Computers & Security 116 (2022) 102674

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

TC 11 Briefing Papers

Cyber security and the Leviathan

Joseph Da Silva

Royal Holloway, University of London, Egham Hill, Egham TW20 0EX, United Kingdom

ARTICLE INFO

Article history:
Received 7 November 2021
Revised 2 February 2022
Accepted 24 February 2022
Available online 2 March 2022

Keywords:
Qualitative research
Cyber security practice
Security studies
Human aspects
Organisational studies
Information security management
Sociological perspectives
Political perspectives
Thomas Hobbes

ABSTRACT

Dedicated cyber-security functions are common in commercial businesses, who are confronted by evolving and pervasive threats of data breaches and other perilous security events. Such businesses are enmeshed with the wider societies in which they operate. Using data gathered from in-depth, semi-structured interviews with 15 Chief Information Security Officers, as well as six senior organisational leaders, we show that the work of political philosopher Thomas Hobbes, particularly Leviathan, offers a useful lens through which to understand the context of these functions and of cyber security in Western society. Our findings indicate that cyber security within these businesses demonstrates a number of Hobbesian features that are further implicated in, and provide significant benefits to, the wider Leviathanesque state. These include the normalisation of intrusive controls, such as surveillance, and the stimulation of consumption. We conclude by suggesting implications for cyber-security practitioners, in particular, the reflexivity that these perspectives offer, as well as for businesses and other researchers.

© 2022 The Author. Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/)

1. Introduction

Cyber-security practice is increasingly recognised as more than a technological exercise. The application of sociological and political viewpoints to such practice, particularly in organisations, is becoming more and more common, e.g., Burdon and Coles-Kemp (2019); Stevens (2016). In this paper, we build on these foundations by applying a number of lenses based on the work of Thomas Hobbes to a study of 15 Chief Information Security Officers (CISOs) and six senior organisational stakeholders representing 18 UK-based, but predominantly multinational, businesses. This work contributes to and extends cyber security scholarship by considering cyber security within business as a component of wider societal power structures. First, this research indicates that cyber security functions within businesses serve the interests of the state Leviathan. This positions those functions as indirect and possibly unwitting agents of the state, and cyber security itself as beneficial to the state and associated hegemonies. Second, it shows that cyber security functions within businesses operate as a Hobbesian form of control within the micro-societies of businesses, who are themselves mini-Leviathans. Third, it provides a novel sociological lens with which to explore cyber security within businesses and wider societies. We consider the key contribution of this research as being to provide a novel viewpoint on cyber-security practice that enables greater reflexivity and reflection for practitioners, as well as offering a pathway for future research.

Our research question, part of a wider study, was 'what is the purpose of a CISO in a commercial organisation?', and, through our analysis, we applied a range of different sociological concepts in order to derive meaning from our data. One of those lenses, motivated by multiple resonances within the data, was that of Hobbes. Hobbes' *Leviathan*, in particular, has had a significant influence on Western political philosophy (Arendt, 2017 (1951; Stevens, 2016) and it is from this text that we develop our analytical lenses, in a similar vein to that followed by Burdon and Coles-Kemp (2019) who applied Smith (2005) as a lens to their study of cyber-security practitioners. Hobbes' thesis, expounded in *Leviathan* and other works that follow a consistent thread, e.g., Hobbes (1839, 2009 (1642), is one of structured power and the establishment of an effective (bourgeois) society (Macpherson, 1985). His philosophy is both political and moral, and influenced a number of other major philosophical works, e.g., (Locke, 1997; Rousseau, 1968 (1762). As others have pointed out, e.g., Claassen (2020), there is a need for caution when applying historical concepts to modern situations without acknowledging the circumstances in which they were authored. However, given the influence Hobbesian thinking has had on modern society (Arendt, 2017 (1951), it would be "a missed opportu-

E-mail addresses: joseph.dasilva.2018@rhul.ac.uk, joseph.dasilva.2018@live.rhul.ac.uk

https://doi.org/10.1016/j.cose.2022.102674
0167-4048/© 2022 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

nity" (Claassen, 2020, p. 103) to ignore the value that can be offered by this analytical lens.[1]

We are not the first to look at modern businesses through a Hobbesian lens, e.g., Chandler and Mazlish (2005); Claassen (2020) and others have invoked Hobbes in reference to cyber security, e.g., Hughes (2010); Kaminski (2010); Stevens (2016). However, we believe we are the first to apply a business-as-Leviathan lens to concepts of cyber security in business and how these relate to the wider state Leviathan. By applying sociological lenses to cyber security within business, we aim to achieve, and encourage, greater reflexivity (Cormack, 2004, p. 119) within both academia and practice as to both the intended and unintended consequences of such functions.

Cyber security is inherently multi-disciplinary (Hall et al., 2015, p. 107) and its sociological aspects have been explored by many scholars e.g., Coles-Kemp et al. (2018); Deibert and Rohozinski (2010); Shires (2018); Stevens (2016), with direct calls being made for sociologists to research cyber security within organisations (Dawson and Thomson, 2018). Examples of sociological viewpoints being applied to cyber security within organisations include the exploration of social practices relating to cyber security within an organisation (Ashenden and Lawrence, 2016) and of trust building (Flechais et al., 2005). Others have explored the role of the CISO, e.g., Ashenden and Sasse (2013); Lanz (2017); Rai and Chukwuma (2019), including the importance of the social aspects of this role (Hooper and McKissack, 2016), and, from a methodological perspective, argued for computer security research to be grounded in an interpretive socio-organisational paradigm (Dhillon and Backhouse, 2001).

We begin by providing a brief conceptual grounding on Hobbes in Section 2. Next, we describe our methodology in Section 3 before presenting our research findings in Section 4. We unpack these in Section 5, employing a number of concepts from Hobbes for the purpose of analysis and interpretation, before concluding in Section 6, suggesting implications for practitioners and businesses, as well as future research directions.

2. Conceptual grounding

In this section, we briefly summarise a number of key concepts from Hobbes which are used as analytical lenses in Section 5 in order to interpret, and gain a deeper understanding of the findings in Section 4. We began with a ground-up analysis of our data, from which we identified a number of references to state power, fear and market dynamics in relation to cyber security. Subsequently, we brought these references into conversation with Hobbesian notions, due to the manifest linkages to his work, using these as a framework on which we built a deeper interpretation and derivation of meaning from the findings. Such an approach is well established in qualitative research that follows an interpretive paradigm, where new knowledge is developed through the application of existing theory to data, e.g., Burdon and Coles-Kemp (2019).

Hobbes has been influential in the very definition of security (Kangas et al., 2019, p. 69). Other scholars have previously employed his work in exploring the links between cyber security and state security, e.g., Coles-Kemp et al. (2018); Kaminski (2010), including aspects of surveillance, e.g., Bauman et al. (2014); Coles-Kemp et al. (2014) and cyber warfare, e.g., Brenner and Clarke (2010). Others have highlighted the importance of corporations in achieving national security, e.g., Carr (2016), with some problematising this relationship, e.g. Eichensehr (2017). The threat that cyber security may pose to national and international security has also been extensively explored by others, e.g., Warf and Fekete (2016), including the societal risks posed, e.g., Siroli (2018), the impacts that responses to this may have on freedoms, e.g., Nissenbaum (2005) and the threats to state power associated with cyber security risk (Carr, 2016). The application of sociological perspectives to businesses is also well established, e.g., Burrell, Morgan, 1987 1979; Silverman (1970); Woodward (1965). More recently, Geppert and Dörrenbächer (2014) summarised how power relations in multinational businesses have been studied from a sociological perspective and highlighted the links to wider societal power structures. In a broader context, the application of social perspectives to risk is well established, e.g., Beck (1992) with the impact, and use of, fear within society, e.g., Beck (2009); Furedi (2006); Giddens (1990) and how this supports wider power structures, e.g., Neocleous (2008), being a common thread.

We now briefly summarise a number of key concepts from Hobbes which form the basis of the analysis in Section 5.

2.1. The state of nature

Leviathan was written during the English Civil War,[2] and this turmoil was a key concern of Hobbes, who believed that his political science could avoid any recurrence and achieve a lasting peace. It is premised on an argument that, without effective governance, humankind would exist in a state of war, "of every man, against every man" (Hobbes, 1985, p. 185).[3] In this state, regardless of the existence of "actuall fighting" (Hobbes, 1985, p. 186), there is "continuall feare, and danger of violent death; And the life of man, solitary, poore, nasty, brutish, and short" (Hobbes, 1985, p. 186). The avoidance of this 'state of nature', as it is referred to, e.g., Merriam (1906), is a primary motivation in the establishment of the Leviathan, which provides security against it in exchange for obedience. This is one of the key tenets of *Leviathan*; citizens enter into a contract with the state in which this exchange takes place (Baumgold, 2013). The observance of this contract, according to Hobbes, was fundamental to achieving peace within a society, and was based on both "the absolute right of sovereigns to command...and the absolute duty of the people to obey" (Bejan, 2010, p. 613). This obedience is consensual (Chapman, 1975, p. 80) although citizens may suffer diminution as a result (Wolin, 1970). This contract, and the extension of Hobbes' ideas, may equate to tyranny, even totalitarianism (Arendt, 2017 (1951; Barkan, 2012). The Leviathan's "ultimate end is accumulation of power" (Arendt, 2017 (1951, p. 180). The tyrannical aspect is something that Hobbes himself does not deny and is, in fact, "proud to admit" (Arendt, 2017 (1951, p. 188); he is dismissive towards accusations of tyranny, labelling these as simply the protestatory responses of malcontents (Hobbes, 1985, p. 240).

While the Leviathan exists to avoid the state of nature, it benefits from the continued presence of this threat in the minds of its citizens. Without this threat, the Leviathan's power and dominion over its citizens is diminished; in order to exchange obedience for protection, there needs to be some peril, otherwise the equation is imbalanced. Security of citizens from threat is "[t]he *raison d'Ōtre* of the state" (Arendt, 2017 (1951, p. 181) (italics in original). Sovereignty is both achieved and maintained through

[1] It should also be noted that extensive conversation regarding Hobbes continues in International Relations and Sociology and it is not within the scope of this paper to explore these debates. Hobbes offers a starting point into wider viewpoints from these disciplines and provides one perspective, rather than an authoritative view on modern societies.

[2] Although it was a development of earlier ideas (Hob, 2021).

