies, onion routing, etc. Also, in the case when information about vulnerabilities is available, uncertainties persists due to the lack of technical knowledge about those systems and their complexity on the part of end users. Likewise, software manufacturers may be reluctant to issue a certain patch before adequately testing it, fearing that they may lead to more vulnerabilities and bugs once applied.

Second, the thesis presented agency as intrinsic to the ontology of information, given information's capacity to organise life beyond human subjectivity. Information is sometimes defined as *the difference that makes a difference*, to signify its power to achieve *order*, *change*, and *causation*. Some approaches even assume a cosmic fundamentality that is linked to information, by either explaining evolution in informational terms or regarding information as reality per se. As the thesis explained, information and cybernetics were important catalysts to post-humanism and new materialism, by viewing humans as information processing entities that can be comparable to intelligent machines. As a result, much of the technical literature on information systems does not approach agency as simply doing and acting, but rather as possessing human-like properties, like autonomy, reactivity, proactivity, intelligence, etc.

Generally, information systems are purposeful; they have to retain some level of intelligence to operate. They may exercise autonomy by choosing among various options and taking decisions with little to no intervention from the human operator. They have varying degrees of proactivity and reactivity to their surrounding environments. The more complex the informational agent is, the more of these properties it possesses. Likewise, the more powerful a software is, the less strictly it follows human instructions or even needs it. Despite being a human creation,

codes/software have the capacity to infringe human control and subjectivity. Although they are given their agency by their human creators, codes/software are capable of distributing this agency back among humans and other objects. They mediate our experience of the world and create digital habitus that shape human behaviour. It is humans that are constantly trying to adapt to the machine, not the other way around. Once put into action, codes/software operate independently of humans, and through advanced algorithms they can take many decisions on behalf of the user without consulting them in the process. This does not just apply to normal users, but even to programmers. Many codes/software are becoming very complex entities, produced by a large number of programmers, making it difficult for a single expert to claim complete understanding of how they operate.

Hence, codes/software are engineered rather than designed, since many of their functionality and potential errors only appear once they start operating. Malwares are one important type of codes/software whose agency is maximised by their ability to self-replicate and self-perpetuate. Their operation reflects the non-linearity of codes/software and their constant state of emergence. Even when carefully designed and executed, malwares may propagate beyond the aggressor's control, spread to un-targeted systems, or produce unintended consequences. They can perform multiple self-preservation techniques that complicate security, such as stealthing, polymorphism, or metamorphism. That is why, cyber incidents caused by malware can be considered a major challenge to ideas of control upon which cybernetics and computing technologies were based. Security is no longer a matter of user's control over the system as it once was in the advent of ICTs.

Thirdly, information is approached in the thesis as a simultaneously physical and non-physical entity. It can only exist through physical representation, but also does not strictly follow the laws of physics. It is fundamentally different from matter and energy, even though it utilises both in its operation. Physicality is evident in the infrastructure that allows digital informational systems to function, including the different forms of hardware, devices, cables, routers, hubs, etc. Yet, digital matter is still not ordinary matter, because it is enabled by bits, codes, and protocols. Its functionality depends on those intangible elements of syntactic information that specify what can

and cannot be done. On the other side, codes/software are not totally abstract, non-physical entities either. Their interaction with the physical can be seen, for instance, in the constant trade-off processes in their operation and evolution to account for the physical limitations of storage, power, and connectivity. Even the textual languages used in programming are dependent on vernaculars linked to physical experiences.

Although digital information is divisible, mobile, and can exist in multiple places simultaneously, its transcendentality is still influenced by a wide range of geopolitical considerations due to its equally important physical existence. Every device or software we use is manufactured somewhere by a private company that is subject to the legal systems of a certain country. Every time someone sends a message online, the data packets of this message take different routes, that may cross borders regardless of the receiver's geographical proximity to us. As explained in Chapter 4, packet-switching is a decentralised process that is often decided by routers, not humans. Additionally, when we use a search engine to search for information, we are establishing a communication with a data centre that has a physical location we know nothing about. We may own our data, but we have no control on where it is at any given time. This all create various security and privacy issues that human users are involuntarily entangled in. The security implications resulting from these geopolitical considerations have proven more salient than futuristic scenarios of apocalyptic cyber conflicts.

In short, thinking about cybersecurity informationally allows us to employ a rich and multi-disciplinary body of literature that introduces important insights to the study of the matter and materialities of this field. Cybersecurity as an infosphere is distinguished by information as its subject matter, referent object, and agency. 'Information is information', as argued by Wiener (Wiener, 1948, p.132). It does not resemble ordinary matter and is fundamentally different from other non-human entities. And if all security fields have informational elements, cybersecurity is informational all the way down. The intrinsic indeterminacies of information systems, the agential capacities of codes/software, and the (non-)physicality of information are all co-constitutive forms of materialities and are generative of cyber (in)security. They co-produce peculiar logics of security that are not reduced to humans' perceptions and discursive constructions; ones that the notion of entropy directly captures.

2. Entropic security: security beyond the Copenhagen School

Security is 'an essentially contested concept' (Buzan, 1991). Traditionally, four main elements in conceptualising security constituted the foundation of this contestation in security studies: the referent objects of security, threat sources, the security agenda, and the link between security, threats, and dangers. These four elements formed a dividing line in the debate between the so-called 'traditionalists' and their military/statist conceptualisation of security on one side, and the 'wideners-deepeners' on the other side. The widening attempts, which the securitization theory is an example of, broadened the security agenda to include social, environmental, economic, and other security topics, and deepened the analysis of the referent objects of security beyond the state. Nevertheless, this is a debate that runs within an anthropocentric framework. It is humans that are the primary subjects of security; it is their discursive utterances and speech acts that construct it; and it is qualities associated with their lives that are the main referent objects of security.

In departing from this anthropocentric understanding of security, the thesis did not engage in a quest for alternatives for mere theoretical purposes. Rather, the theoretical exploration presented in the thesis is one that is imperative to grasp the peculiar materialities of cybersecurity and the specificity of its informational ontology. Acknowledging the materiality of information is a must in a field where even experts admit varying degrees of uncontrollability and unpredictability in managing the security of the systems in question. In so doing, the thesis conceptualised information as both a securitizing actor and referent object in cybersecurity. One direct implication of such assumptions is revisiting the fixed logics of security that the securitization theory introduced, and the CCS criticised. Security that is approached as existential and exceptional should be approached differently once the peculiar materialities of information are considered. Emergency measures and enmity as human choices based on human interests and desires should be challenged. Additionally, the meaning of existentiality should be unpacked instead of taken for granted, and its relationship with urgency and physicality should be problematised. The result challenges the whole essence of security in cybersecurity and its intricate relationship with risk.

The thesis therefore introduced entropic security as an information-theoretic, *non-binary* concept that is capable of illuminating important ontological aspects of cybersecurity, that may not be fully grasped through the separate analytical frameworks of security and risk. The thesis used three definitions of entropy in constructing a trilogy of security logics to capture the complexity of cybersecurity: entropy as uncertainties and disorders (the logic of negentropy), entropy as randomness (the logic of emergence), and entropy as disruption in communication channels (the logic of noise). Each of these three logics was linked to one characteristic of information. That is, the logic of negentropy is co-produced by the indeterminacies of information systems; the logic of emergence is co-produced by the agential capacities of codes/software; and the logic of noise is co-produced by the simultaneous physicality and non-physicality of information.

Entropic security, and its three concurrent logics, thus constitute a *non-anthropocentric* intervention to reformulate the concept of security to account for the materialities of information. The three logics of negentropy, emergence, and noise are essentially linked in their resistance of the idea of *human control* of security and the centrality of *human intentionality*. Entropic security allows us to theorise for the generative capacities of information in co-producing a peculiar meaning for 'security' in cybersecurity, that is not reduced to human subjectivity. Accordingly, entropic security represents an ontological argument about cybersecurity that goes beyond security and risk as modes of governance. As such, entropic security is an overarching conceptualisation that is not reduced to moments of exception or the existence of particular threats/risks. Further, entropic security is a *semantic deviation* from the essentially positive connotations of the term 'security' that does not adequately represent the complexities of cybersecurity.

In a practical sense, through its definition as uncertainty and disorder, entropy as a security analogy enables us to understand the intrinsic link between the (in)security of all users of information systems across geographical boundaries. The multi-stakeholder nature of cybersecurity, the non-geographical interdependencies that characterise cyber threats, and the fact that the security of all actors is as strong as their weakest link are all factors that resembles entropy's additive nature. In addition,

through the analogy of entropy, we can theoretically analyse the paradox of the direct correlation between increasing cyber insecurity on one hand and the growing investments in technological development in general and cybersecurity in particular on the other. Further, defined as randomness and non-linearity, the analogy of entropy can capture the problems of targeting in cyber operations; the challenge of attribution; the contextual/relational aspects of the subjects and objects of cybersecurity; and the dilemma of responsibility/liability. Through the analogy of entropy, cybersecurity can be thus freed from the confines of the friend-enemy logic that characterise other fields like the military security. Though enmity is still part of the cyber threat perception, it does not always have to be anthropocentric; the enemy can be the vulnerability and the malware: code/software. Importantly, cyber defence does not always need a pre-defined enemy or an attack; it can be exercised against the entropic force of increasing disorder and insecurity. Finally, the analogy of entropy as noise is capable of highlighting the importance of mundane cybersecurity and why the urgency of cyber threats should not be bound to understandings of military attacks, existentiality, or high-profile incidents.

As discussed in Chapter 4, the uncertainties and disorders in information systems co-produce an understanding of cybersecurity as a moving target. Here, cybersecurity is entropic because of its tendency towards more insecurity, which is analogous to physical entropy's arrow of time. As a result of this entropic nature, cybersecurity is measured by the relative improvement in the insecurities of the future compared to those of the present. Security thus becomes a process rather than an end goal; it is the quality of the measures implemented rather than the state of being free from threats. This is because absolute security is unattainable and contradictory to the very nature of information systems. Vulnerabilities can be considered the by-product of complexity, and thus can only be managed and reduced, not eliminated. Prevention in the infosphere is not about stopping one big, major attack or threat, because the cyber threat has a continuous nature. Thus, defence in cybersecurity is better conceptualised in terms of negentropy (negative entropy) that represents anti-entropic practises aiming at countering the entropic force of disorder and uncertainties. Negentropy as the essence of cybersecurity is based on risk prioritisation and risk acceptance: accepting

that some attacks will happen anyway, and thus directing most security measures and capabilities to the higher risks. Instead of targeting the eliminations of threats, anti-entropic cyber defence aims at shifting the point of absolute cyber insecurity further away and defying its inherent inevitability – just like physical negentropy aims at shifting the point of heat death away.

Cybersecurity is also entropic given its emergent and non-linear nature. The thesis introduced the logic of emergence in Chapter 5 to counter the assumptions of an in-control human that is implicit in the logics of emergency in securitization theory. Given the complex, dynamic, and decentralised nature of self-organising information systems, their emergent behaviour often leads to complex, dynamic, and emergent security. This emergent security can be seen first in the construction of enmity in cybersecurity. Hostile intents and capabilities alone are not as a strong legitimiser in the infosphere as they maybe in other sectors, particularly military security. In the infosphere, capabilities are difficult to quantify or observe, and are mostly dependent on the existence of exploitable vulnerabilities in the target's system and on the target's level of cyber dependency. Establishing a strong link between a threat and a particular enemy is also made more difficult due to the uncertainties of attribution. Secondly, malwares have the ability to affect the subjectivity of human actors and decide on the parties of interest in every cyber incident. While it is true that the attacker can choose which hardware/software vulnerability to exploit and therefore which entity would have the responsibility to release a patch; it is the malware in many cases that determines in its propagation all the rest of affected targets who would be then required to apply those patches. That is, codes/software are capable of co-constituting actancy and agency in cybersecurity that do not excuslively result from human actions, but rather *emerge* regardless/in spite of them.

In addition, the logic of noise also contributes to the securitization of cybersecurity as entropic security. Just like noise is a challenge of information but one that disrupt rather than destroy, many of the threats that forms the core of cybersecurity lies in the realm of the mundane in contrast to the existential. In the majority of security research, existentiality is seen as intrinsic to security, as an essential legitimiser to urgency/immediacy, and as more than physical. In cybersecurity, however,

existentiality is *not as intrinsic* to security, *not as essential* for legitimising urgency, and is mostly *reduced* to the physical. Here, noise as disruption or interference in signal transmission in information theory can be used analogically to understand how cyber threats are constructed as urgent and immanent, without being existential. The majority of cyber threats resemble noise as a problem of communication in the sense that they are often *disruptive* rather than *destructive*. Existentiality do exist in cybersecurity debates, but just as *another* discourse in which assertions about destructions are usually limited to the military and intelligence. This does not mean that the cyber threat is not sometimes hyped, because hyping the threats does not necessarily entail existentiality. It is the physical elements of information that makes it possible for existentiality to register in cybersecurity discourses, due to the familiarity of the physical to our understanding of threats. Existentiality in the infosphere is connected to the possible physical damages as a result of a cyber attack, that is why most of such discourses are focused on the security of CNIs.