[3] *Leviathan* is "covertly gendered" (Carver, 2014, p. 118), with "the important actors in life [being] men...or very rarely...masculinized women" (Carver, 2014, p. 118). The primacy Hobbes provides to men is clear throughout the text, and he was "writing for a male audience...from a male point of view" (Di Stefano, 1983, p. 635n10).

fear (Lloyd and Sreedhar, 2020). Hobbes describes how "that which enclineth men least to break the Laws, is Fear" (Hobbes, 1985, p. 343) and, further, that fear may in fact be "the onely thing...that makes men keep them [i.e., laws]" (Hobbes, 1985, p. 343). He believed that "feare of some coercive Power" (Hobbes, 1985, p. 196), owned by the sovereign, was necessary in order to make citizens keep their promises (Peacock, 2010). Barkan, discussing Esposito (2008), describes "the sovereign's power to expose life to death as opposing but also interlinked sides of a persistent immunitary [*sic*] dynamic" (Barkan, 2012, p. 89). In other words, it is beneficial for the sovereign for threat to life to exist, so that the sovereign can offer protection to the citizenry from such a threat; if this threat ceases to exist, or ceases to be *perceived* to exist, then the power of the sovereign in commanding obedience is diminished.

Permanent emergency, warfare and power. Within the domain of International Relations (IR), the concept of permanent emergency has been established and discussed by a number of scholars, e.g. Neocleous (2008). This refers to the perpetuation of a state of threat, whereby a population's security, and often its way of life, are subject to, or positioned as being subject to, various forms of continuing menace. This environment facilitates the establishment of various responses to those threats that restrict the freedoms of citizens, in the name of 'security' (Bubandt, 2005; Neocleous, 2008), a concept which has many parallels with Hobbes' state of nature.

In a Hobbesian society, there is a never-ending need for the state to expand its power; "only by constantly extending its authority and only through the process of power accumulation can it remain stable" (Arendt, 2017 (1951, p. 184). If such a society were to achieve "complete security", then the state's power would crumble (Arendt, 2017 (1951, p. 184). Therefore, there is a need for the continual provision of "new props from the outside" (Arendt, 2017 (1951, p. 184), such as novel threats. The "ever-present possibility of war guarantees the Commonwealth a prospect of permanence because it makes it possible for the state to increase its power at the expense of other states" (Arendt, 2017 (1951, p. 184-5). According to Hobbes, "[i]t is rationally required to seek peace, but when peace is unattainable it is rationally allowed to wage war" (Gert, 2001, p. 245). Arendt further elaborates the need for a "never-ending accumulation of power [as being] necessary for the protection of a never-ending accumulation of capital" (Arendt, 2017 (1951, p. 186) and how this has underpinned imperialism and indeed modern society.[4]

Although a Hobbesian state may hold supreme power, its citizens still hold the right to rebel against it if such rebellion is for self-defence (Williams, 1996). As a precaution against such an eventuality, the Hobbesian state must "have recourse to arms to enforce civil order" (Williams, 1996, p. 221). In *De Cive*, Hobbes describes how "[a]ll judgement therefore in a City belongs to him who hath the swords" (Hobbes, 2009 (1642, p. 48). But the state must also remain trusted by its citizens, particularly in its determination of what is and is not a threat (Williams, 1996), and the most important control that the sovereign should have is over "language (which defines what is)" (Williams, 1996, p. 219–220).

Morality and threat In a Hobbesian society, defining 'what is' includes defining what is right and what is wrong. Hobbes viewed morality as subjective, and considered it as the responsibility of the Leviathan to determine what qualified as "good and bad, true and false, right and wrong" (Williams, 1996, p. 230).[5] For Hobbes "truth is a function of logic and language" (Williams, 1996, p. 217) and "what is granted to that authority [i.e., the Leviathan] is the right to decide among irresolvably contested truths: to provide the authoritative criteria for what is" (Williams, 1996, p. 219). This "control of normative doctrine" Lloyd and Sreedhar (2020) assigned to the Leviathan means that as well as defining what is right and wrong, the state can define *who* is right and wrong, and of the latter, what threats they pose. If sovereignty is predicated on, or maintained using, fear, and if the sovereign has authority to determine what is to be feared, then it is in the sovereign's interest for there to exist "demons... villains" (Neocleous, 2008, pp. 119, 223), otherwise not only is the state's authority in question, as its citizens are providing obedience without receiving anything in exchange, as there is nothing to be protected from, but even its identity as a state may be threatened (Heraclides, 2012). Hobbes does not refer to the benefits accruing to the state of maintaining the existence of specific threats, nor encourage their invention, however, in a criticism of religious authority, he does point out "who, that is in fear of Ghosts, will not bear great respect to those that can make the Holy Water, that drives them from him?" (Hobbes, 1985, p. 692).

The role of advisers. Hobbes discusses the value of "Counsell" (Hobbes, 1985, p. 303), distinguishing this from "Command" in that the latter "is directed to a mans [*sic*] own benefit" whereas the former is "to the benefit of another man" (Hobbes, 1985, p. 303). He defines "the first condition of a good Counsellour...[as being that] *his Ends, and Interest, be not inconsistent with the Ends and Interest of him he Counselleth*" (Hobbes, 1985, p. 307) (italics in original) and describes how "the Ability of Counselling proceedeth from Experience, and long study...*No man is presumed to be a good Counsellour, but in such Businesse, as he hath not onely been much versed in, but hath also much meditated on, and considered*" (Hobbes, 1985, p. 307) (italics in original). He further adds that "The wit required for Counsel...is Judgement" (Hobbes, 1985, p. 308) and believed that "[t]he most able Counsellours, are they that have least hope of benefit by giving evill Counsell, and most knowledge of those things that conduce to the Peace, and Defence of the Common-wealth" (Hobbes, 1985, p. 391).

2.2. Education and discipline

Hobbes "sought to cool men off, to pacify them, to drive them into the waiting arms of whoever might be ruling with the frightening imagery of a state of nature" (Chapman, 1975, p. 88). One of the mechanisms through which he intended to achieve this was through education. Hobbes had a clear view on education as being authoritarian and as being a role, indeed, a duty, of the state Bejan (2010). What Hobbes wished to be taught, according to Bejan, was Leviathan's "'doctrine'...This doctrine was no more than the existence of a 'mutual relation between protection and obedience', which required an 'inviolable observation'" (Bejan, 2010, p. 613). Hobbes believed that the sovereign's power should be "utterly authoritarian in principle...and vigilantly oversee the intellectual life of his subjects from the cradle to the universities, and from there to the grave" (Bejan, 2010, p. 621).

Hobbes saw the family unit as playing a crucial role in initiating this obedience; the family is "*Leviathan* writ small" (Chapman, 1975, p. 77) (italics in original). Hobbes saw parents as "representatives of the sovereign power" (Bejan, 2010, p. 620), and that "[b]y direction of the sovereign, the connection between protection and obedience is to be made quite clear" (Chapman, 1975, p. 82). "In teaching a child the nature of obedience in the family, a parent is teaching the nature of obedience in the state" (Chapman, 1975, p. 86) and "[t]o teach one's children that their obedience is due when protection is given is to learn the same lesson for one's self" (Chapman, 1975, p. 88). The control over language that the Leviathan holds, as dis-

[4] Modern globalisation practices being equivalent with imperialistic ones (Chilcote, 2002). Hobbes himself was actively involved in colonial enterprise (Jessen, 2012).

[5] Hobbes' morality continues to be a topic of some interest, and debate, for many scholars, e.g. Lloyd (2009).

cussed above, underpins Hobbes' emphasis on education rather than force as the method by which the Leviathan maintained power (Williams, 1996), such control also helping sustain its identity (Benwell and Stokoe, 2006). However, Bejan (Bejan, 2010, p. 619, p623n17) argues that Hobbes intended to stress discipline rather than education or training which are alternative translations of the *disciplina* used by Hobbes in *De Cive*.[6] Hobbes did appear to consider discipline and chastisement to be productive motivators for learning, with "negative reinforcement...[being] an effective teacher" (Chapman, 1975, p. 85). Beyond educational discipline, Hobbes believed in the value of punishment, for the purpose of "correction, either of the offender, or of others by his example" (Hobbes, 1985, p. 389). He considered that "the severest Punishments are to be inflicted for those Crimes, that are of most Danger to the Publique" (Hobbes, 1985, p. 389).

2.3. Leviathan and mini-Leviathan

As the family was a mini-Leviathan, so too are corporations. Hobbes saw corporations as intrinsic parts of the Leviathan, even as "vital" (Jessen, 2012, p. 66) to it. However, he also identified them as potential threats, as "wormes in the entrayles of a naturall man" (Hobbes, 1985, p. 375), and in order to address these threats, they needed to be adequately governed (Jessen, 2012). This view of corporations as potential threats is similar to his view of children as potential threats to the mini-Leviathan of the family (Chapman, 1975; Hobbes, 2009 (1642) if they are not adequately controlled (through education and punishment) and indeed, Hobbes uses a parent-child metaphor when referring to a form of corporation (Hobbes, 1985; Jessen, 2012).

The mini-Leviathan of the corporation may pose a particular threat to the state-as-Leviathan where it is a multinational and therefore not subject to a single sovereign power (Chandler and Mazlish, 2005; Claassen, 2020). This can result in those corporations being able to direct and influence legislation and regulation differently in the different states they operate in Roach (2005), frustrating attempts to achieve consistent control. Hobbes was concerned that companies would become so strong that they affected the Leviathan's own power (Jessen, 2012). Arendt points out that Hobbes could see multinational corporations as the logical endpoint of the "acquisition of wealth conceived of as a never-ending process...for the accumulating process must sooner or later force open all existing territorial limits" (Arendt, 2017 (1951, p. 189).

Barkan argues that "corporate power and sovereign power are *ontologically linked*" (Barkan, 2013, p. 4) (italics in original). The "entanglement" (Hall, 2014, p. 741) between corporate businesses and states provides a link between the concept of state Leviathans and the corporation as both agent-of-Leviathan[7] and as mini-Leviathan in its own right. Echoing Chapman (1975), Heath *et al.* refer to a corporation as "a society writ small", but also as "an actor within the larger society in which it operates" (Heath et al., 2010, p. 437). Part of the role that a corporation plays as agent-of-Leviathan is in the generation of "social wealth" (Claassen, 2020, p. 123) and partly through enacting regulatory control over the citizenry (Barkan, 2013), even acting as a form of police (Barkan, 2012; Foucault, 2009; Pasquino, 1991).

Viability and survival. Hobbesian logic is based upon the avoidance of "death, pain, and disability" (Gert, 2001, p. 243) and that such "natural reason ...makes use of instrumental reason and verbal reason to achieve its goals" (Gert, 2001, p. 248), that is, "the avoidance of an avoidable death" (Gert, 2001, p. 249). Hobbes believed that "the terrour of present death" was even a valid excuse for an individual to commit a crime "because no Law can oblige a man to abandon his own preservation" (Hobbes, 1985, p. 345), and described how "since every man hath a Right to preserve himself, he must also be allowed a Right *to use all the means, and do all the actions, without which He cannot Preserve himself*" (Hobbes, 2009 (1642, p. 5) (italics in original). However, such is the drive for self-preservation, that, without the governance of the Leviathan, this would lead to the 'war of all against all' (Hobbes, 1985), due to the "independence of the individuals in determining the best means to preserve their own life" (Jessen, 2012, p. 74). As well as self-preservation of individuals, Hobbes is "unequivocal that self-preservation is the primary goal of those forming a commonwealth" (McClure, 2013, p. 115). Hobbes' concerns regarding survival, both of individuals and of the Leviathan itself,[8] are echoed in discussions in classical organisational literature regarding a business's concern with ensuring its own continued viability, e.g. Beer (1979); Mintzberg (1979).

3. Methodology

We collected data between October 2019 and July 2020 through 21 semi-structured interviews and by downloading each company's most recent annual report. 15 CISOs and six organisational leaders were interviewed, as shown in Appendix A. The organisational leaders comprised two Chief Executive Officers (CEOs), two Chief Financial Officers (CFOs), one Non-Executive Director (NED) and one Chief Information Officer (CIO). The organisations represented a range of different industries, although with a particular weighting in one sector. As we began to notice repetition of comments from participants, we considered that data saturation may be approaching, however, data saturation is a problematic concept (O'Reilly and Parker, 2013). Ultimately we made a decision to stop gathering data on "[t]he adequacy of the sample ...[not] solely on the basis of the number of participants but the appropriateness of the data" (O'Reilly and Parker, 2013, p. 195). We regularly revisited and revalidated this decision during the analysis phase, to continually confirm our judgement that the sample size was adequate. The use of annual reports as well as interview data provided triangulation, as well as the gathering of multiple perspectives through the interviewing of non-CISO participants.[9]

One of the researchers is a practising CISO and used their own network of professional contacts to recruit participants, effectively producing a "snowball sample" (Hammersley and Atkinson, 1995, p. 135). Access to Board members is difficult outside of a professional environment and, therefore, these participants were approached through CISOs who were participating in the research, as well as our personal networks. Participants were not compensated for their participation in this research. Interviews took place either face-to-face at their own office locations or online, the latter in response to the COVID-19 pandemic which commenced during data collection. We recorded the interviews and transcribed them as soon as possible following each interview, capturing non-recorded aspects such as body language and spatial information, in a handwritten journal immediately following each interview. Interview guides were prepared with prompts to be used as necessary,[10] however, interviews were approached as conversations rather than extractions of data and, therefore, these were not used in a strict manner, following (Hermanowicz, 2002).

[6] In which Hobbes states "Man is made fit for Society not by Nature, but by Education" (Hobbes, 2009 (1642, p. 8).

[7] A possibly unintended consequence, which we argue in more detail in Section 5.3.

[8] Through the avoidance of war.

[9] Due to difficulties in obtaining access to these senior leaders, it was not possible to obtain multiple perspectives from every organisation, as had been our original intention.

[10] See Appendix B and Appendix C.

The majority of Participants, and all of those in CISO roles, self-identified as male. In addition, there was limited ethnic diversity in the study and all participants can also be considered to be 'elites'. This lack of diversity, however, reflects a broader lack of diversity in the cyber-security industry. We received approval from our our institution's Research Ethics Committee for self-certification before beginning the research and designed the study to minimise both the collection of personally identifiable information and the risk of indirect identification. Participants were provided with consent forms and information sheets[11] two working days before each interview which explained how data would be anonymised and protected. Participants were anonymised, with randomly assigned pseudonyms being utilised which, in this paper, have been substituted for participant numbers. We redacted any sensitive or potentially identifiable information during transcription and destroyed all recordings following transcription.

Interview transcripts were analysed inductively and coded in multiple cycles using NVivo 12 (Qua, 2021) and applying a variety of coding types, following Saldaña (2016). Subsequently, we applied a deductive approach in order to categorise and rationalise the codes. A similar method was used to analyse annual reports, however, as this was performed subsequent to the interview coding cycles, coding became more deductive, as codes and concepts determined at the previous inductive stage were, consciously and unconsciously, reused. We developed themes from our data following Braun and Clarke (2006, 2019). Following others, e.g. Saldaña (2016), we produced analytic memos throughout as well as using diagrams to explore relationships and to identify and explore themes developed from the data, again following Braun and Clarke (2006) and combining several methods from Saldaña Saldaña (2016).[12]

As has been established within cyber-security scholarship, e.g. Burdon and Coles-Kemp (2019), qualitative research that follows an interpretive paradigm is an effective means of studying cyber-security practice. The use of semi-structured interviews to gather data is also well established, e.g. Ashenden and Sasse (2013); Burdon and Coles-Kemp (2019); Moore et al. (2015); Singh et al. (2013), as is analysis of annual reports to derive insight about businesses (Joshi et al., 2018; Zmud et al., 2010), including the use of document coding (Zmud et al., 2010) as discussed further below.

4. Findings

Our thematic analysis produced multiple themes, a number of which had Hobbesian connotations and we present these below.[13] Section 4.1 shows these organisations as mini-Leviathans, Section 4.2 covers aspects of survival articulated by these businesses and Section 4.3 sets out these organisations' role in wider society.[14] Certain quotations are not attributed to limit the risk of identification. No direct quotations from annual reports are included for the same reason and where single quotation marks are used, these indicate paraphrasing.

4.1. The organisation as Leviathan-writ-small

The organisations in this study demonstrated a number of features that indicated their operation as miniature societies. These included references to the organisation having both a culture and 'values', which were observed in the majority of annual reports and approximately half of the interview transcripts. The culture of the organisation affected how the participants viewed their ability to influence cyber-security outcomes. This included a continuum regarding risk posture being described by many participants, from "ludicrously conservative" to less conservative (CISO8). These organisations regulated employee behaviour, indicated by specific mentions of mandatory standards of behaviour and conduct, on which staff were trained, measured and, in some cases, penalised for non-compliance. Organisations in this study expected their staff to comply with their policies, adhere to their 'core values' and even to adjust their 'mindset' as part of working for the company. CISOs described having responsibilities to "introduce the right sort of behaviours and judgements in our workforce" (CISO2).

Cyber security was an area of both discipline and punishment. Part of the role of the cyber-security function in these organisations was "to hold feet to the fire" (CISO5). Compliance with security policies and standards was mandated and failure to comply could result in "[being] on a disciplinary" (CISO3), with staff facing "disciplinary action ...even if they've done nothing wrong" (CISO12). Despite a number of CISOs being keen to avoid the characterisation, cyber-security teams were seen as performing a policing function. This included specific references to being "the police" as well as more subtle references to "stop[ping] people having fun" (CISO1) and "trying to find [staff] doing wrong" (CISO8).

As well as disciplinary action, the organisations in this study linked staff remuneration, particularly at a senior level, to cyber security through their performance objectives, both explicitly and implicitly. These included multiple references to punishment of staff through "clawbacks" of bonus payments in particular. Triggers for the latter included reputational impact, direct losses, regulatory investigations, contractual breaches and, commonly, general failures in risk management. More broadly, remuneration was dependent on a number of factors including both risk management and ethical performance, areas that were commonly linked with cyber security. In some cases, cyber-security objectives were described as specific measures relating to bonus payments, as were measures relating to the completion of mandatory compliance training.

Cyber security was also associated with state punishments, whether through fines, "other sanctions ...from government" (CFO2) and even incarceration. Some of those punishments were viewed as useful by participants. CISO9 described how "it was only when the likes of Marriott Hotels or BA [British Airways] started to get massive fines relating to personal data that suddenly Boards sat up and took notice". The annual reports also indicated that these organisations were concerned that cyber-security failings would lead to punishments, either from regulators or through legal action, with explicit references to enforcement and censure that were considered to be threats to organisational viability, as discussed in Section 4.2.

4.1.1. Cyber security as pedagogy

As well as applying discipline, a key role of the CISOs in our study was educating staff. References to cyber-security education were made by multiple participants as well as across the majority of annual reports. This involved not just "making sure they're [i.e., staff] educated well" (CISO3) but also "[making] cyber-security meaningful for themǪon a personal level" (CISO11). There was a need to "educate" because cyber security was "another language" (CISO5). Senior stakeholders were also included, and their education was specifically called out in a number of annual reports, particularly the recency of such education.

Various methods used by these organisations to educate staff and stakeholders on cyber security were mentioned, including "visual breakdowns" (CISO2) and "games" (CISO11), as well as testing of staff, particularly through simulated phishing attacks. Many

[11] See Appendix D.

[12] See Appendix E for an example.

[13] Other themes will be explored in future research.

[14] Throughout the remainder of the paper, we use 'business' and 'organisation' interchangeably for ease of reading. For the avoidance of doubt, all of the organisations referred to are commercial businesses.

of the references in the annual reports to this education included the modifier 'mandatory'. There were indications of the deliberate use of fear in relation to cyber security, such as the use of "war games [with senior leaders] ...and you watch them shit themselves" (CISO11). CEO1 described the value in using fear, stating that "[when staff] see the art of the possible and it's scary ...they say okay, I'm gonna whine less". CISOs acknowledged that "it's very difficult for a conversation [about cyber security] not to gravitate back to being scary and inevitable" (CISO8) but were conscious of the risk of "scaremongering" (CISO5).

Cyber security was consistently characterised by participants as having an ethical or moral dimension, with "rights and wrongs" relating to cyber security being a common refrain observed throughout the data. One CISO described their department as "the moral police force of the company" (CISO8). Cyber security personnel had a "duty to communicate risk" (CFO2) and to "hold [the organisation] to account to make sure they're doing the right thing" (CISO7). Cyber-security failures at a single organisation could have wider societal impacts; one participant described their company as "the soft underbelly" for their customers, who themselves supported wider societal goals such as distribution of food. The articulation of cyber threats in moral terms was also consistent. This included references to cyber threat actors as "bad guys" (CISO9) and a statement that "the mission [of the cyber-security function] really is to protect against crime" (CISO8).