However, it is the simultaneous non-physicality of information that makes it difficult for existentiality to dominate the cyber threat perception. The general invisibility of cyber insecurity; the absence of adequate imagery; the replicability and retrievability of digital data; its capacity to exist in multiple places simultaneously; and the universality of digital devices are all important factors that challenge existentiality perceptions. Non-physicality too engenders uncertainties about whether an intrusion has taken place, identifying its starting point, and estimating the scale of the resulting damages even if/when an intrusion is detected. Nevertheless, just like noise in information theory, disruptive cyber incidents are seen as the parasite of information technologies in cybersecurity. They are normalised as an intrinsic element of the infosphere, yet one that needs to be resisted and minimised. This less than existential logic of noise is capable of invoking urgency and immediacy without existentiality and exceptionality.

Hitherto, all such conclusions are only valid when three methodological considerations are acknowledged as part of the non-anthropocentric approach of the thesis. The first is expanding the empirical analysis to include cybersecurity practices and policies, not just discursive utterances or speech acts. The second is applying a

multi-actor approach that considers the role of both state and non-state actors. These two points are important, because an approach that only analyses speech-acts of state actors – as done by the cyber securitization literature – would necessarily reach different conclusions about the security logics mentioned above. Existentiality, enmity, and emergency measures register more in speech acts than practices, and mostly in government discourses - particularly in those of the intelligence and the military. Thirdly, the assumptions and arguments presented by this thesis would not be applicable to a study of cybersecurity that only focus on high-profile, government-backed cyber attacks. While not denying their significance, these attacks are far less in number and frequency than all the other forms of cyber threats that constitute cybersecurity. Again, this is related to an adoption of a multi-actor approach that does not lock cybersecurity within security perceptions of the military and intelligence agencies. When private actors are included, the everyday and mundane cyber threats that might not get as much media attention would appear as important as the highly publicised ones in understanding the nature of security in this realm. That is to say, an approach that only focuses on speech-acts, state actors, and big cyber incidents, would still be confined to the Copenhagen School's assumptions about security logics, even if attempted to counter its anthropocentrism.

3. Contributions, limitations, and prospects for further research

This thesis contributes to the theoretical understanding of cybersecurity as a field that remains policy-oriented and under-theorised in International Relations and Security Studies. It does so by employing an inter-disciplinary approach that brings new insights to the study of cybersecurity from information sciences that have direct links to the evolution of its technologies. This is an approach that attends to the inherent multi-displinarity of this realm that cannot be grasped by resorting to theories of security alone. Additionally, it established a theoretical link between the 'cyber' and the 'informational' beyond the traditional distinctions between cybersecurity and information security. This is meant to overcome the ambiguities of the cyber terminology and account for the arguable novelty of this field by problematising its ontology instead of stopping at the stage of conceptualisations and definitions. The thesis also contributes to the study of the materialities of cybersecurity by transcending

the confines of anthropocentrism and representationalism. This was done to challenge perceptions of human control in constructing the security of information systems that evolved in paths humans could not fully envision; that operate in ways they cannot fully predict; and that produce threats they are not able to completely manage.

In a broader sense, the thesis also speaks to securitization theory, CSS, and the strand of research that aims at developing securitization beyond the Copenhagen School. It presented a form of securitization that is non-anthropocentric, problematises the referent object, and contextualises security logic(s) in constructing security as a process of co-production by human and non-human agents. Although this theorisation was specific to cybersecurity, it can be used to inductively study the securitization of other fields. Furthermore, the thesis is a contribution to the dialogue between new materialism and International Relations in general, and Security Studies in particular. By emphasising information as different from the *matter* that new materialism theorised for, the thesis can be considered an attempt to further develop ideas on the peculiarity of non-human agency, particularly in security construction. Importantly, it demonstrated the need for investigating the specificity of the different types of the non-human *things* instead of dealing with them as one homogenous category.

Moreover, through the notion of entropic security, the thesis shows that what matters for understanding security is not just the mere identification of referent objects as part of a security discourse. Instead, we need to study the ontology of the non-human referent object as a co-constitutive force in constructing the meaning and essence of security at large. This argument also speaks to CSS that attempt to incorporate new materialism or post-humanism in analysing security and questions of agency. It highlights the need for a study of security that goes beyond the mere inclusion of the non-human towards a search for alternative new materialist, post-humanist, or non-anthropocentric conceptualisations of 'security' that dismantles its humanist underpinnings.

However, this informational framework to the study of cybersecurity has been developed in relation to US policy, so more research is needed to explore its applicability in different cultural and political contexts. Despite the centrality of the case of the US in the origination and evolution of cybersecurity debates to date, it remains one among

many other important cases, and thus care must be taken in generalising from one case study. Although the theorisation of information as peculiar and agential is valid across cases, how this peculiarity and materiality are manifested empirically in the construction of cybersecurity could be context-specific. The theoretical framework advanced by this thesis can therefore lead to different conclusions when applied to different contexts; something that can only be proven by further research. This can be true particularly in cases where the terminology of *information* is used to counter the arguably Western *cyber* terminology, such as in Russia and China. It would be also important to see if the thesis arguments hold in cases that are traditionally seen as similar to the USA, such as the UK, and to be able to theoretically explain any possible deviances using the same non-anthropocentric, informational framework.

In addition to application to other cases, further research is also needed to examine the possible transformational capacity of information in other security fields. The core argument of the thesis is that information is peculiar, and its peculiarity engenders a peculiar cybersecurity due to its informational ontology. This was done to challenge the perception of cybersecurity as just another sector in which the dynamics of other security fields can be detected. It would thus be interesting to take this argument further to see how the transformative capacity of information can contribute to cybersecurity's potential transformative influences on the general meaning, practices, and logic(s) of security in other fields. It is a need for investigating how just as cybersecurity has broadened the security agendas of all state and non-state actors around the world, it may have also interacted transformatively across other security sectors. That is, further research is needed to examine not just how security is different in the infospere, but how the infosphere also transforms our general understanding of security beyond cybersecurity. It would be also useful for future research to explore whether entropic security and its logics could be applicable to other security sectors, particularly to ones that are considered relatively 'new', like food security, health security, etc. As put by Bruce Schneier in explaining the technical challenge of cybersecurity – a statement that can be extended to our theoretical understanding of security in International Relations:

> “We have some tricks, and we know how to avoid some obvious problems, but we have no scientific theory of security. It’s still a black art and, although we’re learning all the time, we have a long way to go.” (Overview of the Cyber Problem, 2003, p11)

BIBLIOGRAPHY

10 Cyber Security Facts and Statistics for 2018. (n.d.). Symantec. Retrieved 5 August 2019, from https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

Aalberts, T. E., & Werner, W. G. (2011). Mobilising Uncertainty and the Making of Responsible Sovereigns. *Review of International Studies*, *37*(05), 2183–2200.

Abbate, J. (1999). *Inventing the Internet*. MIT Press.

Abbate, J. (2001). Government, Business, and the Making of the Internet. *Business History Review*, *75*(01), 147–176.

Ablon, L., & Bogart, A. (2017). *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*. Rand Corporation.

Adams, C., & Thompson, T. L. (2016). *Researching a Posthuman World: Interviews with Digital Objects*. Springer.

Adriaans, P., & van Benthem, J. (Eds.). (2008). *Philosophy of Infomrmation* (Vol. 8). North Holland.

Agar, J. (2012). *Science in the 20th Century and Beyond*. Polity.

Agent-Based Software Development. (2004). Artech House.

Ahern, T. (1982, April 27). Experts Urge Computer Security. *The Associated Press*. https://www.nexis.com/

Aksoy, P., & DeNardis, L. (2007). *Information Technology in Theory*. Cengage Learning.

Albert, M., & Buzan, B. (2011). Securitization, Sectors and Functional Differentiation. *Security Dialogue*, *42*(4–5), 413–425.

Albeshri, A., Boyd, C., & Nieto, J. G. (2014). Enhanced Geoproof: Improved Geographic Assurance for Data in the Cloud. *International Journal of Information Security*, *13*(2), 191–198.

Aljunied, S. M. A. (2019). The Securitization of Cyberspace Governance in Singapore. *Asian Security*, 1–20.

Alker, H. R. (2006). On securitization politics as contexted texts and talk. *Journal of International Relations and Development*, *9*(1), 70–80.

Ames, Jr. (1980). Security Kernels: Are They the Answer to the Computer Security Problem. *Wescon Technical Papers*, *23*.

America is Under Cyber Attack: Why Urgent Action is Needed: Hearing before the Subcommittee on Oversight, Investigation, and Management, of the Committee on Homeland Security (Serial No. 112-85), U.S. House of Representatives, 112th Cong. (2012)

Amoore, L. (2013). *The Politics of Possibility: Risk and Security Beyond Probability*. Duke University Press.

Andersen, R. S., Vuori, J. A., & Mutlu, C. E. (2014). Visuality. In C. Aradau, J. Huysmans, A. Neal, & N. Voelkner (Eds.), *Critical Security Methods: New Frameworks for Analysis* (pp. 95–117). Routledge.

Applegate, S. (2015). Cyber Conflict: Disruption and Exploitation in the Digital Age. In F. Lemieux (Ed.), *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*. Springer.

Aradau, C. (2004). Security and the Democratic Scene: Desecuritization and Emancipation. *Journal of International Relations and Development*, *7*(4), 388–413.

Aradau, C. (2010). Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue*, *41*(5), 491–514.

Aradau, C. (2014). The Promise of Security: Resilience, Surprise and Epistemic Politics. *Resilience*, *2*(2), 73–87.

Aradau, C. (2016). Risk, (in)security and International Politics. In A. Burgess, J. O. Zinn, & A. Alemanno (Eds.), *Routledge Handbook of Risk Studies*. Routledge, Taylor & Francis Group.

Aradau, C., Lobo-Guerrero, L., & Van Munster, R. (2008). Security, Technologies of Risk, and the Political: Guest Editors' Introduction. *Security Dialogue*, *39*(2–3), 147–154.

Aradau, C., & Van Munster, R. (2007). Governing Terrorism Through Risk: Taking Precautions,(un) Knowing the Future. *European Journal of International Relations*, *13*(1), 89–115.

Aradau, C., & Van Munster, R. (2016). Poststructuralist Approaches to Security. In *Routledge Handbook of Security Studies: Second Edition* (pp. 75–84). Taylor and Francis.

Arnheim, R. (2010). *Entropy and Art: An Essay on Disorder and Order*. University of California Press.

Arquilla, J. (2009). Information Wars. In G. H. Fagan & R. Munck (Eds.), *Globalization and Security: Social and cultural aspects. Introduction to volume 2* (pp. 206–220). ABC-CLIO.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar Is Coming! *Comparative Strategy*, *12*(2), 141–165.

Arquilla, J., & Ronfeldt, D. (1996). Information, Power, and Grand Strategy: In Athena's Camp. *Significant Issues Series-Center for Strategic and International Studies*, *18*, 132–180

Aven, T. (2016). The Reconceptualization of Risk. In A. Burgess, J. O. Zinn, & A. Alemanno (Eds.), *Routledge Handbook of Risk Studies* (pp. 58–72). Routledge, Taylor & Francis Group.

Ashby, W. R. (1958). *An Introduction to Cybernetics*. Chapman and Hall.

Assessing Persistent and Emerging Cyber Threats to the U.S. in the Homeland, Joint hearing before the Subcommittee on Counterterrorism and Intelligence and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security (Serial No. 113-69), U.S. House of Representatives, 113th Cong. (2014).

Babcock, C. R. (1977, June 17). Justice Puts Computer Plan on 'Hold'; Plan Raised Fears of 'Police State' Jurisdictional Crime Data Exchange. *The Washington Post*. https://www.nexis.com/

Bakke, B. B. (1983, April 25). Computer Security a Major Headache. *United Press International*. https://www.nexis.com/

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

Balzacq, T. (2009). Constructivism and Securitization Studies. In M. D. Cavelty & V. Mauer (Eds.), *The Routledge Handbook of Security Studies* (pp. 56–72). Routledge.

Balzacq, T. (2011). Enquiries into Methods: A New Framework for Securitization Analysis. In T. Balzacq (Ed.), *Securitization Theory: How Security Problems Emerge and Dissolve* (pp. 31–54). Routledge.

Balzacq, T., & Dunn Cavelty, M. (2016). A Theory of Actor-Network for Cyber-Security. *European Journal of International Security*, *1*(02), 176–198.

Balzacq, T., Leonard, S., & Depauw, S. (2015). The Political Limits of Desecuritization: Security, Arms Trade, and the EU's Economic Targets. In T. Balzacq (Ed.), *Contesting Security: Strategies and Logics* (pp. 104–121). Routledge.

Bammer, G., Smithson, M., & the Goolabri Group. (2012). The Nature of Uncertainty. In G. Bammer & M. Smithson (Eds.), *Uncertainty and Risk: Multidisciplinary Perspectives* (pp. 289–304). Routledge.

Barad, K. (2003). Posthumanist Performativity: Toward an Understanding of How Matter Comes to Matter. *Journal of Women in Culture and Society*, *28*(3), 801–831.

Barad, K. (2007). *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*. Duke University Press.

Barbour, J. (2015). Bit from It. In A. Aguirre, B. Foster, & Z. Merali (Eds.), *It From Bit or Bit From It?: On Physics and Information* (pp. 197–212). Springer.

Barnard-Wills, D., & Ashenden, D. (2012). Securing Virtual Space Cyber War, Cyber Terror, and Risk. *Space and Culture*, *15*(2), 110–123.

Battail, G. (2013). *Information and Life*. Springer Science & Business Media.