4.1.2. The CISO as advisor

As well as being an educator, the CISO for these organisations also performed a role as a form of advisor to the organisation. This was summed up by one senior leader who described the need to be told "no you don't need to be worried about that, yes you do need to be worried about this" (CEO1). Many CISOs articulated this role explictly, such as being "a trusted advisor to the business ...to provide guidance, provide advice" (CISO12). Annual reports also indicated the advisory role that specialist risk management functions, including cyber security, provided to these businesses, describing the use of such advisers in providing both predictability and interpretation of uncertainty. Such advisers were trusted to provide "judgements" (CISO2).

CISOs were aware that their functions were "going to be there for the long term that's for sure" (CISO3), with senior leaders agreeing that it was "certainly not gonna get less important" (CFO1). However, CISOs in this study indicated concerns that they could be subject to punishment through job losses. They were "not under any illusions [as] to where accountability sits" (CISO3). They knew that they "wouldn't escape the spotlight" (CISO2) and "that it's implicit with our role, if something goes wrong, you're the guy [that gets fired]" (CISO12).

4.2. Viability and survival

The large majority of businesses in our study expressed cyber-security threat as a survival-level concern, with cyber-security incidents being able to "destroy the business" (CEO1) or "bring the company to its knees [and] drive us to bankruptcy" (NED1). In many cases cyber security was explicitly referenced in the viability statements made in their annual reports.[15] Cyber-security incidents were positioned as threats to this viability by many of these organisations, with fear of regulatory action and associated fines and reputational damage being a prime concern. Such incidents were considered as existential threats and phrases such as "absolute catastrophe" (CISO11) and "disastrous" (CISO9) were common. Cyber security functions were, in a number of cases, seen as assuagement against this threat to viability, with CISOs providing "a level of comfort" (CISO14) to their senior leaders.

Cyber security threats were considered to be both permanent and fearful. They were "really scary" (NED1) and resulted in "sleepless nights" (CISO1). For these participants, it was "when not if [a cyber-security incident occurs]" (CISO14), and they needed to "accept the fact that we are going to be compromised" (CISO11). This normalisation of cyber-security incidents was also indicated by senior leaders, with them being characterised as "the kind of things that happen all the time" (CEO2). NED1 described how cyber security was "gonna get worse not better", with CFO1 describing cyber security as "a continuing moving goal post". Cyber-security threats were "so sophisticated [and] change almost on a daily basis" (CISO14), and there were "troubled times ahead" (CISO4). Similar statements were observed in the annual reports, with references to the "sophisticated" and "continual" nature of cyber threat being common throughout.

As well as explicit references to the potentially catastrophic nature of a cyber-security incident, we also observed more implicit references to fear in connection with cyber security, such as mentions of cyber crime and cyber terrorism. Threats were also seen to originate from other sources, including hacktivists and, in particular, nation states. One CISO described how "the whole concept of state sponsored threat actors is frightening" (CISO14). Some of these states were named, e.g., "the Chinese ...somebody sitting in Siberia ...North Koreans" (CEO1), "Iran ...China ...Russia" (CISO8), whereas other references were generic, unnamed nation states. Explicit references to cyber warfare were also observed, with cyber security being a "method of attack against the nation" (CISO3). Cyber security was positioned as a component of national security by multiple participants and annual reports, highlighting their organisation's role within this, which we describe further below. Metaphors of war in connection with cyber security were common throughout the data, including "attack", "defend", "war stories" and "war games".[16]

4.3. The organisation in wider society

Virtually all of the organisations in this study articulated, through their annual reports, the broader societal role that they played, and the benefits that society derived as a result. These included the contributions those companies made through investment, through community support and the delivery of "critical services" to that society. Annual reports included language relating to societal obligations and responsibilities, societal impacts, and even direct references to the social contract. Participants also mentioned the role that their organisations played in wider society. Some referred to their organisations as being critical to the functioning of the UK economy, while many referred to the role that they played in national security. One organisation's cyber-security department was assessed by a UK military agency before they were "allowed to bid" on a contract, with "the quality of the cyber-security team [being] very much the litmus test". Another organisation's CISO described being "conscious of ...our responsibility ...to defend against [a cyber attack on the country]" while one of the CEOs described being obligated by government to take actions in relation to national security. Other references to the role these organisations

[15] All organisations in this study made reference to various threats to their ongoing viability in their annual reports, however, this is unsurprising given that such statements are a requirement of the UK Corporate Governance Code (Council, 2018).

[16] Other stereotypically masculine language and concepts were observed throughout much of the data. These included participants referring to their businesses being like a "bearpit" (CISO6), needing to avoid being "too soft" (CISO13) and being "browbeaten" (CISO1). Similar language was seen in the annual reports, with the use of conventionally masculine concepts such as aggression, conflict, strength and even penetration being common. Both the interview data and the annual reports also featured multiple references to competition, another masculine archetype.

played in national cyber security included participating in national security working groups and being regularly assessed by security services and other government departments.[17] It appeared there were double standards regarding evaluation by government, with government departments charged with assessing these businesses responding with "oh Lord no, we would never achieve it" when asked if they complied with the same requirements. There were also references to invitation-only and industry-specific information exchanges with representatives from state security services where specific threats were shared with attendees as well as indications of more indirect governmental influence. The latter included senior leaders being invited by government departments to participate in "roundtable discussions" and being encouraged to utilise certain frameworks. One CEO described how "the UK government has been quite vocal [on cyber security]", with another CEO stating that "[governments, plural] keep an eye out, which works in ways that neither you or I need to know how it works but they keep an eye out". A number of annual reports alluded to potential negative impacts on revenue if the focus of their government customers moved away from security-related products and services. It was also noted that a number of these organisations had senior leaders who either currently or previously held positions within the military, government or quasi-government organisations.

4.3.1. Security versus freedom

A perceived dualism between security and freedom in relation to cyber security was indicated within the data. CISO4 described there being "an amount of disruption that is necessary in order to do the right thing". Security controls were "very tight" (CFO2) with an expectation that they would "get tighter and tighter" (NED1). CEO1 linked this to fear, describing how "the more that we go and scare ourselves ...the more the organization becomes willing to tolerate some inconvenience in what it does".

Organisations in this study surveilled their staff in a number of ways. These included monitoring of company vehicle use, for both health and safety and ethical reasons, i.e., vehicle emissions, as well as monitoring of technology systems for cyber security and IT reasons. As well as surveilling their staff, there were also examples of organisations surveilling their customers in terms of how their products and services were used by them, although with an acknowledgement from CISO8 that "it is a tough balance, not everybody wants it [i.e., monitoring of product usage] ...some people are really paranoid". They described difficulties in achieving "a balance between inspection and surveillance", and potential impacts upon "free speech", with their customers holding different views ranging from "absolutely no problem [with monitoring]" to monitoring of activity being "abhorrent". There were also indications of deference, even servility, to wider surveillance occurring at state level, as per the final CEO comment in Section 4.3.

5. Discussion

In this section, we unpack our findings by applying a number of Hobbesian concepts in an attempt to provide deeper meaning. We first describe in Section 5.1 how Hobbes can be used to read the threat to survival that cyber security posed to these organisations. Next, in Section 5.2 we apply Hobbes to cyber-security related discipline and punishment enacted by these organisations. Finally, in Section 5.3 we explore the wider role of cyber security in the context of the state Leviathan.

[17] One participant described having recently been visited by representatives from the UK intelligence services directly preceding our interview for this research, which may have affected their responses.

5.1. "Perpetuall feare"

Cyber security is often characterised as fearful, with cyber threats being both permanent and evolving (Ehrlicher, 2021), and cyber attacks being seen as inevitable (Pearlson et al., 2021). The businesses in our study seemed to agree, with cyber threat appearing to be normalised. Participants, both CISO and non-CISO, considered these threats to be enduring and businesses needed to accept that they would be compromised. This implies a "perpetuall cyber warre" (Stevens, 2016, p. 120). These businesses existed in "continuall feare" (Hobbes, 1985, p. 186), threatened by "death, poverty, or other calamity" (Hobbes, 1985, p. 169) arising from something, i.e, cyber security, that was not well understood, even mystical,[18] as "perpetuall feare, [is] always accompanying mankind in the ignorance of causes" (Hobbes, 1985, p. 169-70).[19] The role of the CISO may be valued as one "that can make the Holy Water" (Hobbes, 1985, p. 692) that provides protection from fearful things, and, therefore, is motivated to maintain the fear and dread that underpins their value.[20]

Survival was clearly a concern for these businesses. Cyber security was positioned as a threat to viability by many of these organisations, with fear of regulatory action and associated fines and reputational damage in particular being a prime concern. Such concerns with viability and survival, arguably the primary motivation for businesses (Beer, 1979), are analogous with seeking to avoid punishment that could lead to "pain, and disability" and, ultimately, "death" (Gert, 2001, p. 243). The punishments they sought to avoid were enacted by the larger Leviathan of the state and, as mini-Leviathans, these businesses cascaded this concept, instituting their own mechanisms of punishment for their employees, as we discuss below. Internal experts were positioned by many of these organisations as "guards" that protected them against the various harms that they faced. Cyber security functions were seen as assuagement against threats to business viability and helped these businesses to manage the uncertainty they experienced as a result of these threats and ensure their continued survival. This allowed them to shape their future to a certain extent, aligning with Hobbes' encouragements towards continued attentiveness to threats (Stevens, 2016), but also provided a resource that articulated and predicted those threats, based on both past, and imagined future, events.

5.1.1. Permanent cyber emergency

Many of these organisations played a role in national cyber security, including participating in invitation-only national security working groups. Such fora, in which government intelligence services share details of cyber threats with specific industries, demonstrate the role that governments play in maintaining a state of permanent cyber emergency. They provide a mechanism through which governments can both maintain fear and amplify it. This could be achieved through exaggeration or even fabrication, particularly when considering the reliance of the state Leviathan on the persistence of this fear.[21]

[18] The impacts of cyber-security threats may be considered by these organisations as "real" but the threats themselves, including their sources, may be considered more ephemeral. The mystical nature of cyber security was a separate theme developed from the data which will be explored in future research.

[19] The state of nature may even be considered as a "secular hell" (Bejan, 2010, p. 618). Similar metaphors have been used with reference to cyber security, such as "cyber hell" (Shrobe et al., 2018, p. 480) and "cyber apocalypse" (Stevens, 2016, p. 105).

[20] The potential that this offers for "cyber sophistry" will be explored in future research.

[21] The use of falsehoods in the service of continued peace was something that Hobbes appeared to support (Hobbes, 1985, p. 703) (Arendt, 2006, p. 224, pp. 290-1), although, as Bejan summarises, this reading is debated and other scholars have

A permanent emergency offers benefits as a "master narrative" (Smith and Sparkes, 2008, p. 18) that can be invoked to support actions taken by businesses and individuals within that business, whether to justify investment or to justify restrictive controls such as surveillance, as we discuss in Section 5.3. The positioning of cyber security as warfare, which is a narrative repeated by both media and governments (Stevens, 2016), establishes that concept in the minds of all parties to that war, whether attacker or attacked. Adversaries, or even just those who disagree, will respond to the narrative of cyber security-as-war and then treat it as such, focusing on attack and defence, rather than seeing it as anything else, for example, as a collective problem of identifying and addressing weaknesses that threaten all. This could lead to actions that have unintended consequences, such as state purchasing, and hoarding, of vulnerabilities, e.g. Hoeksma (2017). Cyber security-as-collective-problem could be considered a "flattened narrative" (Farley, 2001), with preference instead provided to the cyber security-as-war concept which supports the maintenance of existing power structures. This can also be considered as indexing a "meta-narrative" (Symon et al., 2014, p. 3) of existing or 'traditional' enemies (Stevens, 2016), and the "superiority of ...the West" (Neocleous, 2008, p. 172), as suggested by the references to (ex-)communist states[22] observed in the data. There is an almost paradoxical relevance of both Foucault's and von Clausewitz's perspectives on war, with cyber war being a "mere continuation of policy by other means" (von Clausewitz, 1873, p. 12) and cyber politics being "the continuation of war by other means" (Foucault, 2004, p. 15).[23] Each of these also provides economic benefits (Neocleous, 2008), as we discuss below.

Positioning cyber security as an existential threat, as a war with "apocalyptic" (Stevens, 2016, p 121) consequences, may also allow for exceptionalism and deviance from existing laws, both national and supranational. Hobbes explicitly permitted defiance of law if motivated "by the terrour of present death" (Hobbes, 1985, p. 345). Such exceptionalism based on existential threat can be observed in modern societies, e.g. Government (2000, 2006); USA (2001), including in relation to cyber security threats (Walker, 2006). References to national security also connect with this warfare motif. As the nation is 'under threat' then there is a collective sense of conflict and, therefore, a suggestion that everyone has to play their part.

The fear generated by these threats propels citizens into "the waiting arms of whoever might be ruling" (Chapman, 1975, p. 88). Such fear may be a "necessity-justification" (Chapman, 1975, p. 89) for enduring power, and, as Chapman suggests, it is straightforward to conceive of such "justification ...[occurring] at the state level, as a function of real or manufactured inter-state crises" (Chapman, 1975, p. 89), particularly with regard to threats that are hard to understand or somewhat ephemeral in nature, such as those related to cyber security. If cyber-security threats result in fearful and bewildered citizens, those citizens are easier to moderate. Educating citizens on, or even communicating the existence of, cyber threats may couple "paranoia with pacification" (Chapman, 1975, p. 90).

Businesses that publicly articulate their cyber-security capability, through references to the existence of dedicated personnel and the actions they are taking to mitigate cyber risk, are demonstrating their strength and their readiness for war in a "calculated presentation" (Foucault, 2004, p. 92). Such pronouncements, particularly in annual reports, also serve to maintain the organisation's power by "memorializ[ing]" what the organisation has achieved, arguably also creating "an obligation" (Foucault, 2004, p. 67) for future leaders of that organisation.

5.1.2. Cyber discourse

The collocation of certain words observed in the data, e.g. 'sophisticated' and 'threat', which are also seen in broader cyber-security discourse, e.g., Noonan (2021), may carry "encoded ideologies" (Benwell and Stokoe, 2006, p. 113) that also serve to maintain power structures. References to 'nation state' alongside 'cyber threat' carry an association of war being waged, particularly by previously established 'enemies of the West'. As "packaged, homogenized violence" (Baudrillard, 1998, p. 160), such references not only maintain hegemonical power ('we' are threatened by 'them' therefore we must take action) but also provides a means by which citizens are mollified, arguably even tranquillised, as well as driving consumption (Baudrillard, 1998), as we discuss in Section 5.3.

Hobbes saw the importance of the Leviathan having control over language. By maintaining discourse that defines, or repeats, who and what are threats, and the relative urgency of those threats, the state can maintain broader narratives of fear, war, friend and enemy, good and bad, and right and wrong. Such narratives in connection with cyber security featured in our data but, in particular, the articulation of cyber threats in moral terms was consistent. A moral association may strengthen the power and importance of these threats for citizens but also result in unquestioning acceptance of those positions. Although morality may (arguably) be subjective (Zimmerman, 2006),[24] it may be *experienced* objectively in everyday life (Hofmann et al., 2014) and, therefore, by assigning a moral dimension to cyber security, citizens may be discouraged from challenging the 'need' for intrusive controls associated with it.

The use of specialist cyber-security language, which is inaccessible to non-specialists, provides power to those that can understand it, and this power is increased when there is an interpretation being provided. An interpretation provides an opportunity, conscious or unconscious, to imbue its translation with other meanings, whether moral, political or emotional. Language is a means by which reality is both experienced and constructed (Benwell and Stokoe, 2006), with those who have the power to interpret specialist or 'foreign' language also having the power to construct reality for their audience. Cyber security may offer a channel through which sentiments and beliefs that are beneficial to the Leviathan can be established and maintained, such as those relating to 'enemy threats' or those relating to 'security versus privacy', a questionable dualism (Neocleous, 2008) that we discuss below.

Cyber security in both academic and mass media communication abounds with military tropes, e.g. Bond (2018); Corera (2017); Kanniainen (2019); Limnéll (2016) and many metaphors of war were observed throughout our data. Such militaristic references may be motivated by a desire for those who work in cyber security, most of whom are male (Peacock and Irons, 2017),[25] to cast themselves as heroic, a masculine trait that is strongly Hobbesian (Di Stefano, 1983). The perception of always being 'at war' from a cyber-security perspective, besides the ontological 'comfort' this may provide Mitzen (2006), may also be motivated by a masculine desire for such valorous narratives, demonstrating masculin-

found his intentions "far less sinister" (Bejan, 2010, p. 623n13). However, Hobbes was clear that the authority of the sovereign was absolute, even in matters of "Prophecy" (Hobbes, 1985, p. 466–469).

[22] Who are also competing state Leviathans.

[23] It is outside the scope of this paper to explore these arguments in more detail, however, future research will apply a number of Foucauldian lenses to our Findings.

[24] It is outside the scope of this paper to explore the ongoing and unresolved philosophical debate concerning this highly contentious position.

[25] Modern corporations are also male-dominated (Connell and Wood, 2005), often with hierarchical structures that feature inherent masculinity through militaristic associations (Carver, 2014).

ity through "metaphor, and bravado" (Carver, 2014, p. 115). Such language may also be deeply performative (Butler, 2002 (1990; Carver, 2014). Cyber security professionals may possess a distinctive and exceptional "power" that helps form their heroic identity, namely "knowledge" and "right method" (Di Stefano, 1983, p. 642) which represents "the requisite special weapon of the epic hero" (Di Stefano, 1983, p. 642), and, similar to Hobbes' self-conception as heroic, cyber-security professionals may be "proposing a solution to a predicament that [is] more masculine than human in tenor" (Di Stefano, 1983, p. 643).

5.2. Protection in exchange for (cyber) obedience

Cyber security was an area of discipline and of punishment. Organisations in this study required obedience from their staff, in terms of policy compliance, as well as alignment with standards of behaviour. Obedience, whether through completion of mandatory training, compliance with cyber security policies and standards, or through effective management of cyber-security risk, was mandatory and non-compliance would be punished. As well as disciplinary action, non-compliance resulted in impacts upon staff remuneration, particularly at a senior level. The potential for the organisation to remove a level of security from its staff, in terms of the security of continued employment and income, suggests what Barkan[26] describes as an "immunitary dynamic" (Barkan, 2012, p. 89). As with the Leviathan, these businesses were providing protection in exchange for obedience and if this obedience was not received, their protection could be removed.

As discussed above, the Leviathan is tyrannical. While our study has not focused on all aspects of corporate life, some indications of tyranny that align with Friedrich and Brzezinski (1961 (1956) description of typical totalitarian features were observed. The cyber security departments in these organisations appeared to function as an official police force, despite CISOs wishing to avoid this characterisation, and performed surveillance of staff. They acted as agents of the mini-Leviathan, applying discipline and punishment. Beyond cyber security, these organisations applied punishments if staff did not comply with their dictates, including if they behaved contrary to their values. This may also have been motivated by a lack of parity between the interests of the organisation and the interests of individual employees. Punishment was imbued with morality by extending a concept of 'doing the right thing'. These organisations educated and indoctrinated their staff, with fear being a component of these processes.

Cyber security was also associated with state-directed punishment. The threat of punishments relating to cyber security had a regulatory effect on these organisations, with considerable attention paid in the annual reports to addressing how compliance was monitored and enforced, including references to the organisational capabilities charged with these responsibilities. Organisations in this study wanted to "do the right thing" in order to avoid punishment by the Leviathan and internally, as mini-Leviathans, instituted mechanisms of punishment for their employees, extending that same concept. The references that participants made to the "usefulness" of cyber security incidents affecting other organisations, including explicit references to those that resulted in regulatory action, suggest a Hobbesian view of punishment as providing examples for others but also a spectacular nature to cyber-security punishment. This is similar to that described by both Foucault (1991 (1977) and Farley (2001),[27] and punishment itself is a representation of power (Foucault, 1991 (1977). The Leviathan is terrorised by cyber-security threats, whether real or imagined, which, in the most fearful type, arise from the Leviathan's known enemies. It expects its "lesser Common-wealths" (Hobbes, 1985, p. 375) to take action against these threats for the benefit of the larger commonwealth. Failure to obey results in punishment by the Leviathan, such punishments being public spectacles that provide examples to others.