Baur-Ahrens, A. (2017). The Power of Cyberspace Centralisation: Analysing the Example of Data Territorialisation. In M. Leese & S. Wittendorp (Eds.), *Security/Mobility: Politics of Movement* (pp. 37–56). Oxford University Press.

Beck, U. (1992). *Risk Society: Towards a New Modernity*. SAGE Publications Ltd.

Beck, U. (1999). *World Risk Society*. Polity.

Beck, U. (2002). The Terrorist Threat: World Risk Society Revisited. *Theory, Culture & Society*, *19*(4), 39–55.

Beck, U. (2006). Living in the World Risk Society. *Economy and Society*, *35*(3), 329–345.

Behnke, A. (2006). No way out: Desecuritization, emancipation and the eternal return of the political - A reply to Aradau. *Journal of International Relations and Development*, *9*(1), 62–69.

Behrenshausen, B. G. (2016). *Information in Formation: Power and Agency in Contemporary Informatic Assemblages* [Ph.D., The University of North Carolina at Chapel Hill]. https://search.proquest.com/docview/1805474652/abstract/FD12EAFABFF54374PQ/1

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

Ben-Naim, A. (2008). *A Farewell to Entropy: Statistical Thermodynamics Based on Information*. World Scientific.

Bennett, J. (2009). *Vibrant Matter: A Political Ecology of Things*. Duke University Press.

Bennett, J. (2010). A Vitalist Stopover on the Way to a New Materialism. In D. Coole & S. Frost (Eds.), *New Materialisms: Ontology, Agency, and Politics* (pp. 47–69). Duke University Press.

Bennett, J. (2015). Systems and Things: On Vital Materialism and Object-Oritened Philosophy. In R. A. Grusin & R. Grusin (Eds.), *The Nonhuman Turn* (pp. 223–240). University of Minnesota Press.

Berry, D. (2011). *The Philosophy of Software: Code and Mediation in the Digital Age*. Springer.

Berry, D., & Dieter, M. (Eds.). (2015). *Postdigital Aesthetics: Art, Computation And Design*. Springer.

Berry, D. M. (2012). The Social Epistemologies of Software. *Social Epistemology*, *26*(3–4), 379–398.

Berry, D. M. (2014). *Critical Theory and the Digital*. A&C Black.

Best, S. (1991). Chaos and entropy: Metaphors in postmodern science and social theory. *Science as Culture*, *2*(2), 188–226.

Betz, D. J., & Stevens, T. (2013). Analogical Reasoning and Cyber Security. *Security Dialogue*, *44*(2), 147–164.

Bieber, F. (2000). Cyberwar or Sideshow? The Internet and the Balkan Wars. *Current History*, *99*(635), 124–128.

Bigo, D. (2000). When Two Become One: Internal and External Securitisations in Europe. In M. Kelstrup & M. Williams (Eds.), *International Relations Theory and The Politics of European Integration: Power, Security and Community* (pp. 171–204). Routledge.

Bigo, D. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives*, *27*(1), 63–92.

Bigo, D. (2006). Security, Exception, Ban and Surveillance. In D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond* (pp. 46–68). Willan Publishing.

Bigo, D. (2008). Globalised (In)security: The Field and the Ban-Opticon. In D. Bigo & A. Tsoukala (Eds.), *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11* (pp. 5–49). Routledge.

Biham, E., Carmeli, Y., & Shamir, A. (2016). Bug Attacks. *Journal of Cryptology*, *29*(4), 775–805.

Bishop, M. (2003). What Is Computer Security? *IEEE Security & Privacy*, *1*(1), 67–69.

Blanchette, J.-F. (2011). A Material History of Bits. *Journal of the American Society for Information Science and Technology*, *62*(6), 1042–1057.

Blum, A. (2012). *Tubes: Behind the Scenes at the Internet*. Penguin UK.

Boebert, W. E. (2010). A Survey of Challenges in Attribution. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 41–52.

Bogost, I. (2012). *Alien Phenomenology, Or, What It's Like to be a Thing*. University of Minnesota Press.

Boomen, M. van den. (2009). *Digital Material: Tracing New Media in Everyday Life and Technology*. Amsterdam University Press.

Booth, K. (1991). Security and Emancipation. *Review of International Studies*, *17*(4), 313–326.

Booth, K. (2007). *Theory of World Security* (1 edition). Cambridge University Press.

Bourne, M., Johnson, H., & Lisle, D. (2015). Laboratizing the Border: The Production, Translation and Anticipation of Security Technologies. *Security Dialogue*, *46*(4), 307–325.

Bousquet, A. (2013). Welcome to the Machine: Rethinking Technology and Society through Assemblage Theory. In S. Curtis (Ed.), *Reassembling International Theory: Assemblage Thinking and International Relations* (pp. 91–97). Springer.

Bousquet, A., & Curtis, S. (2011). Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations. *Cambridge Review of International Affairs*, *24*(1), 43–62.

Bowles, M. D. (1996). US Technological Enthusiasm and British Technological Skepticism in the Age of the Analog Brain. *IEEE Annals of the History of Computing*, *18*(4), 5–15.

Boyd, D. (2010). Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In Z. Papacharissi (Ed.), *A Networked Self: Identity, Community, and Culture on Social Network Sites* (pp. 39–58). Routledge.

Bradshaw, J. M. (1997). Introduction. In J. M. Bradshaw (Ed.), *Software Agents* (pp. 3–48). AAAI Press.

Braidotti, R. (2013). *The Posthuman*. John Wiley & Sons.

Brantly, A. F. (2014). Cyber Actions by State Actors: Motivation and Utility. *International Journal of Intelligence and Counterintelligence*, *27*(3), 465–484.

Bratteteig, T. (2010). A Matter of Digital Materiality. In I. Wagner, D. Stuedahl, & T. Bratteteig (Eds.), *Exploring Digital Design: Multi-Disciplinary Design Practices* (pp. 147–169). Springer, London.

Braun, B., Schindler, S., & Wille, T. (2018). Rethinking Agency in International Relations: Performativity, Performances and Actor-Networks. *Journal of International Relations and Development*, *22*(4), 787–807.

Brendon, L. K. (2001). ARPANET: An Efficient Machine as Social Discipline. *Science as Culture*, *10*(1), 73–95.

Brenner, S. W. (2007). History of Computer Crime. In K. M. M. de Leeuw & J. Bergstra (Eds.), *The History of Information Security* (pp. 705–721). Elsevier Science B.V.

Brenner, W., Zarnekow, R., & Wittig, H. (2012). *Intelligent Software Agents: Foundations and Applications*. Springer Science & Business Media.

Brink. (2000). Secular Icons: Looking at Photographs from Nazi Concentration Camps. *History and Memory*, *12*(1), 135.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., & Filar, B. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. *arXiv preprint arXiv:1802.07228*.

Bryant, L. R. (2011). *The Democracy of Objects*. Open Humanities Press.

Bryant, L. R. (2014). *Onto-Cartography: An Ontology of Machines and Media* (1 edition). Edinburgh University Press.

Buchanan, B. (2016a). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. C. Hurst & Co Publishers.

Buchanan, B. (2016b). Cryptography and Sovereignty. *Survival*, *58*(5), 95–122.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Buckland, M. K. (1991). *Information and Information Systems*. ABC-CLIO.

Burgess, A. (2016). Introduction. In A. Burgess, A. Alemanno, & J. O. Zinn (Eds.), *Routledge Handbook of Risk Studies*. Routledge, Taylor & Francis Group.

Burgin, M. (2010). *Theory of Information: Fundamentality, Diversity and Unification*. World Scientific.

Burgin, M., & Dodig-Crnkovic, G. (2013). *The Nature of Computation and the Development of Computational Models*. Computability in Europe 2013 (CiE 2013). https://pdfs.semanticscholar.org/3c18/1e61ef5a48cbcb084e68e93433ed40671612.pdf

Burks, A. W. (2014). From ENIAC to the Stored-Program Computer: Two Revolutions in Computers. In N. Metropolis (Ed.), *History of Computing in the Twentieth Century* (pp. 311–344). Elsevier.

Burnham, D. (1985, June 28). Lack of Security in Computers Seen. *The New York Times*. https://www.nexis.com/

Buzan, B. (1991). *People, States and Fear: An Agenda for International Security in the Post-Cold War Era*. Harvester Wheatsheaf.

Buzan, B., & Little, R. (1998). *International Systems in World History: Remaking the Study of International Relations*. Oxford University Press, U.S.A.

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

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

Byles, T. (1988, December 9). Public Awareness Vital to Computer Security. *Journal of Commerce*. https://www.nexis.com/

Bynum, T. W. (2008). Norbert Wiener and the Rise of Information Ethics. In J. Weckert & J. Van Den Hoven (Eds.), *Information Technology and Moral Philosophy* (pp. 1–25). Cambridge University Press.

Bynum, T. W. (2016). Informational Metaphysics: The Informational Nature of Reality. In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 203–218). Routledge.

Campbell-Kelly, M., Aspray, W., Ensmenger, N., Yost, J. R., & Aspray, W. (2014). *Computer: A History of the Information Machine* (Third edition). Westview Press, A Member of the Perseus Books Group.

Cannizzaro, S. (2016). The Philosophy of Semiotic Information. In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 290–303). Routledge.

Carr, J. (2012). *Inside Cyber Warfare* (2nd ed). O'Reilly.

Carr, M. (2016). Public–Private Partnerships in National Cyber-Security Strategies. *International Affairs*, *92*(1), 43–62.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press.

Ceruzzi, P. (2012). *Computing: A Concise History*. MIT Press.

Ceruzzi, P. E. (2003). *A History of Modern Computing* (2nd ed). MIT Press.

Chandler, D. (2014). *Resilience: The Governance of Complexity*. Routledge.

Chernus, I. (2008). *Apocalypse Management: Eisenhower and the Discourse of National Insecurity* (1 edition). Stanford University Press.

Chesnoy, J. (Ed.). (2015). *Undersea Fiber Communication Systems*. Academic Press.

Chittister, C. G., & Haimes, Y. Y. (2006). Cybersecurity: From Ad Hoc Patching to Lifecycle of Software Engineering. *Journal of Homeland Security and Emergency Management*, *3*(4), 17–24.

Chong, J. (2016). Bad Code: Exploring Liability in Software Development. In R. Harrison, T. Herr, & R. J. Danzig (Eds.), *Cyber Insecurity: Navigating the Perils of the Next Information Age* (pp. 69–86). Rowman & Littlefield Publishers.

Choucri, N., & Clark, D. D. (2013). Who Controls Cyberspace? *Bulletin of the Atomic Scientists*, *69*(5), 21–31.

Chun, W. H. K. (2011). *Programmed Visions: Software and Memory*. MIT Press.

Ciută, F. (2009). Security and the Problem of Context: A Hermeneutical Critique of Securitisation Theory. *Review of International Studies*, *35*(02), 301.

Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.

Cobb, S., & Lee, A. (2014). *Malware is Called Malicious for a Reason: The Risks of Weaponizing Code*. 71–84.

Colburn, T. R. (1999). Software, Abstraction, And Ontology. *The Monist*, *82*(1), 3–19.

Collins, A. (2005). Securitization, Frankenstein's Monster and Malaysian Education. *The Pacific Review*, *18*(4), 567–588.

Columbus, L. (2020, April 5). 2020 Roundup Of Cybersecurity Forecasts And Market Estimates. *Forbes*. https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/

Cooper, C. (2018, May 16). *WannaCry: Lessons Learned 1 Year Later*. https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later

Corning, P. A. (2002). The Re-Emergence of "Emergence": A Venerable Concept in Search of a Theory. *Complexity*, *7*(6), 18–30.

Cornish, P. (2015). Governing Cyberspace through Constructive Ambiguity. *Survival*, *57*(3), 153–176.

Corry, O. (2012). Securitisation and 'Riskification': Second-Order Security and the Politics of Climate Change. *Millennium - Journal of International Studies*, *40*(2), 235–258.

Crime Computers. (1977, April 11). *The Washington Post*. https://www.nexis.com/

Cudworth, E., Hobden, S., & Kavalski, E. (2018). Introduction: Framing the Posthuman Dialogues in International Relations. In E. Cudworth, S. Hobden, & E. Kavalski (Eds.), *Posthuman Dialogues in International Relations* (pp. 1–14). Routledge.

Cyber Incident Response: Bridging the Gap between Cybersecurity and Emergency Management, *Joint hearing before the Subcommittee on Emergency Preparedness, Response, and Communications, of the Committee on Homeland Security* (Serial No. 113-39), U.S. House of Representatives, 113th Cong. (2013).

Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure: Hearing before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, of the Committee on Homeland Security House of Representatives (Serial No. 110-26), U.S. House of Representatives, 112th Cong. (2007).

Cyber Preparedness and Response at the Local Level, Field Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 114-62), U.S. House of Representatives, 114th Cong. (2016).

Cyber Security – 2010: Hearings before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 111-1103), U.S. Senate, 111th Cong. (2010).

Cyber Security, Hearing before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 113-790), U.S. Senate, 113th Cong. (2014).

Cyber Security: Recovery and Reconstitution of Critical Networks, Hearing before the Federal Financial Management, Government Information, and International Security Subcommittee, of the Committee on Homeland Security and Governmental Affairs, U.S. Senate, Cong. 109th. (2006).

Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed Healthcare.gov? Hearing before the Committee on Homeland Security (Serial No. 113-41), U.S. House of Representatives, 113th Cong. (2013).

Cyber Storm: Securing Cyber Space. (n.d.). Department of Homeland Security. Retrieved 15 October 2018, from https://www.dhs.gov/cyber-storm

Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure, Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 113-9), U.S. House of Representatives, 113th Cong. (2013).

Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 113-9), House of Representatives, 113th Cong. (2013).

Cybersecurity – Getting It Right: Hearing of the subcommittee on Cybersecurity, Science, and Research, and Development, before the Select Committee on Homeland Security (Serial No. 108-18), U.S. House of Representatives, 108th Cong. (2003)

Cybersecurity Recommendations for the Next Administration, Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, of the Committee on Homeland Security (Serial No. 110-138), U.S. House of Representatives, 110th Cong. (2008).

Cybersecurity-2009, Hearings before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 111-724), U.S. Senate, 111th Cong. (2009).

Cybersecurity-2010, Hearings before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 111-1103), U.S. Senate, 111th Cong. (2010).

Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland, Hearing before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 113-712), U.S. Senate, 113th Cong. (2014).

Cybersecurity: Developing a National Strategy: Hearing before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 111-724), U.S. Senate, 111th Cong. (2009).

Cybersecurity: DHS' Role, Federal Efforts, and National Policy: Hearing before the Committee on Homeland Security (Serial No. 117-71), U.S. House of Representatives, 111th Cong. (2010).

Daskal, J. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. *Stanford Law Review*. https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/

Data Breach on the Rise: Protecting Information from Harm: Hearing before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 113-790), U.S. Senate, 113th Cong. (2014).

Davies, P. (2019). *The Demon in the Machine: How Hidden Webs of Information Are Finally Solving the Mystery of Life*. Penguin UK.

De Goede, M. (2004). Repoliticizing Financial Risk. *Economy and Society*, *33*(2), 197–217.

Deacon, T. W. (2010). What is Missing from Theories of Information? In P. Davies & N. H. Gregersen (Eds.), *Information and the Nature of Reality: From Physics to Metaphysics* (pp. 146–169). Cambridge University Press.

Deibert, R. (2015). The Geopolitics of Cyberspace After Snowden. *Current History*, *114*(768), 9–15.

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War. *Security Dialogue*, *43*(1), 3–24.

Deibert, Ronald J., & Crete-Nishihata, M. (2012). Global Governance and the Spread of Cyberspace Controls. *Global Governance*, *18*(3), 339–361.

Dembski, W. A. (2016). *Being as Communion: A Metaphysics of Information*. Routledge.

DeNardis, L. (2007). A History of Internet Security. In K. M. M. de Leeuw & J. Bergstra (Eds.), *The History of Information Security* (pp. 681–704). Elsevier Science B.V.

Department of Homeland Security. (2011). *Blueprint for a Secure Cyber Future*. https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure: Hearing before the Committee on Homeland Security (Serial No. 113-4), U.S. House of Representatives, 113th Cong. (2013).

Dillon, M. (2002). Network Society, Network-centric Warfare and the State of Emergency. *Theory, Culture & Society*, *19*(4), 71–79.

Dipert, R. R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics*, *9*(4), 384–410.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information Security: The Moving Target. *Computers & Security*, *28*(3–4), 189–198.

Do the Payment Card Industry Data Standards Reduce Cybercrime? Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, of the Committee on Homeland Security (Serial No. 111-14), U.S. House of Representatives, 111th Cong. (2009).

Dourish, P., & Mazmanian, M. (2013). Media as Material: Information Representations as Material Foundations for Organizational Practice. In P. R. Carlile, D. Nicolini, A. Langley, & H. Tsoukas (Eds.), *How Matter Matters: Objects, Artifacts, and Materiality in Organization Studies* (pp. 92–118). OUP Oxford.

Dourish, P. (2016). Rematerializing the Platform: Emulation and the Digital-Material. In S. Pink, E. Ardèvol, & D. Lanzeni (Eds.), *Digital Materialities: Design and Anthropology* (pp. 29–44). Bloomsbury Publishing.

Dourish, P. (2017). *The Stuff of Bits: An Essay on the Materialities of Information*. MIT Press.

Doyle, J. J. (1984, February 20). '"Hackers"' Biggest Security Threat to Computer Industry. *United Press International*. https://www.nexis.com/

Draft Legislative Proposal on Cybersecurity, Hearing before the Subcommittee on Cybersecurity Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 112-61), U.S. House of Representatives, 102th Cong. (2011).

Drake, W. J. (2005). *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG)*. United Nations Publications.

Dunn Cavelty, M. (2008a). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge.

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), 19–36.

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

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715.

Dunn Cavelty, M. (2016). Cyber-Security and Private Actors. In R. Abrahamsen & A. Leander (Eds.), *Routledge Handbook of Private Security Studies* (pp. 89–99). Routledge, Taylor & Francis Group.

Dunn Cavelty, M. (2019). The Materiality of Cyberthreats: Securitization Logics in Popular Visual Culture. *Critical Studies on Security*, *7*(2), 138–151.

Dunn Cavelty, M. (2020). Cybersecurity Between Hypersecuritization and Technological Routine. In E. Tikk & M. Kerttunen (Eds.), *Routledge Handbook of International Cybersecurity*. Routledge.

Dunn Cavelty, M., Balzacq, T., & Fischer, S.-C. (2017). Killer robots' and Preventive Arms Control. In *Routledge Handbook of Security Studies* (pp. 457–468). Routledge.

Dunn Cavelty, M., & Suter, M. (2009). Public–Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179–187.

Durante, M. (2017). *Ethics, Law and the Politics of Information: A Guide to the Philosophy of Luciano Floridi*. Springer.

Dyer-Witheford, N. (2002). E-Capital and the Many-Headed Hydra. In G. Elmer (Ed.), *Critical Perspectives on the Internet* (pp. 129–164). Rowman & Littlefield.

Dyson, F. (2001, March 13). *Is Life Analog or Digital?* https://www.edge.org/conversation/freeman_dyson-is-life-analog-or-digital

Eastman, T. E., & Keeton, H. (Eds.). (2004). *Physics and Whitehead: Quantum, Process, and Experience*. SUNY Press.

Easttom, C. (2011). *Computer Crime, Investigation, and the Law*. Cengage Learning.

Edwards, P. N. (1997). *The Closed World: Computers and the Politics of Discourse in Cold War America*. MIT Press.

EINSTEIN. (n.d.). Department of Homeland Security. Retrieved 15 October 2018, from https://www.dhs.gov/einstein

Eisenhower, D. D. (1960). *Public Papers of the Presidents of the United States, Dwight D. Eisenhower: Containing the Public Messages, Speeches, and Statements of the President, January 20, 1953 to January 20, 1961*. U.S. Government Printing Office.

Elbe, S. (2008). Risking Lives: AIDS, Security and Three Concepts of Risk. *Security Dialogue*, *39*(2–3), 177–198.

Eldred, M. (2013). *The Digital Cast of Being: Metaphysics, Mathematics, Cartesianism, Cybernetics, Capitalism, Communication*. Walter de Gruyter.

Ellis, R., & Mohan, V. (Eds.). (2019). *Rewired: Cybersecurity Governance*. John Wiley & Sons.

Ellison, R. (1978). Does Computer Security Meet Privacy Requirements. *Information Privacy*, *1*(1), 33–37.

Elmer-Dewitt, P. (1988, September 26). Technology: Invasion of the Data Snatchers. *Time*. http://content.time.com/time/subscriber/article/0,33009,968508-2,00.html

Emerging Cyber Threats to the United States: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 114-55), U.S. House of Representatives, Cong. 114th. (2016).

Emerson, R. G. (2016). Limits to a Cyber-Threat. *Contemporary Politics*, *22*(2), 178–196.

Enhancing and Implementing the Cybersecurity Elements of the Sector-Specific Plans: Joint Hearing before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, joint with the Subcommittee on Transportation Security and Infrastructure Protection, of the Committee on Homeland Security (Serial No. 110-82), U.S. House of Representatives, 110th Cong. (2007).

Enhancing Preparedness and Response Capabilities to Address Cyber Threats: Joint Hearing before the Subcommittee on Emergency Preparedness, Response, and Communications, and the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, of the Committee on Homeland Security (Serial No. 114-71), U.S. House of Representatives, 114th Cong. (2016).

Eriksson, Johan. (2001). Cyberplagues, IT, and Security: Threat Politics in the Information Age. *Journal of Contingencies and Crisis Management*, *9*(4), 200–210.

Etzioni, A. (2011). Cybersecurity in the private sector. *Issues in Science and Technology*, *28*(1), 58–62.

Evans, J., & Schneider, G. (2008). *New Perspectives on the Internet, Brief*. Cengage Learning.

Evens, A. (2015). *Logic of the Digital*. Bloomsbury Publishing.

Examining the Cyber Threat to Critical Infrastructure and the American Economy: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 112-11), U.S. House of Representatives, 112th Cong. (2012).

Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal, Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 112-33), U.S. House of Representatives, 112th Cong. (2011).

Examining the President's Cybersecurity Information-sharing Proposal, Hearing before the Committee on Homeland Security (Serial No. 114-4), U.S. House of Representatives, 114th Cong. (2015).

Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 113-17), House of Representatives, 113th Cong. (2013).

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40.

Ferrando, F. (2013). Posthumanism, Transhumanism, Antihumanism, Metahumanism, and New Materialisms: Differences and Relations. *Existenz*, *8*(2), 26–32.

Fidler, M. (2016). Government Acquisition and Use of Zero-Day Software Vulnerabilities. In R. Harrison & T. Herr (Eds.), *Cyber Insecurity: Navigating the Perils of the Next Information Age* (pp. 3–18). Rowman & Littlefield Publishers.

Fine, L. H. (1982). The Total Computer Security Concept and Security Policy. *EDPACS*, *10*(5), 1–20.

FireEye. (2012). *Deep Dive into Cyber Reality: Security Effectiveness Report 2020*. https://content.fireeye.com/security-effectiveness/rpt-security-effectiveness-2020-deep-dive-into-cyber-reality

Fitzgerlad, J. (1984, February 3). Insiders Threat to Computer Security. *The American Banker*. https://www.nexis.com/

Flamm, K. (1988). *Creating the Computer: Government, Industry, and High Technology*. Brookings Institution Press.

Fliegauf, M. T. (2016). In Cyber (Governance) We Trust. *Global Policy*, *7*(1), 79–82.

Floridi, L. (2008). Modern Trends in Philosophy of Information. In P. Adriaans & J. van Benthem (Eds.), *Philosophy of Information* (pp. 117–136). North Holland.

Floridi, L. (2009). Philosophical Conceptions of Information. In G. Sommaruga (Ed.), *Formal Theories of Information: From Shannon to Semantic Information Theory and General Concepts of Information* (pp. 13–53). Springer.

Floridi, L. (2010). *Information: A Very Short Introduction*. OUP Oxford.

Floridi, L. (2010). Ethics after the Information Revolution. In L. Floridi (Ed.), *The Cambridge Handbook of Information and Communication Ethics* (pp.3-19). Cambridge University Press.

Floridi, L. (2013a). *The Philosophy of Information*. OUP Oxford.

Floridi, L. (2013b). *The Ethics of Information*. OUP Oxford.

Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. OUP Oxford.

Floridi, L. (Ed.). (2016). *The Routledge Handbook of Philosophy of Information*. Routledge.

Floyd, R. (2011). Can Securitization Theory Be Used in Normative Analysis? Towards a Just Securitization Theory. *Security Dialogue*, *42*(4–5), 427–439.

Floyd, R. (2015). Just and Unjust Desecuritization. In T. Balzacq (Ed.), *Contesting Security: Strategies and Logics* (pp. 122–138). Routledge.

Floyd, R. (2016). Extraordinary or Ordinary Emergency Measures: What, and Who, Defines the 'success' of Securitization? *Cambridge Review of International Affairs*, *29*(2), 677–694.

Forman, P. (1987). Behind Quantum Electronics: National Security as Basis for Physical Research in the United States, 1940-1960. *Historical Studies in the Physical and Biological Sciences*, *18*(1), 149–229.

Frabetti, F. (2015). *Software Theory: A Cultural and Philosophical Study*. Rowman & Littlefield International.

Fradkov, A. (2007). *Cybernetical Physics: From Control of Chaos to Quantum Control*. Springer.

Francisco, S. (1982, March 2). Students Figure Way To Foil Computer Security. *The Associated Press*. https://www.nexis.com/

Fraser, E. (2016). Data Localisation and the Balkanisation of the Internet. *SCRIPTed*, *13*(3), 359–373.

Fresco, N., & Wolf, M. J. (2016). Information Processing and Instructional Information. In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 77–89). Routledge.

Friis, K., & ReichBorn-Kjennerud, E. R. (2016). From Cyber Threats to Cyber Risks. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives* (pp. 39–54). Routledge.

Friis, K., & Ringsmose, J. (Eds.). (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. Routledge.

Fry, H. (2018). *Hello World: How to be Human in the Age of the Machine*. Penguin Random House UK.

Futter, A. (2018). 'Cyber' Semantics: Why We Should Retire the Latest Buzzword in Security Studies. *Journal of Cyber Policy*, *3*(2), 201–216.