5.2.1. CISO as teacher and "counsellour"

The CISOs in these organisations were educators, which included "teaching ...obedience" (Chapman, 1975, p. 86) and applying discipline. They taught staff about the existence of cyber-security threats, communicated a defined set of rules, indoctrinated them into acceptable behaviours, monitored their compliance against these, and punished them when they transgressed. Staff were educated that both they, and the organisation itself, were subject to cyber-security threats. In order for the organisation to mitigate those threats, protecting both itself and its staff, those staff must forgo certain liberties and agree to be regulated. CISOs utilised fear in their instruction, aligning with Hobbes' template Chapman (1975).

As well as being teachers, CISOs were advisors, "Counsellours" (Hobbes, 1985, p. 391), for these businesses. They had "knowledge of those things that conduce to the Peace, and Defence of the Common-wealth" (Hobbes, 1985, p. 391). Although such counsellours may be expected to have consistent "Ends and Interest" with the organisation, they may still derive "benefit by giving evill Counsell" (Hobbes, 1985, p. 391), particularly if that benefit is continued employment. One area where the CISO may not share equivalence with Hobbes' counsellours is in their risk of scapegoating. Hobbes' view was that "he that demandeth Counsell, is Author of it; and therefore cannot punish it" (Hobbes, 1985, p. 304), however, the CISOs in this study indicated concerns that they were subject to punishment through job losses.

5.3. Cyber security and the Leviathan(s)

It is not in the interests of a Hobbesian society to achieve "complete security" (Arendt, 2017 (1951, p. 184). Both the relative novelty of cyber-security threats and the continued emergence of new types of such threats, including the 'sophisticated' aspects thereof, can be viewed as "new props from the outside" (Arendt, 2017 (1951, p. 184) that stoke the flames of the possibility of war, particularly when attributed to nation states. These threats also offer "new and ever-growing fields for the honorable and profitable employment" (Hobson, 1900, p. 28) of citizens,[28] particularly the bourgeoisie who are appeased by new job opportunities, and further stimulate consumption and growth (Arendt, 2017 (1951).

In a (post)modern world where threats to the state are less obvious or apparent, i.e., there is no obvious invader on the doorstep, particularly since the end of the Cold War, the inclination of the citizen towards obedience may be weaker. The state may, therefore, feel the need to motivate obedience by making it clear that it is still offering protection, but not against obvious invaders. Rather, it is against opaque, mysterious, and highly sophisticated threats, from which the state is providing protection. Not only do these threats need to be explained by specialists, due to their complexity, they also need to be 'sold' to citizens through education. It is even conceivable that such teachings could be contrary to "true Philosophy" (Hobbes, 1985, p. 703) but serve the benefit of the state, as well as securing the continued employment of the teacher (Arendt, 2006). This could motivate the embellishment of any threats communicated. It may be more advantageous for the state Leviathan to have such education delivered not

[26] Discussing Esposito (Esposito, 2008).

[27] Farley also invokes Hobbes in his exploration of state punishment.

[28] Specifically, the employment of "sons" (Hobson, 1900, p. 28).

through a state organ but rather through another component of society such as businesses. Rather than a conscious decision taken by the Leviathan this may be a fortuitous benefit, but one that it seeks to encourage through, e.g., communicating the 'responsibility' that businesses have in protecting wider society against cyber threats (Government, 2016).

Dedicated cyber-security functions support, and repeat, messages relating to a broader security agenda (Neocleous, 2008), both among a company's employees and their customers. There is a wider security industry that "mustQensure that security is never really achieved" (Neocleous, 2008, p. 156). This provides commercial benefits, as well as supporting an insecurity that is relied on by the state to achieve its aims (Neocleous, 2008), as previously noted by Arendt (2017 (1951). If states ultimately seek the perpetuation of (at least partial) insecurity, then it may be in their interests to define 'security' in an insecure manner, at the same time encouraging organisations and wider society to achieve a level of 'insecure security'. Recent attempts by governments to weaken or circumvent strong encryption, e.g. Google (2019); Thomson (2019), some successful, e.g. Taylor (2019), can be argued as demonstrating this desire.[29] In addition, motivating organisations to operate a cyber-security function that inures employees, who are also citizens, to increased and intrusive surveillance and monitoring may also contribute to this same "insecure security", albeit potentially providing associated benefits to those employees, such as greater privacy.

These organisations taught their staff about the existence of cyber-security threats, communicated a defined set of rules, indoctrinated them into acceptable behaviours, monitored their compliance against these, and punished them when they transgressed. In order for both the organisation and their staff to be protected from these threats, staff must forgo certain liberties and agree to certain controls, such as being surveilled. In this manner, the employee-as-citizen is indoctrinated into a mindset of being subject to cyber threats and becomes inured to the custom of exchanging privacy for security. Considering power relations as interactive, processual and two-way (Benwell and Stokoe, 2006, p. 89), cyber security within business can be seen as a mechanism through which citizen-employees participate in the maintenance of hegemonic power.[30] Cyber security personnel ensure that messages of insecurity and threat are repeated, as well as performing a policing role that normalises surveillance, while other citizen-employees support hegemonic power in the role they play as the surveilled.

Cyber security can be used to terrorise citizens into compliance and to justify their surveillance. Cyber-security controls have an effect not just on the employee-as-employee but also the employee-as-citizen. Educating employees on what they need to be protected from, and what they need to obey in order to be protected, may, directly or indirectly, inure or condition employees towards broader obedience, including acceptance of controls that could be used beyond purposes of cyber security, providing benefits to the state beyond citizen protection.[31] The use, and acceptance, of surveillance in these organisations may function as a normative control (Beech, 2008), conditioning or preparing staff (citizens) to be surveilled in wider society and supporting a wider meta-narrative in relation to security versus privacy. The Leviathan-writ-small of the business plays a role on behalf of the state Leviathan in conditioning the employee-as-citizen towards obedience, and surrendering of liberties, in exchange for protection from threat. The opaque and relatively unseen nature of the threat, which requires specialists to deliver education about its existence, is beneficial to the state for ensuring continued obedience, and even in maintaining its own identity (Heraclides, 2012), and its own history (Sims, 2005).

5.3.1. Consumption

Companies within a broader security industry accrue benefit from perpetuating a state of insecurity (Krahmann, 2018). This may be exploited through a narrative of unforeseeable risks that builds uncertainty (Krahmann, 2018), fear stimulating consumption (Baudrillard, 1998) in the same way as war (Walker, 1993). The security and defence industries need there to be something to be defended against (Neocleous, 2008). As well as cyber security being one of these industries, with cyber-security crises leading to increases in budgets (Tal, 2021), even in other, unaffected, businesses (Havakhor et al., 2019), cyber capability is a factor in being "allowed to play" in others, and can be a barrier to entry. Cyber security is thus enmeshed with a much broader aspect of modernity in the sense of continued consumption, both as an industry in its own right and as a facet of other industries. Some organisations in this study indicated the benefit they accrued from governmental spending on security-related products and services, further demonstrating the link between societal threat and certain business sectors. The Leviathan, which seeks continued and never-ending growth, can stimulate expansion by creating a need for spending that counteracts fear and anxiety (Baudrillard, 1998). Such spending can arguably "in some way "improve" life in civil society" (Walker, 1993, p. 111). Where that fear and anxiety is generated by unseen and ever-more-sophisticated sources, there is, in theory, no upper limit to the growth that could be achieved.

6. Conclusion

This paper has shown that Hobbes' work provides a useful lens through which to view the role that cyber security plays in society within and without businesses, particularly given the importance of Hobbesian thinking to Western political thought and the enmeshed nature of states and corporations. Cyber security offers a useful mechanism from which the Leviathan derives benefit. It supports the establishment of fear and discipline, therefore, cementing power through obedience and conformance. Additionally, although less obviously, it also drives accumulation of capital through consumption of products and services, and job creation.

Businesses play a crucial role for the Leviathan. They employ and educate citizens, inuring them to surveillance and punishing them when they transgress. They maintain narratives of morality. They generate and expand capital. In some cases, they operate critical infrastructure and perform other state functions on the Leviathan's behalf. Businesses are themselves mini-Leviathans, and are in fear of threats to their existence. Cyber security functions within those businesses provide a means by which they seek to avoid a state of nature. They also, indirectly, provide that function to the state, supporting its attempts to dominate competing state Leviathans. Actions taken by businesses in relation to cyber security involve spending that provides fuel for the continued growth of the Leviathan's power, and that of the hegemony that the Leviathan supports.

Our research opens up a number of interesting future directions. The Hobbesian perspective that we introduce may encourage the application of broader contexts from International Relations (IR), using other IR theorists and perspectives to explore cyber security within businesses and wider society. In particular, we consider there to be benefit to research avenues relating to the

[29] Although increased surveillance may be possible without weakening encryption (Gasser et al., 2016).

[30] Other hegemonical linkages included the roles that these businesses played in national security and the presence of senior leaders representing military or governmental actors, as well as references to both direct and indirect governmental influences on these organisations.

[31] "The most potent weapon in the hands of the oppressor is the mind of the oppressed" (Biko, 1981, p. 137).

context of businesses within globalisation and geopolitics, including the establishment of cyber norms and other developing areas of study. Most significantly, our research encourages greater reflexivity within the discipline of cyber security, both for researchers and for practitioners. The latter may benefit from considering the role they unwittingly perform in the maintenance of both political and commercial power structures. Businesses themselves may benefit from reflecting on the role that they play in supporting the state Leviathan, and indeed in wider globalisation of Hobbesian models of control. Such reflexivity and improved awareness of broader contexts offers empowerment for individuals within those businesses, particularly CISOs in this case. Part of the role of a CISO is being the agent of two Leviathans, the mini-Leviathan of the business that employs them, and the larger Leviathan of the state. The latter role may not be as immediately obvious or recognisable and may be uncomfortable for many CISOs. However, recognising this allows for reflexive consideration and engagement with the implications, or at the very least an acknowledgement of what the CISO does or does not agree with. The CISO may acknowledge that there is value in implementing surveillance in order to protect the business-as-Leviathan but if that helps to normalise surveillance by the state Leviathan on the employee-citizen, there may be a potential internal conflict that they need to either resolve or come to terms with. We have considered whether this perspective could potentially lead to (perceived) negative outcomes for the cyber-security industry. For example, will there be less surveillance within organisations as a result of CISOs resisting the support that they indirectly provide to state surveillance? We consider this to be unlikely, however, it opens up further avenues of potential research, particularly to explore whether or not a CISO's primary focus is on their employer. After all, their employer is offering them the most immediate protection, in terms of salary and continued employment, and, similar to the Hobbesian family structure, is where their primary interest and indeed obedience may lie. Therefore, the CISO may do what is in the interest of their employer and ensure that they protect them as best they can, including implementing controls that they would feel less comfortable with if they were in place in wider society. Their employer's interests may also be more closely aligned with their own, particularly in terms of ensuring continued viability, than with the state Leviathan's, and this symbiotic relationship may be an important factor in any decision-making regarding controls. Future research could also consider the possibility of 'deviant' corporations and the concept of insider threats through a Hobbesian lens.[32] The latter, in particular, could also be expanded to consider the perspective of resistance.[33] Further, there may be an interesting parallel to explore with regard to biological threats, such as Covid-19, and cyber threats. Each of these can be considered as unseen, ephemeral threats that require specialist advisors and motivate restrictive controls that could be considered as offering additional benefits to a Hobbesian state.[34]

Our Findings offer a broad perspective on cyber-security practice within organisations. As such, they will also be interpreted through other analytical lenses and connected to other, existing, models of managing cyber security.

Credit Author Statement

The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

[32] We thank one of the anonymous reviewers for these suggestions.

[33] This has potential parallels with prior work performed by Coles-Kemp et al. (2018).

[34] Again, we thank one of the anonymous reviewers for inspiring this angle.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Interview details

Below in Table A1 we provide a brief summary of the industry sectors represented in this study, whereas Table A2 provides details of the participant interviews.

Appendix B. Interview topic guide: CISOs

This details the themes and example interview questions that were asked of CISO participants. Following Hermanowicz, these questions were not intended to be "an inflexible list that the interviewer follows rigidly" (Hermanowicz, 2002, p. 483); rather, they provided a series of prompts to direct the conversation.

Interview prompts

References are included, where questions have been adopted verbatim from existing work.

Table A1
Industry sectors represented in this study.

ICB Super-sector	*Number of organisations*
Banks	1
Food, Beverage and Tobacco	1
Industrial Goods and Services	6
Personal Care, Drug and Grocery Stores	2
Real Estate	1
Technology	1
Telecommunications	2
Travel and Leisure	1
Utilities	3
Total	**18**

Coverage of industries represented in this research based on classifications taken from Com (2021); Ind (2018).

Table A2
Participants & interviews.

Participants		Interview	
ID	*Duration*	*Medium*	*Timing*
CISO1	00:48:29	F2F	Oct19
CISO2	00:49:28	F2F	Oct19
CISO3	00:47:33	F2F	Dec19
CISO4	00:44:41	F2F	Dec19
CISO5	00:43:44	F2F	Dec19
CISO6	00:41:38	F2F	Jan20
CISO7	00:45:19	F2F	Jan20
CISO8	00:49:41	F2F	Mar20
CISO9	00:51:30	F2F	Mar20
CISO10	00:38:43	Remote	Apr20
CISO11	00:55:45	Remote	May20
CISO12	00:40:56	Remote	May20
CISO13	00:40:07	Remote	Jun20
CISO14	00:46:07	Remote	Jul20
CISO15	00:50:02	Remote	Jul20
CEO1	00:24:59	F2F	Dec19
CEO2	00:42:45	F2F	Jan20
CFO1	00:45:41	F2F	Jan20
CFO2	00:40:52	Remote	Apr20
CIO1	00:47:28	Remote	Jul20
NED1	00:27:52	F2F	Dec19

In addition to 15 CISOs, we conducted semi-structured interviews with two Chief Executive Officers (CEOs), two Chief Financial Officers (CIOs), one Non-Executive Director (NED) and one Chief Information Officer (CIO), between October 2019 and July 2020.

- Could you describe your role for me?
- How long have you been in that role (at this organisation)?
- What do you consider to be the overall purpose of the cyber-security function?
- "Who or what is being secured?" (Smith, 2005, p. 487)
- How have your views about the cyber-security function changed over the years?
- To whom do you report?
- What is your opinion on your reporting line?
- What information relating to cyber-security do you provide to the board?
- Do you consider that information to be useful? How do you think that information helps the board?
- What do you think they appreciate about the cyber-security function?
- How would they describe its purpose?
- What do you think they find frustrating about it?
- What do you think the perception of top management on cyber security is?
- How would you describe your responsibility with regard to cyber security?
- What would be the impact to the organisation if it did not have a dedicated cyber-security function?
- What would your impression be of an organisation in your industry that did not have a dedicated cyber-security function?
- In relation to cyber security, "I would finally like to ask about something you are most proud of. What stands out as something that has left a strong positive impression on you?" (Hermanowicz, 2007, p. 646)
- Request permission to use anonymised verbatim quotes
- Request for optional and anonymised demographic information

Appendix C. Interview topic guide: non-CISOs

This details the themes and example interview questions that were asked of non-CISO participants. As above, these were prompts to direct the conversation rather than a fixed list.

Interview prompts

References are included, where questions have been adopted verbatim from existing work.

- Could you describe your role for me?
- How long have you been in that role (at this organisation)?
- What are the main challenges of being a board member?
- What does cyber security mean to you?
- From where do you tend to hear about cyber-security issues?
- Tell me about the organisation's cyber-security function
- If they don't have anyone responsible for cyber security – is that a conscious decision? any particular rationale?
- What do you consider to be the purpose of the cyber-security function?
- Why do you think the function is important to the organisation?
- From your perspective, "[w]ho or what is being secured?" (Smith, 2005, p. 487)
- How have your views about the cyber-security function changed over the years?
- What responsibility do you consider the board to have regarding cyber security?
- What would you consider to be the biggest cyber-security risk to your organisation?
- How would you rank cyber security versus other risks to the organisation? Has that changed? Do you anticipate that changing in future? If so, why?
- How would you know about cyber risk if you didn't have someone in the organisational responsible for it? Is that different to any other risk?
- Have you experienced any significant cyber-security incidents?
- Are there any technological advances/changes that you anticipate affecting the cyber security of your organisation?
- Are you confident that the cyber-security function is effective?
- How do you know they're doing a good job / the right thing?
- What information relating to cyber security do you receive?
- What do you consider to be the goal of that information?
- Do you think you get enough information on cyber security? Or too much?
- What do you think the organisation has done particularly well with regard to cyber security?
- How could the cyber-security function be improved?
- How is cyber security governed?
- How would you describe the rest of the board's perspective on cyber security?
- What visibility of the cyber-security function do you have?
- How do you feel about cyber risk?
- How do you feel when you hear about cyber-security incidents affecting other companies?
- How would you describe the responsibility that the CISO has with regard to cyber security?
- What would be the impact to the organisation if it did not have a dedicated cyber-security function?
- What would your impression be of an organisation in your industry that did not have a dedicated cyber-security function?
- What do you consider the future to look like with regard to cyber security?
- Do you have any other thoughts on cyber security that we haven't covered today?
- Request permission to use anonymised verbatim quotes
- Request for optional and anonymised demographic information

Appendix D. Participant Information Sheet

Invitation to take part

You are being invited to take part in a research project. Before you decide whether or not you would like to take part it is important for you to understand why the research is being done and what it will involve. Please read the following information carefully and discuss it with others if you wish. If you have any questions or particular concerns, please let us know. You will find the relevant contact details on the last page of this document.

Why is this research being done?

This research aims to:

1. understand the purpose and benefit of a cyber-security function within a commercial organisation, as perceived by the leaders of that function and the leaders of the overall organisation (including how that may differ)
2. explore how commercial organisations structure their cyber-security functions and how those structures reflect the purpose of the function

This project is intended to complete by 2022.

Who is doing the research

The researcher is REDACTED.

Why have I been chosen?

You have been chosen on the basis of your job role, either as a Chief Information Security Officer or as a senior leader within a commercial organisation that has a senior listing on the London Stock Exchange. This study intends to capture input from across a broad range of industries and the target number of companies surveyed is 20–40.

Do I have to take part?

No. It is up to you to decide whether or not to take part. If you do decide to take part, you will be asked to sign a Consent Form. You can withdraw during the interview at any time without giving a reason and your data will be removed from the study. Once the interview has finished you can still withdraw your data up to the point where the data has been analysed and anonymised, so that your identity cannot be determined. Your decision to take part or not to take part will involve no penalty or loss, now or in the future.

What will taking part involve?

Taking part will involve participating in a one-hour interview with the researcher. The interview will be recorded using an encrypted digital recording device. You may also be asked to provide related documentation such as organisational charts or policy documents. Details on how data will be protected are shown below. You may subsequently be invited to take part in a focus group to share your feedback on the results; a separate information sheet will be provided in this event.

What are the possible benefits and/or disadvantages of taking part?

One benefit of taking part is that you contribute to academic research that will be beneficial to future researchers and businesses; by understanding how the purpose and structure of a cyber-security function differs across industries and company types, reusable models or common measurements may be possible and it may be possible to infer from this analysis which models suit which scenarios. You may also benefit from the reflection that will take place as part of the interview process which may provide insights to your own business or role that prove useful.

Other than giving up your time to take part, no disadvantages to taking part in this research are foreseen. There is a small risk of identification from narrative quotation which is explained further below.

Will my taking part be kept confidential?

All the information collected about you during the course of the research will be kept strictly confidential in accordance with current data protection regulations (for more information, please see INSTITUTION REDACTED Data Management Policy). Data storage and access will also be managed in line with the General Data Protection Regulation (GDPR) (for more information on your rights when it comes to accessing interview-related data, please see INSTITUTION REDACTED Data Protection Policy). You will not be identifiable in any reports or publications without specific consent. All data will be identified only by a code, with personal details kept on a secure computer, accessible only by the researcher.

All interviews will be recorded using a digital recording device where audio is encrypted at the point of capture. Backup recordings will be captured on another encrypted device and deleted once the primary recording has been confirmed as successful. Recordings will be transferred to an encrypted drive for storage and transcription purposes and then deleted from the recording device. Interviews will be transcribed verbatim and anonymised; sensitive information will be redacted during transcription. Anonymisation will be performed using a random assignment of a pseudonym; mapping to company and role will be recorded on an encrypted spreadsheet stored on an encrypted drive, accessible only to the researcher and stored in a locked safe when not in use. Any company documentation provided will also be stored on an encrypted drive, accessible only to the researcher and stored in a locked safe.