G. Wiesel. (1973). Computer crime. Part 2: Data security. *Data Report*, *1*(4), 24–27.

Gardner, P. E. (1989). The Internet Worm: What Was Said and When. *Computers and Security*, *8*(4), 305–316.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, *38*(2), 41–73.

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, *24*(2), 316–348.

Geers, K. (2011). *Strategic Cyber Security*. Kenneth Geers.

Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *Washington Post*. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Georgieva, I. (2020). The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace. *Contemporary Security Policy*, *41*(1), 33–54.

Gershenson, C. (2012). The World as Evolving Information. In A. A. Minai, D. Braha, & Y. Bar-Yam (Eds.), *Unifying Themes in Complex Systems VII: Proceedings of the Seventh International Conference on Complex Systems* (pp. 100–115). Springer Science & Business Media.

Giles, K., & Ii, W. H. (2013). *Divided by a Common Language: Cyber Definitions in Chinese, Russian and English* (K. Podins, J. Stinissen, & M. Maybaum, Eds.; p. 17). NATO CCD COE Publications.

Gjelten, T. (2013). FIRST STRIKE: US Cyber Warriors Seize the Offensive. *World Affairs*, *175*(5), 33–43.

Gleick, J. (2011). *The Information: A History, a Theory, a Flood*. HarperCollins Publishers.

Goffey, A. (2017). The Obscure Objects of Object Orientation. In M. Fuller (Ed.), *How To Be a Geek: Essays on the Culture of Software* (pp. 15–36). John Wiley & Sons.

Goodman, S. E., Kirk, J. C., & Kirk, M. H. (2007). Cyberspace as a Medium for Terrorists. *Technological Forecasting and Social Change*, *74*(2), 193–210.

Graham, S. D. N. (2005). Software-Sorted Geographies. *Progress in Human Geography*, *29*(5), 562–580.

Greenfield, A. (2010). *Everyware: The Dawning Age of Ubiquitous Computing*. New Riders.

Gregoire, N., & Catherine, N. (2012). *Foundations of Complex Systems: Emergence, Information And Prediction* (2nd Edition). World Scientific.

Gregor, S., & Hart, D. N. (2005). *Information Systems Foundations: Constructing and Criticising: Constructing and Criticising*. ANU E Press.

Greven, A., Keller, G., & Warnecke, G. (Eds.). (2014). *Entropy*. Princeton University Press.

Grisogono, A.-M. (2017). How Did Information Emerge? In S. I. Walker, P. C. W. Davies, & G. F. R. Ellis (Eds.), *From Matter to Life: Information and Causality* (pp. 61–96). Cambridge University Press.

Grösser, S. N., & Zeier, R. (2012). *Systemic Management for Intelligent Organizations: Concepts, Models-Based Approaches and Applications*. Springer Science & Business Media.

Guide to NIST (National Institute of Standards and Technology). (1997). DIANE Publishing.

H.R. 285: Department of Homeland Security Cybersecurity Enhancement Act of 2005: Hearing before the Subcommittee Economic Security, Infrastructure Protection, and Cybersecurity, of the Committee on Homeland Security (Serial No. 109-11), House of Representatives, 109th Cong. (2005).

Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security: Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology (Serial No. 110-52), House of Representatives, 110th Cong. (2007).

Hafner, K., & Lyon, M. (1998). *Where Wizards Stay up Late: The Origins of the Internet* (Touchstone ed edition). Simon & Schuster.

Hagmann, J., & Dunn Cavelty, M. (2012). National Risk Registers: Security Scientism and the Propagation of Permanent Insecurity. *Security Dialogue*, *43*(1), 79–96.

Halbert, D. (2016). Intellectual Property Theft and National Security: Agendas and Assumptions. *The Information Society*, *32*(4), 256–268.

Hallberg, B. (2009). *Networking: A Beginner's Guide* (Fifth Edition). McGraw Hill Professional.

Hancock, J. L. (1981, February 10). Management Involvement is Essential to Computer Security. *The American Banker*. https://www.nexis.com/

Hansen, H. K. (2017). What Do Big Data Do in Global Governance? *Global Governance: A Review of Multilateralism and International Organizations*, *23*(1).

Hansen, L. (2011). Theorizing the image for Security Studies: Visual securitization and the Muhammad Cartoon Crisis. *European Journal of International Relations*, *17*(1), 51–74.

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

Haraway, D. (2006). A Cyborg Manifesto: Science, technology, and Socialist-Feminism in the Late 20th Century. In *the International Handbook of Virtual Learning Environments* (pp. 117-158). Springer, Dordrecht.

Harding, L. (2014). *The Snowden Files: The Inside Story of the World's Most Wanted Man*. Guardian Faber Publishing.

Hare, F. (2009). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? *Cryptology and Information Security Series*, *3*, 88–105.

Hare, Forrest. (2012). The Significance of Attribution to Cyberspace Coercion: A Political Perspective. *Cyber Conflict (Cycon), 2012 4th International Conference On Cyber Conflict*, 1–15.

Harman, G. (2009). *Prince of Networks: Bruno Latour and Metaphysics*. Re.Press.

Harman, G. (2018). *Object-Oriented Ontology: A New Theory of Everything*. Penguin UK.

Harshman, N. L. (2016). Physics and Information. In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 7–14). Routledge.

Hart, J. A. (2011). The Net Neutrality Debate in the United States. *Journal of Information Technology & Politics*, *8*(4), 418–443.

Harvey, R., & Weatherburn, J. (2018). *Preserving Digital Materials*. Rowman & Littlefield.

Hayles, N. K. (2008). *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. University of Chicago Press.

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, *5*(1).

Heide, L. (2009). *Punched-Card Systems and the Early Information Explosion, 1880–1945*. JHU Press.

Hellström, T. (2007). Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework. *Safety Science*, *45*(3), 415–430.

Hempell, T. (2006). *Computers and Productivity: How Firms Make a General Purpose Technology Work*. Springer Science & Business Media.

Herzog, M., & Schmid, J. (2016). Who Pays for Zero-Days? Balancing Long-Term Stability in Cyber Space Against Short-Term National Security Benefits. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives* (pp. 97–114). Routledge.

Heumann, S. (2017). Security in Cyberspace: The Limites of Nation-State Centric Approaches to Security in Global Networks. In J. D. Bindenagel, M. Herdegen, & K. Kaiser (Eds.), *International Security in the 21st Century: Germany's International Responsibility* (pp. 121–130). V&R unipress GmbH.

HEW Computer Security. (1977, November 14). *The Washington Post*. https://www.nexis.com/

Hicks, C. R. (1998). Places in the'Net: Experiencing Cyberspace. *Cultural Dynamics*, *10*(1), 49–70.

Hidalgo, C. (2015). *Why Information Grows: The Evolution of Order, from Atoms to Economies*. Penguin UK.

Hill, J. (2014). *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders* (ID 2430275). The Hague Institute for Global Justics, Conference on the Future of Cyber Governance. https://papers.ssrn.com/abstract=2430275

Hill, J. F., & Noyes, M. (2019). Rethinking Data, Geography, and Jurisdiction: A Common Framework for Harmonizing Global Data Flow Controls. In R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity Governance* (pp. 195–230). John Wiley & Sons.

Hirsch, C. (2018). Collateral Damage Outcomes are Prominent in Cyber Warfare, Despite Targeting. In L. Leenen (Ed.), *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (pp. 281–286). ACPIL.

Hoffmeyer, J. (2008). *A Legacy for Living Systems: Gregory Bateson as Precursor to Biosemiotics*. Springer Science & Business Media.

Hofkirchner, W. (2011). Does Computing Embrace Self-Organization? In G. D. Crnkovic & M. Burgin (Eds.), *Information and Computation: Essays on Scientific and Philosophical Understanding of Foundations of Information and Computation* (pp. 185–202). World Scientific.

Hofkirchner, W. (2012). Emergent Information. When a Difference Makes a Difference…. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *11*(1), 6–12.

Hofkirchner, W. (2013). *Emergent Information: A Unified Theory of Information Framework*. World Scientific.

Hoijtink, M., & Leese, M. (2019). How (not) to Talk About Technology: International Relations and the Question of Agency. In M. Hoijtink & M. Leese (Eds.), *Technology and Agency in International Relations* (pp. 1–24). Routledge.

Homeland Cybersecurity and DHS Enterprise Architecture Budget Hearing for Fiscal Year 2005: Hearing before the Subcommittee on Cybersecurity, Science, and Research and Development of the Select Committee on Homeland Security (Serial No. 108-44), House of Representatives, 108th Cong. (2004).

Humphreys, P. (2016). *Emergence*. Oxford University Press.

Huntley, W. L. (2016). *Strategic Implications of Offense and Defense in Cyberwar*. 5588–5595. https://doi.org/10.1109/HICSS.2016.691

Hurel, L. M., & Lobato, L. C. (2018). Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs. *Journal of Cyber Policy*, *3*(1), 61–76.

Iasiello, E. (2014). Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*, *7*(1), 54–67.

IBM Security. (2019). *Cost of a Data Breach Report* (p. 76). Ponemon Institute. https://www.ibm.com/downloads/cas/ZBZLY7KL

Illari, P., & Russo, F. (2016). Information and Causality. In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 235–248). Routledge.

Implications of Cyber Vulnerabilities on the Resilience and Security of the Electric Grid, Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, of the Committee on Homeland Security (Serial No. 110-117), U.S. House of Representatives, 110th Cong. (2008).

Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: Joint Hearing of the Subcommittee on Cybersecurity, Science, and Research and Development (Serial No. 108-23), House of Representatives, 108th Cong. (2003).

Industry Perspectives on the President's Cybersecurity Information-sharing Proposal, Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 114-7), U.S. House of Representatives, 114th Cong. (2015).

Industry Speaks on Cybersecurity: Hearing of the Subcommittee on Cybersecurity, Science and Research, and Development, before the Select Committee on Homeland Security (Serial No. 108-16), U.S. House of Representatives, 108th Cong. (2003).

Inoperable Computers and System Networks. (n.d.). Kaspersky. Retrieved 24 October 2019, from https://usa.kaspersky.com/resource-center/threats/computer-operations

Iranian Cyber Threat to the U.S. Homeland: Joint hearing before the Subcommittee on Counterterrorism and Intelligence, and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 112-86), U.S. House of Representatives, 112th Cong. (2012).

Jacobsen, K. L., & Monsees, L. (2019). Co-production: The Study of Productive Processes at the Level of Materiality and Discourse. In M. Hoijtink & M. Leese (Eds.), *Technology and Agency in International Relations* (pp. 24–41). Routledge.

Janich, P. (2018). *What Is Information?* University of Minnesota Press.

Jarvis, L., Macdonald, S., & Whiting, A. (2016). Analogy and Authority in Cyberterrorism Discourse: An Analysis of Global News Media Coverage. *Global Society*, *30*(4), 605–623.

Jasanoff, S. (Ed.). (2004). *States of Knowledge: The Co-production of Science and the Social Order*. Routledge.

Johnson, J. (2006). Can Complexity Help Us Better Understand Risk? *Risk Management*, *8*(4), 227–267.

Jordan, T. (1999). *Cyberpower: An Introduction to the Politics of Cyberspace.* Routledge.

Joseph, H. (1988). Computer Viruses Can Be Deadly. *EDPACS*, *15*(12), 1–6.

Junio, T. J. (2013). How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. *Journal of Strategic Studies*, *36*(1), 125–133.

Kafri, O., & Kafri, H. (2013). *Entropy: God's Dice Game*. Createspace Independent Pub.

Kak. (1983). Data Security in Computer Networks: Guest Editor's Introduction. *Computer*, *16*(2), 8–10.

Kallender, P., & Hughes, C. W. (2017). Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. *Journal of Strategic Studies*, *40*(1–2), 118–145.

Kallinikos, J. (2010). *Governing Through Technology: Information Artefacts and Social Practice*. Springer.

Kallinikos, J. (2012). Form, Function, and Matter: Crossing the Border of Materiality. In P. M. Leonardi, B. A. Nardi, & J. Kallinikos (Eds.), *Materiality and Organizing: Social Interaction in a Technological World* (pp. 67–87). OUP Oxford.

Kaltofen, C. (2018). With a Posthuman Touch: International Relations in Dialogue with the Posthuman—A Human Account. In E. Cudworth, S. Hobden, & E. Kavalski (Eds.), *Posthuman Dialogues in International Relations* (pp. 32–51). Routledge.

Kaplan, F. (2017). *Dark Territory: The Secret History of Cyber War*. Simon and Schuster.

Karnani, M., Pääkkönen, K., & Annila, A. (2009). The Physical Character of Information. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *465*(2107), 2155–2175.

Kaufmann, M. (2019). Who Connects the Dots? Agents and Agency in Predictive Policing. In M. Hoijtink & M. Leese (Eds.), *Technology and Agency in International Relations* (pp. 141–164). Routledge.

Keizer, G. (2010, October 1). *Why did Stuxnet worm spread?* Computerworld. https://www.computerworld.com/article/2516109/why-did-stuxnet-worm-spread-.html

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

Kello, L. (2017). *The Virtual Weapon and International Order* (1 edition). Yale University Press.

Kessler, O., & Daase, C. (2008). From Insecurity to Uncertainty: Risk and the Paradox of Security Politics. *Alternatives*, *33*(2), 211–232.

Keyes, R. W. (1977). Physical Uncertainty and Information. *IEEE Transactions on Computers*, *C–26*(10), 1017–1025.

Kim, D., & Solomon, M. G. (2016). *Fundamentals of Information Systems Security*. Jones & Bartlett Publishers.

King, R. (2012, November 8). Stuxnet Infected Chevron's IT Network. *The Wall Street Journal*. https://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/

Kisak, P. F. (Ed.). (2015). *Entropy and Negentropy: The End and the Beginning*. Createspace Independent Publishing Platform.

Kitchin, R. (2011). The Programmable City. *Environment and Planning B: Planning and Design*, *38*(6), 945–951.

Kitchin, R. (2018). Thinking Critically About and Researching Algorithms. In D. Beer (Ed.), *The Social Power of Algorithms* (pp. 14–29). Routledge.

Kitchin, R., & Dodge, M. (2005). Code and the Transduction of Space. *Annals of the Association of American Geographers*, *95*(1), 162–180.

Kitchin, R., & Dodge, M. (2011). *Code/space: Software and Everyday Life*. MIT Press.

Kittel, C. (2012). *Elementary Statistical Physics*. Courier Corporation.

Kittler, F. (1995). There is No Software. *Ctheory*, 10–18.

Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). Information Security Policy: An Organizational-Level Process Model. *Computers & Security*, *28*(7), 493–508.

Knight, W. (2017a, July 12). Biased Algorithms Are Everywhere, and No One Seems to Care. *MIT Technology Review*. https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/

Knight, W. (2017b, October 3). Google's Ai Chief Says Forget Elon Musk's Killer Robots, and Worry About Bias in Ai Systems Instead. *MIT Technology Review*. https://www.technologyreview.com/s/608986/forget-killer-robotsbias-is-the-real-ai-danger/

Konheim, A. (1981). Guest Editor's Prologue. *IEEE Transactions on Communications*, *29*(6), 761–761.

Krahmann, E. (2011). Beck and Beyond: Selling Security in the World Risk Society. *Review of International Studies*, *37*(01), 349–372.

Krämer, J., Wiewiorra, L., & Weinhardt, C. (2013). Net neutrality: A progress report. *Telecommunications Policy*, *37*(9), 794–813.

Kramer, L. (1977, November 18). Thieves, Swindlers Plague U.S. Business; Crimes Cost U.S. Business $30 Billion; Computer Bandits, Too. *The Washington Post*. https://www.nexis.com/

Kramer, L. (1978, June 22). Action Urged To Curb Crime By Computer. *The Washington Post*. https://www.nexis.com/

Krapp, P. (2011). *Noise Channels: Glitch and Error in Digital Culture*. University of Minnesota Press.

Krieger, K. (2016). Resilience and Risk Studies. In A. Burgess, J. O. Zinn, & A. Alemanno (Eds.), *Routledge Handbook of Risk Studies* (pp. 335–343). Routledge, Taylor & Francis Group.

Kroker, A. (2014). *Exits to the Posthuman Future*. John Wiley & Sons.

Landauer, R. (1991). Information is Physical. *Physics Today*, *44*(5), 23–29.

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, *8*(1), 100–115.

Landauer, R. (1999). Information Is a Physical Entity. *Physica A: Statistical Mechanics and Its Applications*, *263*(1–4), 63–67.

Landwehr, C. E. (1981). Formal Models for Computer Security. *ACM Computing Surveys (CSUR)*, *13*(3), 247–278.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. OUP Oxford.

Lavington, S. (2012). *Alan Turing and His Contemporaries: Building the World's First Computers*. BCS, The Chartered Institute.

Law, J. (2002). Objects and Spaces. *Theory, Culture & Society*, *19*(5–6), 91–105.

Law, J., & Singleton, V. (2005). Object Lessons. *Organization*, *12*(3), 331–355.

Lawson, S. (2012). Putting the "war" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States. *First Monday*, *17*(7). http://firstmonday.org/ojs/index.php/fm/article/view/3848

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics*, *10*(1), 86–103.

Lawson, S., Yeo, S. K., Yu, H., & Greene, E. (2016). The Cyber-Doom Effect: The Impact of Fear Appeals in the Us Cyber Security Debate. *Cyber Conflict (CyCon), 2016 8th International Conference On*, 65–80. http://ieeexplore.ieee.org/abstract/document/7529427/

Lazarevic, A., Kumar, V., & Srivastava, J. (2005). Intrusion Detection: A Survey. In V. Kumar, J. Srivastava, & A. Lazarevic (Eds.), *Managing Cyber Threats: Issues, Approaches, and Challenges* (pp. 19–78). Springer US.

Leach, T. (2020). *Machine Sensation: Anthropomorphism and 'Natural' Interaction with Nonhumans*. Open Humanities Press.

Lee, N. (2013). *Counterterrorism and Cybersecurity: Total Information Awareness*. Springer Science & Business Media.

Lee, R. M. (2016). Protecting Industrial Control Systems in Critical Infrastructure. In R. Harrison, T. Herr, & R. J. Danzig (Eds.), *Cyber Insecurity: Navigating the Perils of the Next Information Age* (pp. 31–46). Rowman & Littlefield Publishers.

Lee, R. M., & Rid, T. (2014). OMG Cyber!: Thirteen Reasons Why Hype Makes for Bad Policy. *The RUSI Journal*, *159*(5), 4–12.

Leonardi, P. M. (2010). Digital Materiality? How Artifacts Without Matter, Matter. *First Monday*, *15*(6–7). https://firstmonday.org/article/view/3036/2567

Leonardi, P. M. (2012). Materiality, Sociomateriality, and Socio-Technical Systems: What Do These Terms Mean? How Are They Different? In P. M. Leonardi, B. A. Nardi, & J. Kallinikos (Eds.), *Materiality and Organizing: Social Interaction in a Technological World* (pp. 25–48). OUP Oxford.

Leslie, S. (1993). *The Cold War and American Science: The Military-Industrial-Academic Complex at MIT and Stanford* (New Ed edition). Columbia University Press.

Lewes, G. H. (1875). *The Principles of Certitude. from the Known to the Unknown. Matter and Force. Force and Cause. the Absolute in the Correlations of Feeling and Motion. Appendix: Imaginary Geometry and the Truth of Axioms. Lagrange and Hegel: The Speculative Method. Action at a Distance*. Trübner & Company.

Li, D., & Du, Y. (2017). *Artificial Intelligence with Uncertainty*. CRC Press.

Li, J., Ou, X., & Rajagopalan, R. (2009). Uncertainty and Risk Management in Cyber Situational Awareness. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), *Cyber*

Situational Awareness: Issues and Research (pp. 51–70). Springer Science & Business Media.

Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND.

Libicki, M. C., Ablon, L., & Webb, T. (2015). *The Defender's Dilemma: Charting a Course Toward Cybersecurity*. Rand Corporation.

Limnell, J., & Rid, T. (2014). Is Cyberwar Real: Gauging the Threats. *Foreign Affairs*, *93*, 166.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404.

Lloyd, S. (2000). Ultimate Physical Limits to Computation. *Nature*, *406*(6799), 1047–1054.

Lloyd, S. (2006). *Programming the Universe: A Quantum Computer Scientist Takes on the Cosmos*. Knopf Doubleday Publishing Group.

Lloyd, S. (2010). The Computational Universe. In P. Davies & N. H. Gregersen (Eds.), *Information and the Nature of Reality: From Physics to Metaphysics* (pp. 92–103). Cambridge University Press.

Loader, B. D. (Ed.). (1997). *The Governance of Cyberspace: Politics, Technology and Global Restructuring*. Routledge.

Lobato, L. C., & Kenkel, K. M. (2015). Discourses of Cyberspace Securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional*, *58*(2), 23–43.

Lombardi, O. (2016). Mathematical Theory of Information (Shannon). In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 30–36). Routledge.

Lombardi, O., & López, C. (2017). Information, Communication, and Manipulability. In O. Lombardi, S. Fortin, F. Holik, & C. López (Eds.), *What is Quantum Information?* (pp. 53–76). Cambridge University Press.

López, C. A., & Lombardi, O. I. (2019). No Communication Without Manipulation: A Causal-Deflationary View of Information. *Studies in History and Philosophy of Science Part A*, *73*, 34–43.

Lundborg, T., & Vaughan-Williams, N. (2015). New Materialisms, Discourse Analysis, and International Relations: A Radical Intertextual Approach. *Review of International Studies*, *41*(1), 3–25.

Lutz, E., & Ciliberto, S. (2015). From Maxwell's Demon to Landauer's Eraser. *Physics Today*, *68*(9).

Lynn, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, *89*(5), 97–108.

M. Berry, D. (Ed.). (2012). *Life in Code and Software: Mediated Life in a Complex Computational Ecology*. Open Humanities Press. http://www.livingbooksaboutlife.org/books/Life_in_Code_and_Software

Mačák, K. (2017). From Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers. *Leiden Journal of International Law*, *30*(4), 877–899.

MacKenzie, A. (2003). The Problem of Computer Code: Leviathan or Common Power. *Institute for Cultural Research, Lancaster University*.

MacKenzie, A. (2006). *Cutting Code: Software and Sociality*. Peter Lang Inc., International Academic Publishers.

Mahon, P. (2017). *Posthumanism: A Guide for the Perplexed*. Bloomsbury Academic.

Malapi-Nelson, A. (2017). *The Nature of the Machine and the Collapse of Cybernetics: A Transhumanist Lesson for Emerging Technologies*. Springer.

Malaspina, C. (2018). *An Epistemology of Noise*. Bloomsbury Publishing.

Marczyk, J., & Deshpande, B. (2010). Measuring and Tracking Complexity in Science. In A. A. Minai, D. Braha, & Y. Bar-Yam (Eds.), *Unifying Themes in Complex Systems: Vol VI: Proceedings of the Sixth International Conference on Complex Systems* (pp. 27–33). Springer Science & Business Media.

Marion, N., & Hill, J. B. (2016). *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. Praeger.

Marson, S. M. (1997). A Selective History of Internet Technology and Social Work. *Computers in Human Services*, *14*(2), 35–49.

Mason, M. (2009). *Complexity Theory and the Philosophy of Education*. John Wiley & Sons.

Masur, P. K. (2018). *Situational Privacy and Self-Disclosure: Communication Processes in Online Environments*. Springer.

Mazanec, B. M., & Thayer, B. A. (2015). *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*. Palgrave Macmillan.

Mc Cue, L. J. (1983, August 30). Computer Crime Fault of Security. *The American Banker*. https://www.nexis.com/

McDonald, M., & Mitchell, A. (2017). Introduction: Posthuman International Relations. In C. Eroukhmanoff & M. Harker (Eds.), *Reflections on the Posthuman in International Relations: The Anthropocene, Security and Ecology*. E-International Relations.

McGraw, G. (2013). Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, *36*(1), 109–119.

McGuffin, C., & Mitchell, P. (2014). On Domains: Cyber and the Practice of Warfare. *International Journal: Canada's Journal of Global Policy Analysis*, *69*(3), 394–412.

McHarris, Wm. C. (2015). It from Bit from It from BIt...Nature and Nonlinear Logic. In A. Aguirre, B. Foster, & Z. Merali (Eds.), *It From Bit or Bit From It?: On Physics and Information* (pp. 225–234). Springer.

McMullin, E. (2010). From Matter to Materialism ... And (almost) Back. In P. Davies & N. H. Gregersen (Eds.), *Information and the Nature of Reality: From Physics to Metaphysics* (pp. 13–37). Cambridge University Press.

Meijer, H., Hoepman, J.-H., Jacobs, B., & Poll, E. (2007). Computer Security Through Correctness and Transparency. In K. M. M. de Leeuw & J. Bergstra (Eds.), *The History of Information Security* (pp. 637–653). Elsevier Science B.V.

Miccoli, A. (2017, September 27). Posthuman Suffering. *Critical Posthumanism Network*. http://criticalposthumanism.net/posthuman-suffering/

Mihalache, A. (2002). The Cyber Space-Time Continuum: Meaning and Metaphor. *The Information Society*, *18*(4), 293–301.

Miller, D. (Ed.). (2005). *Materiality*. Duke University Press.

Milne, P. (2016). Probability and Information. In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 15–22). Routledge.

Misra, S., & Goswami, S. (2017). *Network Routing: Fundamentals, Applications, and Emerging Technologies*. John Wiley & Sons.

Mitchell, A. (2014a). Only human? A worldly approach to security. *Security Dialogue*, *45*(1), 5–21.

Mitchell, A. (2014b, July 24). Dispatches from the Robot Wars; Or, What is Posthuman Security? *The Disorder of Things*. https://thedisorderofthings.com/2014/07/24/dispatches-from-the-robot-wars-or-what-is-posthuman-security/

Mitnick, K. (2019). *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*. Little, Brown.

Mody, S. S. (2001). National Cyberspace Regulation: Unbundling the Concept of Jurisdiction Note. *Stanford Journal of International Law*, *37*, 365–390.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, *58*(1), 7–38.

Morçöl, G. (2013). *A Complexity Theory for Public Policy*. Routledge.

More Computer Security Needed. (1984, April 11). *The Associated Press*. https://www.nexis.com/

More Security, Less Waste: What Makes Sense for our Federal Cyber Defense, Hearing before the Federal Financial Management, Government Information, Federal Services, and International Security Subcommittee, of the Committee on Homeland Security and Governmental Affairs (S. Hrg. 111-662), U.S. Senate, 111th Cong. (2009)

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press.

Muller, L. P. N. (2016). How to Govern Cyber Security? The Limits of the Multi-Stakeholder Aproach and the Need to Rethink Public-Private Cooperation. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives* (pp. 115–126). Routledge.

Murphy, B. M. (2002). A Critical History of the Internet. In G. Elmer (Ed.), *Critical Perspectives on the Internet* (pp. 27–48). Rowman & Littlefield.

Ness, H. C. V. (2012). *Understanding Thermodynamics*. Courier Corporation.

NHS Trusts 'at Fault' Over Cyber-Attack. (2017, October 27). *BBC*. https://www.bbc.com/news/technology-41753022

Nicolis, G. (2012). *Foundations of Complex Systems: Emergence, Information and Prediction*. World Scientific.

Nissenbaum, H. (1997). Accountability in a Computarized Society. In B. Friedman (Ed.), *Human Values and the Design of Computer Technology* (pp. 41–64). Cambridge University Press.

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

Norman, D. (2009). *The Design of Future Things*. Hachette UK.

Norman, D. A. (1997). How Might People Interact with Agents. In J. M. Bradshaw (Ed.), *Software Agents* (pp. 49–56). AAAI Press.

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44–71.

Oberman, M. R. (1983). *Communication Security in Remote Controlled Computer Systems*. 219–227.

O'Malley, P. (2012). *Risk, Uncertainty and Government*. Routledge-Cavendish.

Orman, H. (2003). The Morris Worm: A Fifteen-Year Perspective. *IEEE Security Privacy*, *1*(5), 35–43.

Ormes, E., & Herr, T. (2016). Understanding Information Assurance. In R. Harrison & T. Herr (Eds.), *Cyber Insecurity: Navigating the Perils of the Next Information Age* (pp. 3–18). Rowman & Littlefield Publishers.

Oversight of Executive Order 13636 and Development of the Cybersecurity Framework: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 113-27), House of Representatives, 113th Cong. (2013)

Oversight of the Cybersecurity Act of 2015, Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 114-76), U.S. House of Representatives, 114th Cong. (2016).

Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk, Hearing of the Subcommittee on Cybersecurity, Science, and Research, and Development, before the Select Committee on Homeland Security (Serial No. 108-13), U.S. House of Representatives, 108th Cong. (2003)

Overview of the Cyber Problem: A Nation Dependent and Dealing with Risk: Hearing of the Subcommittee on Cybersecurity, Science, and Research, and Development, Before the Select Committee on Homeland Security (Serial No. 108-13), U.S. House of Representatives, 108th Cong. (2003).

Palma, F. (1980, October 14). Need for Computer Security Specialists on the Rise. *The American Banker*. https://www.nexis.com/

Panagiotis, K. (2006). *Digital Crime and Forensic Science in Cyberspace*. Idea Group Inc (IGI).

Panek, C. (2019). *Networking Fundamentals*. John Wiley & Sons.

Parikka, J. (2007). *Digital Contagions: A Media Archaeology of Computer Viruses*. Peter Lang.

Parikka, J. (2017). *Digital Contagions: A Media Archaeology of Computer Viruses*. Peter Lang.

Parks, L., & Starosielski, N. (2015). *Signal Traffic: Critical Studies of Media Infrastructures*. University of Illinois Press.

Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. *European Journal of International Security*, *5*(2), 233–254.

Pepperell, R. (1995). *The Post-Human Condition*. Intellect Books.

Petersen, K. L. (2016). Risk and Security. In M. Dunn Cavelty & T. Balzacq (Eds.), *Routledge Handbook of Security Studies* (pp. 117–125). Routledge, Taylor & Francis Group.

Pettersen, K. (2016). Understanding Uncertainty: Thinking Through in Relation to High-Risk Technologies. In A. Burgess, A. Alemanno, & J. O. Zinn (Eds.), *Routledge Handbook of Risk Studies* (pp. 39–48). Routledge, Taylor & Francis Group.

Pias, C. (2005). Analog, Digital, and the Cybernetic Illusion. *Kybernetes*.

Pias, C., & Foerster, H. V. (2016). *Cybernetics: The Macy Conferences 1946-1953*. University of Chicago Press.

Piccinini, G., & Scarantino, A. (2016). Computation and Information. In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 23–29). Routledge.

Pickard, V., & Berman, D. E. (2019). *After Net Neutrality: A New Deal for the Digital Age*. Yale University Press.

Ponemon Institute. (2016). *New Ponemon Study on Malware Detection and Prevention Released*. https://www.ponemon.org/blog/new-ponemon-study-on-malware-detection-prevention-released

Ponemon Institute. (2019). *Costs and Consequences of Gaps in Vulnerability Response*. ServiceNow. https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf

Prigogine, I., & Stengers, I. (2018). *Order Out of Chaos: Man's New Dialogue with Nature* (Reprint edition). Verso.

Primiero, G. (2016). Information in the Philosophy of Computer Science. In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 90–106). Routledge.

Promoting and Incentivizing Cybersecurity Best Practices: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No. 114-29), U.S. House of Representatives, 114th Cong. (2015).

Protecting America From Cyber Attacks: The Importance of Information Sharing: Hearing before the Committee on Homeland Security and Governmental Affairs (Serial No. 114-412), U.S. Senate, 114th Congress. (2015).

Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century: Hearing before the Committee on Homeland Security and Governmental Affairs (Serial No. 111-1103), U.S. Senate, 111th Cong. (2010).

Protecting Cyberspace: Assessing the White House Proposal, Hearing before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 112-221), U.S. Senate, 112th Cong. (2011).

Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports at Risk for a Cyber Attack? Hearing before the Subcommittee on Border and Maritime Security, of the Committee on Homeland Security (Serial No. 114-35), U.S. House of Representatives, 114th Cong. (2015).

Rammert, W. (2012). Distributed Agency and Advanced Technology Or: How to Analyze Constellations of Collective Inter-Agency. In J.-H. Passoth, B. Peuker, & M. Schillmeier (Eds.), *Agency without Actors?: New Approaches to Collective Action*. Routledge.

Randell, B. (1982). Colossus: Godfather of the Computer. In B. Randell (Ed.), *The Origins of Digital Computers* (pp. 349–354). Springer, Berlin, Heidelberg.

Rasmussen, M. V. (2001). Reflexive Security: NATO and International Risk Society. *Millennium*, *30*(2), 285–309.

Rasmussen, M. V. (2004). It Sounds Like a Riddle': Security Studies, the War on Terror and Risk. *Millennium-Journal of International Studies*, *33*(2), 381–395.

Rattray, G. J. (2009). An Enviornmental Approach to Understanding Cyberpower. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 253–274). Potomac Books, Inc.

Ratzan, L. (2004). *Understanding Information Systems: What They Do and why We Need Them*. American Library Association.

Reddy, Y. (1979). Data-Security in Computer-Networks. *Electronics Information & Planning*, *6*(12), 937–950.

Reisman, D. (2017, May 22). *Where Is Your Data, Really?: The Technical Case Against Data Localization*. Lawfare. https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization

Reuvid, J. (2006). *The Secure Online Business Handbook: A Practical Guide to Risk Management and Business Continuity*. Kogan Page Publishers.

Reviewing the Federal Cybersecurity Mission: Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, of the Committee on Homeland Security (Serial No.111-5), U.S. House of Representatives, 111th Cong. (2009)

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32.

Rid, T. (2013a). *Cyber War Will Not Take Place*. Oxford University Press.

Rid, T. (2013b). More Attacks, Less Violence. *Journal of Strategic Studies*, *36*(1), 139–142.

Rid, T. (2016). *Rise of the Machines: A Cybernetic History*. W W NORTON & CO INC.

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37.

Rifkin, J., & Howard, T. (1989). *Entropy: Into the Greenhouse World*. Bantam Books.

Rivera, J., & Hare, F. (2014). The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures. *2014 6th International Conference on Cyber Conflict (CyCon 2014)*, 99–116.

Robertson, J., & Riley, M. (2018, October 4). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies—Bloomberg. *Bloomberg Businessweek*. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Roe, P. (2012). Is Securitization a 'Negative' Concept? Revisiting the Normative Debate over Normal versus Extraordinary Politics. *Security Dialogue*, *43*(3), 249–266.

Roe, Paul. (2008). Actor, Audience (s) and Emergency Measures: Securitization and the UK's Decision to Invade Iraq. *Security Dialogue*, *39*(6), 615–635.

Rose, J., & Truex, D. (2000). Machine Agency as Perceived Autonomy: An Action Perspective. In R. Baskerville, J. Stage, & J. I. DeGross (Eds.), *Organizational and Social Perspectives on Information Technology: IFIP TC8 WG8.2 International Working Conference on the Social and Organizational Perspective on Research and Practice in Information Technology June 9–11, 2000, Aalborg, Denmark* (pp. 371–388). Springer US.

Rosenberg, M., & Nixon, R. (2017, September 13). Kaspersky Lab Antivirus Software Is Ordered Off U.S. Government Computers. *The New York Times*. https://www.nytimes.com/2017/09/13/us/politics/kaspersky-lab-antivirus-federal-government.html

Rowe, N. C. (2017). Ethics and Policies for Cyber Operations. In L. Glorioso & M. Taddeo (Eds.), *Challenges of Civilian Distinction in Cyberwarfare* (pp. 33–48). Springer, Cham.

Rushe, D., Ackerman, S., & Ball, J. (2013, October 31). Reports That Nsa Taps into Google and Yahoo Data Hubs Infuriate Tech Giants. *The Guardian*. http://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links

Russell, A., & Wang, H. (2002). How to Fool an Unbounded Adversary with a Short Key. In L. R. Knudsen (Ed.), *Advances in Cryptology—EUROCRYPT 2002* (pp. 133–148). Springer.

Russell, D., & Gangemi, G. T. (1991). *Computer Security Basics*. O'Reilly Media, Inc.

Rutledge, L. S., & Hoffman, L. J. (1986). A Survey of Issues in Computer Network Security. *Computers & Security*, *5*(4), 296–308.

Ruttan, V. W. (2006). *Is War Necessary for Economic Growth?* Oxford University Press.

Ryan, J. (2010). *A History of the Internet and the Digital Future*. Reaktion Books.

Sabbah, C. (2018). Pressing Pause: A New Approach for International Cybersecurity Norm Development. In T. Minárik, R. Jakschis, & L. Lindström (Eds.), *CyCon X: Maximising Effects* (p. 20).

Salter, M. B. (2008a). Imagining Numbers: Risk, Quantification, and Aviation Security. *Security Dialogue*, *39*(2–3), 243–266.

Salter, M. B. (2008b). Securitization and Desecuritization: A Dramaturgical Analysis of the Canadian Air Transport Security Authority. *Journal of International Relations and Development*, *11*(4), 321–349.

Salter, M. B. (2015). Introduction: Circuits and Motions. In M. B. Salter (Ed.), *Making Things International 1: Circuits and Motion*. U of Minnesota Press.

Salter, M. B. (2019). Security Actor-Network Theory: Revitalizing Securitization Theory with Bruno Latour. *Polity*, *51*(2), 349–364.

Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2016). Automation, Algorithms, and Politics: When the Algorithm Itself is a Racist: Diagnosing Ethical Harm in the Basic Components of Software. *International Journal of Communication*, *10*(0), 19.

Sapolsky, H. M. (1990). *Science and the Navy: The History of the Office of Naval Research*. Princeton University Press. http://www.jstor.org/stable/j.ctt7zvnbn

Scarfone, K., & Mell, P. (2010). Intrusion Detection and Prevention Systems. In P. Stavroulakis & M. Stamp (Eds.), *Handbook of Information and Communication Security* (pp. 177–192). Springer Science & Business Media.

Schandorf, M., & Karatzogianni, A. (2018). Agency in a Posthuman IR: Solving the Problem of Technosocially Mediated Agency. In E. Cudworth, S. Hobden, & E. Kavalski (Eds.), *Posthuman Dialogues in International Relations* (pp. 89–108). Routledge.

Schutte, S. (2012). Cooperation Beats Deterrence in Cyberwar. *Peace Economics, Peace Science and Public Policy*, *18*(3).

Schwabach, A. (2014). *Internet and the Law: Technology, Society, and Compromises*. ABC-CLIO.

Schwarz, E. (2017). Hybridity and Humility: What of the Human in Posthuman Security? In C. Eroukhmanoff & M. Harker (Eds.), *Reflections on the Posthuman in International Relations: The Anthropocene, Security and Ecology* (pp. 29–28). E-International Relations.

Scott, S. V. (2012). The Securitization of Climate Change in World Politics: How Close Have We Come and Would Full Securitization Enhance the Efficacy of Global Climate Change Policy? *Review of European Community and International Environmental Law*, *21*(3), 220–230.

Securing America's Future: The Cybersecurity Act of 2012, Hearing before the Committee on Homeland Security and Governmental Affairs, U.S. Senate (S. Hrg. 112-524), Cong. 112th, (2012).

Securing Critical Infrastructure in the Age of Stuxnet: Hearing before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 111-103), U.S. Senate, 111th Cong. (2010).

Securing Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges, Hearing before the Federal Financial Management, Government Information, and International Security Subcommittee, of the Committee on Homeland Security and Governmental Affairs, U.S. Senate (S. Hrg. 109-402), Cong. 109th (2005).

Securing the Modern Electric Grid from Physical and Cyber Attacks, Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and technology (Serial No. 111-30), U.S. House of representatives, 111th Cong. (2009).

Shackelford, S. J. (2014). *Managing Cyber Attacks in International Law, Business, and Relations*. Cambridge University Press.

Shah, R. C., & Kesan, J. P. (2007). The Privatization of the Internet's Backbone Network. *Journal of Broadcasting & Electronic Media*, *51*(1), 93–109.

Shannon, C. E. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal*, *27*, 379–423.

Shaw, I., & Akhter, M. (2014). The Dronification of State Violence. *Critical Asian Studies*, *46*(2), 211–234.

Siegel, P. (2008). *Communication Law in America*. paul siegel.

Siegfried, T. (2000). *The Bit and the Pendulum: From Quantum Computing to M Theory--The New Physics of Information*. WILEY.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Skoudis, E., & Zeltser, L. (2004). *Malware: Fighting Malicious Code*. Prentice Hall Professional.

Slack, C. (2016). Wired yet Disconnected: The Governance of International Cyber Relations. *Global Policy*, *7*(1), 69–78.

Sloman, A. (2011). What's Information, for an Organism or Intelligent Machine? How Can a Machine or Organism Mean? In G. D. Crnkovic (Ed.), *Information and Computation: Essays on Scientific and Philosophical Understanding of Foundations of Information and Computation*. World Scientific.

Smithson, M. (2012). The Many Faces and Masks of Uncertainty. In G. Bammer & M. Smithson (Eds.), *Uncertainty and Risk: Multidisciplinary Perspectives* (pp. 13–26). Routledge.

Solomon, T. (2015). Embodiment, Emotions, and Materialism in International Relations. In L. Åhäll & T. Gregory (Eds.), *Emotions, Politics and War* (pp. 58–70). Routledge.

Soni, J., & Goodman, R. (2017). *A Mind at Play: How Claude Shannon Invented the Information Age*. Simon and Schuster.

Sonne, J. C. (1985). Entropic Communication in Families with Adolescents. *International Journal of Family Therapy*, *7*(3), 178–191.

Standish, R. K. (2001). On Complexity and Emergence. *ArXiv:Nlin/0101006*, *9*. http://arxiv.org/abs/nlin/0101006

Starosielski, N. (2015a). *The Undersea Network*. Duke University Press.

Starosielski, N. (2015b). Fixed Flow: Undersea Cables as Media Infrastructures. In L. Parks & N. Starosielski (Eds.), *Signal Traffic: Critical Studies of Media Infrastructures* (pp. 53–70). University of Illinois Press.

Steinhart, E. (1998). Digital Metaphysics. In T. W. Bynum & J. H. Moor (Eds.), *The Digital Phoenix: How Computers are Changing Philosophy* (pp. 117–134). Blackwell Publishers, Ltd.

Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*, *33*(1), 148-170.

Stevens, T. (2012). *Information Matters: Informational Conflict and the New Materialism*. Paper for presentation at Millennium Annual Conference, 'Materialism and World Politics', 20-21 October 2012, London School of Economics. Available at http://dx.doi.org/10.2139/ssrn.2146565

Stevens, T. (2015). *Cyber Security and the Politics of Time* (1 edition). Cambridge University Press.

Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance, 6*(2), 1-4.

Stevens, T. (2020). Knowledge in the Grey Zone: AI and Cybersecurity. *Digital War*. https://doi.org/10.1057/s42984-020-00007-w

Stillman, R. B., & Defiore, C. R. (1980). Computer Security and Networking Protocols: Technical Issues in Military Data Communications Networks. *IEEE Transactions on Communications*, *28*(9), 1472–1477.

Stockdale, L. P. D. (2013). Imagined Futures and Exceptional Presents: A Conceptual Critique of 'pre-Emptive Security'. *Global Change, Peace & Security*, *25*(2), 141–157.

Stohl, M. (2007). Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games? *Crime, Law and Social Change*, *46*(4–5), 223–238.

Stone, J. (2013). Cyber War Will Take Place! *Journal of Strategic Studies*, *36*(1), 101–108.

Stonier, T. (1991). Towards a new theory of information. *Journal of Information Science*, *17*(5), 257–263.

Stonier, T. (2012). *Information and the Internal Structure of the Universe: An Exploration into Information Physics*. Springer Science & Business Media.

Straube, T. (2017). Situating Data Infrastrcutures. In R. Kitchin, T. P. Lauriault, & G. McArdle (Eds.), *Data and the City*. Routledge.

Striking the Rights Balance: Protecting our Nation's Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties: Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security (Serial No.113-13), U.S. House of Representatives, 113th Cong. (2013).

Stritzel, H. (2011). Security, the Translation. *Security Dialogue*, *42*(4–5), 343–355.

Stritzel, H., & Chang, S. C. (2015). Securitization and Counter-Securitization in Afghanistan. *Security Dialogue*, *46*(6), 548–567.

Suber, P. (1988). What is Software? *Journal of Speculative Philosophy*, *2*(2), 89–119.

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword. *Nature Machine Intelligence*, *1*(12), 557–560.

Taureck, R. (2006). Securitization Theory and Securitization Studies. *Journal of International Relations and Development*, *9*(1), 53–61.

The Comptroller General of the United States. (1976a). *Computer-Related Crimes in Federal Programs: Report to the Congress*. U.S. General Accounting Office. http://hdl.handle.net/2027/pur1.32754062639160

The Comptroller General of the United States. (1976b). *Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities, Multiagency :report to the Congress*. U.S. General Accounting Office. http://hdl.handle.net/2027/uiug.30112027352290

The Cyber Initiative, Hearing before the Committee on Homeland Security (Serial No. 110-98), U.S. House of Representatives, 110th Cong. (2008).

The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid, Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, of the Committee on Homeland Security (Serial No. 110-78), U.S. House of Representatives, 110th Cong. (2007).

The Cybersecurity Partnership between the Private Sector and Our Government: Protecting our National and Economic Security, Joint Hearing before the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs, (S. Hrg. 113-295), U.S. Senate, 113th Cong. (2013).

The Department of Defense. (2006). *The National Military Strategy fo Cyberspace Operations*. https://www.hsdl.org/?view&did=35693

The Department of Defense. (2011). *Department of Defense Strategy for Operating in Cyberspace*. United States Government. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-050.pdf

The Department of Defense. (2015). *The Department of Defense Cyber Strategy*. http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf

The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure, *Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security* (Serial No. 112-19), U.S. House of Representatives, 112th Cong. (2011).

The Future of Cyber and Telecommunications Security at DHS, *Hearing before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, of the Committee on Homeland Security* (Serial No. 109-102), U.S. House of Representatives, 109th Cong. (2006).

The Role of Cyber Insurance in Risk Management, Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, *of the Committee on Homeland Security* (Serial No. 114-61), U.S. House of Representatives, 114th Cong. (2016).

The White House. (2003). *The National Strategy to Secure Cyberspace*. United States Government. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

The White House. (2013). *Presidential Policy Directive—Critical Infrastructure Security and Resilience*. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Thrift, N., & French, S. (2002). The Automatic Production of Space. *Transactions of the Institute of British Geographers*, *27*(3), 309–335.

Timpson, C. (2016). The Philosophy of Quantum Information. In L. Floridi (Ed.), *The Routledge Handbook of Philosophy of Information* (pp. 219–234). Routledge.

Timpson, C. G. (2013). *Quantum Information Theory and the Foundations of Quantum Mechanics*. OUP Oxford.

Top 5 Most Notorious Cyberattacks. (2018, November 6). Kaspersky. https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/

Trombetta, M. J. (2008). Environmental Security and Climate Change: Analysing the Discourse. *Cambridge Review of International Affairs*, *21*(4), 585–602.

Tse, P. (2013). *The Neural Basis of Free Will: Criterial Causation*. MIT Press.

Turing, A. M. (1956). Can a Machine Think. *The World of Mathermatics*, *4*, 2099–2123.

Ullman, E. (1997). *Close to the Machine: Technophilia and Its Discontents*. City Lights Books.

Under Attack: Federal Cybersecurity and the OPM Data Breach, Hearing before the Committee on Homeland Security and Governmental Affairs (S. Hrg. 114-449), U.S. Senate, 114th Cong. (2015).

Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.

Valkenburg, G., & van der Ploeg, I. (2015). Materialities Between Security and Privacy: A Constructivist Account of Airport Security Scanners. *Security Dialogue*, *46*(4), 326–344.

van der Hoek, W., & Wooldridge, M. (2003). Towards a Logic of Rational Agency. *Logic Journal of the IGPL*, *11*(2), 135–159.

Vedral, V. (2018). *Decoding Reality: The Universe as Quantum Information*. Oxford University Press.

Vee, A. (2017). *Coding Literacy: How Computer Programming is Changing Writing*. MIT Press.

Von Solms, R., & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, *38*, 97–102.

Vonderau, P., & Holt, J. (2015). 'Where the Internet Lives': Data Centers as Cloud Infrastructure. In L. Parks & N. Starosielski (Eds.), *Signal Traffic: Critical Studies of Media Infrastructures* (pp. 71–93). University of Illinois Press.

Vuori, J., & Saugmann, R. (Eds.). (2018). *Visual Security Studies: Sights and Spectacles of Insecurity and War*. Routledge.

Wæver, O. (1988). *Security, the Speech Act*.

Wæver, O. (1993). *Identity, Migration and the New Security Agenda in Europe*. Pinter.

Wæver, O. (1995). Securitization and Desecuritization. In R. D. Lipschutz (Ed.), *On Security*. Columbia University Press. http://s3.amazonaws.com/s3.libraryofsocialscience.com/pdf/Lipschutz--On_Security-3--Waever-Securitization.pdf

Wæver, O. (2009). What Exactly Makes a Continuous Existential Threat Existential—And How Is It Discontinued? In O. Barak & G. Sheffer (Eds.), *Existential Threats and Civil-security Relations* (pp. 19–36). Rowman & Littlefield.

Wæver, O., Buzan, B., Kelstrup, M., & Lemaitre, P. (Eds.). (1993). *Identity, Migration and the New Security Agenda in Europe*. Palgrave Macmillan.

Waldrop, M. M. (1993). *Complexity: The Emerging Science at the Edge of Order and Chaos*. Simon and Schuster.

Walker, S. I. (2014). Top-Down Causation and the Rise of Information in the Emergence of Life. *Information*, *5*(3), 424–439.

Watson, I. (2012). *The Universal Machine: From the Dawn of Computing to Digital Consciousness*. Springer Science & Business Media.

Wassenaar: Cybersecurity and Export Controls: Joint hearing before the Subcommittee on Information Technology, of the Committee on Oversight and Government Reform and the Subcommittee on Cybersecurity Infrastructure Protection, and Security Technologies, *of the Committee on Homeland Security* (Serial No. 114-102, 114-49), U.S. House of Representatives., 114th Cong. (2016).

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism*, *28*(2), 129–149.

Weinstein, D. (2014). Snowden and U.S. Cyber Power. *Georgetown Journal of International Affairs*, 4–11.

Wheeler, J. A. (1992). Recent Thinking about the Nature of the Physical World: It from Bita. *Annals of the New York Academy of Sciences*, *655*(1), 349–364.

Wicken, J. S. (1987). Entropy and Information: Suggestions for Common Language. *Philosophy of Science*, *54*(2), 176–193.

Wiener, N. (1948). *Cybernetics: Or, Control and Communication in the Animal and the Machine*. Wiley & Sons.

Wiener, N. (1988). *The Human Use Of Human Beings: Cybernetics And Society*. Hachette UK.

Wilkinson, C. (2011). The Limits of Spoken Words: From Meta-narratives to Experiences of Security. In T. Balzacq (Ed.), *Securitization Theory: How Security Problems Emerge and Dissolve* (pp. 94–115). Routledge.

Williams, M. C. (2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly*, *47*(4), 511–531.

Williams, M. J. (2008). (In)Security Studies, Reflexive Modernization and the Risk Society. *Cooperation and Conflict*, *43*(1), 57–79.

Willson, M. (2018). Algorithms (and the) everyday. In D. Beer (Ed.), *The Social Power of Algorithms* (pp. 137–150). Routledge.

Winkler, I., & Gomes, A. T. (2016). *Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies*. Syngress.

Winkler, S., & Danner, L. (1974). Data Security in the Computer Communication Environment. *Computer*, *7*(2), 23–31.

Wolfe, A. J. (2013). *Competing with the Soviets: Science, Technology, and the State in Cold War America*. Johns Hopkins University Press.

Wolfe, C. (2010). *What is Posthumanism?* U of Minnesota Press.

Wooldridge, M., & Jennings, N. R. (1995). Intelligent Agents: Theory and Practice. *The Knowledge Engineering Review*, *10*(2), 115–152.

Yost, J. R. (2007). A History of Computer Security Standards. In K. M. M. de Leeuw & J. Bergstra (Eds.), *The History of Information Security: A Comprehensive Handbook* (pp. 595–621). Elsevier Science.

Zeilinger, A. (2005). *What do you believe is true even though you cannot prove it?* Edge. https://www.edge.org/response-detail/10380

Zhu, J., & Knoespe. (2007). Continuous Materiality: Through a Hierarchy of Computational Codes. *Proceedings of the Seventh International Digital Arts and Culture Conference*, 188–198. http://eleven.fibreculturejournal.org/fcj-076-continuous-materiality-through-a-hierarchy-of-computational-codes/