You will be asked specifically if you consent to the use of anonymised verbatim quotations in the final thesis; although anonymised, there is a risk of identification in the event that you use (or have used) a similar narrative in any public material, whether in the past or in future. If you decline, then no verbatim quotations from your contribution will be published.

What will happen to the results of the research project?

Results will be written up as REDACTED. Results will be presented in terms of themes arising, with comparisons across industry segments. If any individual data are presented, the data will be completely anonymous, without any means of identifying the individuals involved, subject to the limitation described above if quotations are used. Anonymised results or analysis of these results may appear in future academic publications.

Ethical review of the study

The project has been self-certified by the researcher as compliant with INSTITUTION REDACTED Research Ethics requirements.

Contact for further information

REDACTED

Appendix E. Coding diagrams

Analytic diagram detailing the different categories of codes from the interview data that contributed to the development of the Hobbesian themes described above, with their relative coding densities and breadth of coverage. This forms a subset of a larger series of diagrams analysing further themes developed from the same data that are not shown for reasons of space.

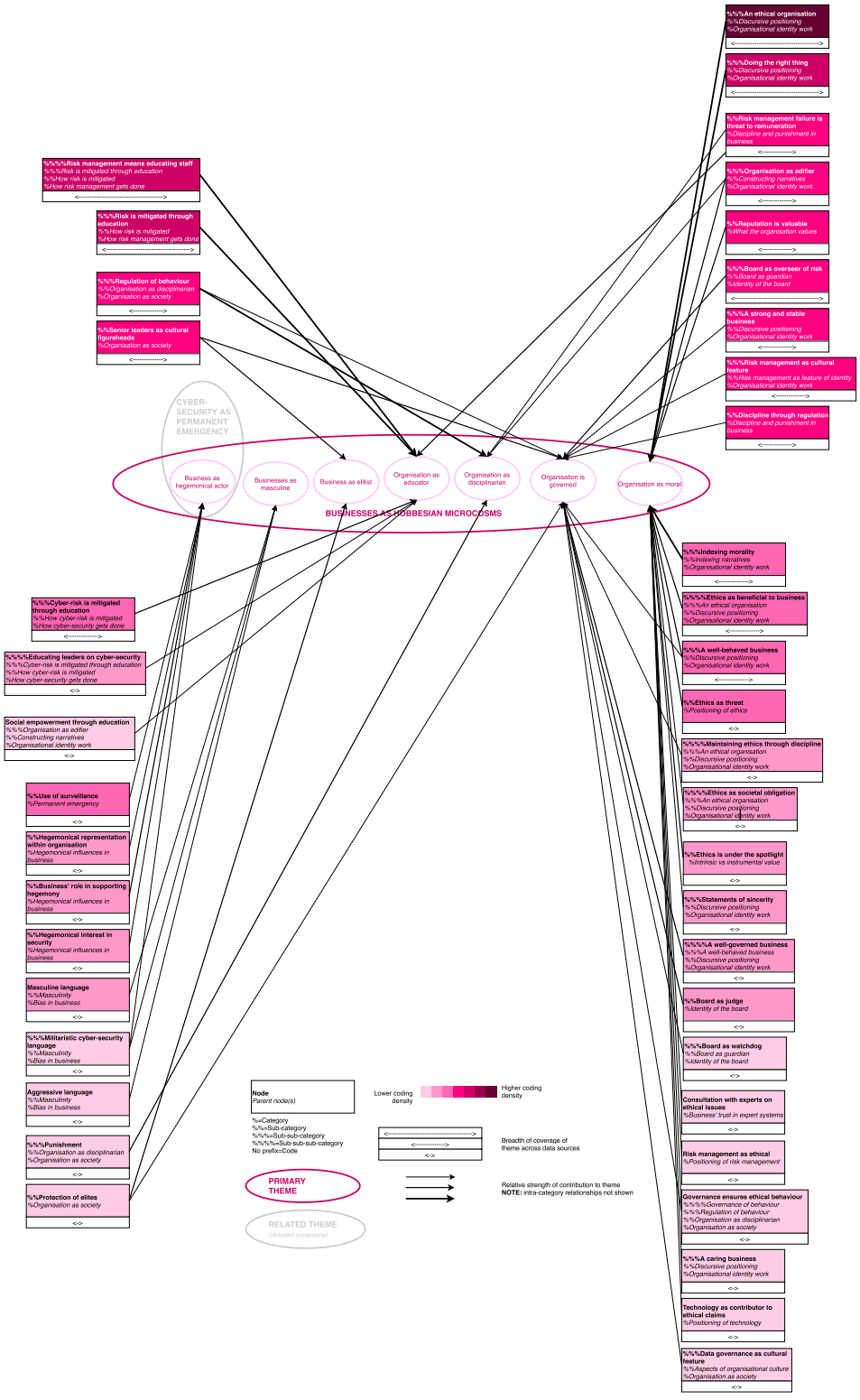

Fig. 1. Snapshot of data codes and categories used in the analysis process.

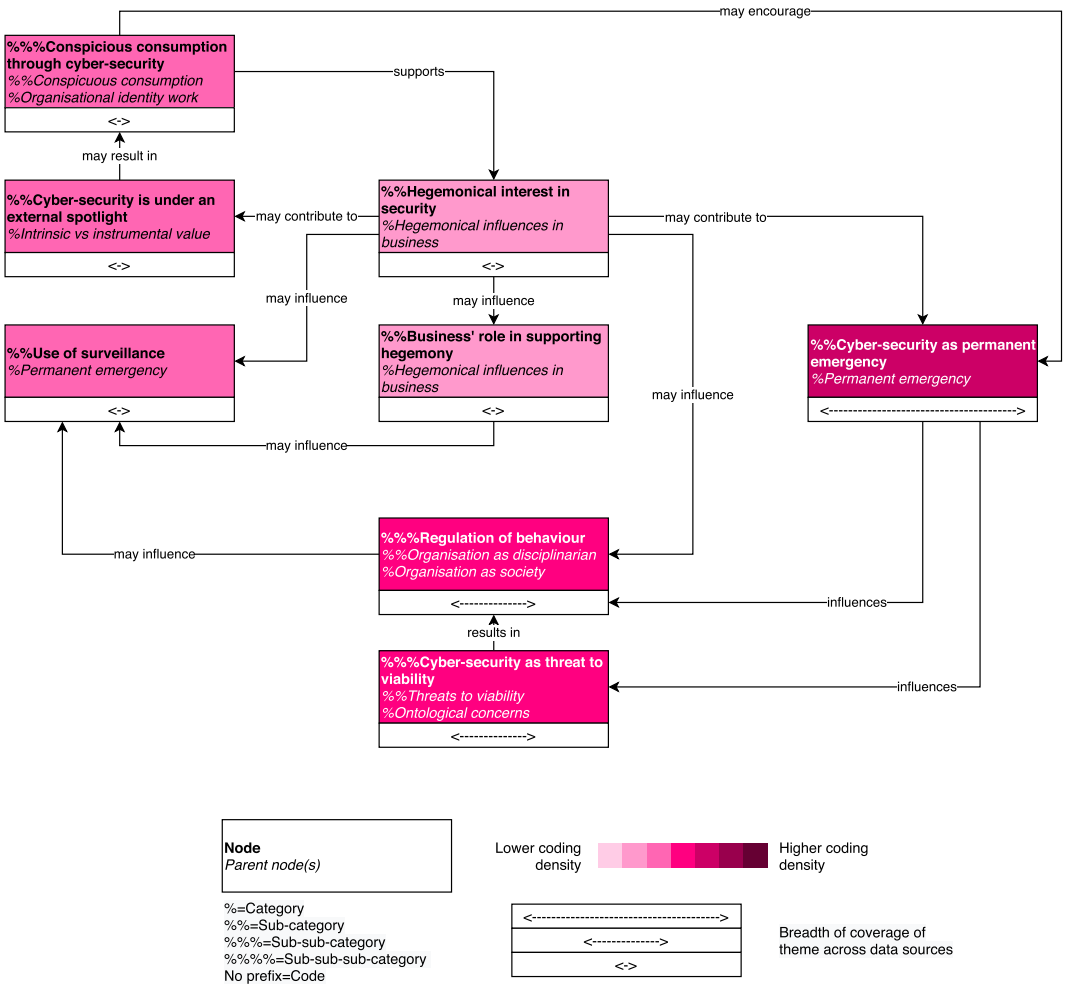

Fig. 2. Analytic diagram proposing potential relationships between key codes.

Further analytic diagram detailing potential relationships between key codes, with their relative coding densities and breadth of coverage.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2022.102674.

References

Arendt, H., 2006. Between Past and Future. Penguin Publishing Group.

Arendt, H., 2017 (1951). The Origins of Totalitarianism. Penguin Books Limited.

Ashenden, D., Lawrence, D., 2016. Security dialogues: building better relationships between security and business. IEEE Security & Privacy 14 (3), 82–87. doi:10.1109/MSP.2016.57.

Ashenden, D., Sasse, A., 2013. CISOs and organisational culture: their own worst enemy? Computers & Security 39, 396–405. doi:10.1016/j.cose.2013.09.004.

Barkan, J., 2012. Roberto Esposito's political biology and corporate forms of life. Law, Culture and the Humanities 8 (1), 84–101. doi:10.1177/1743872110363401.

Barkan, J., 2013. Corporate Sovereignty: Law and Government Under Capitalism. University of Minnesota Press.

Baudrillard, J., 1998. The Consumer Society: Myths and Structures. London: Sage, London.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., Walker, R.B.J., 2014. After Snowden: rethinking the impact of surveillance. International Political Sociology 8 (2), 121–144. doi:10.1111/ips.12048.

Baumgold, D., 2013. "Trust" in Hobbes's political thought. Polit Theory 41 (6), 838–855. doi:10.1177/0090591713499764.

Beck, U., 1992. Risk Society: Towards a New Modernity. Sage, Los Angeles, [Calif.].

Beck, U., 2009. World at Risk. Polity Press.

Beech, N., 2008. On the nature of dialogic identity work. Organization 15 (1), 51–74. doi:10.1177/1350508407084485.

Beer, S., 1979. The heart of the enterprise. Wiley.

Bejan, T.M., 2010. Teaching the Leviathan: Thomas Hobbes on education. Oxford Review of Education 36 (5), 607–626. doi:10.1080/03054985.2010.514438.

Benwell, B., Stokoe, E., 2006. Discourse and Identity. Edinburgh: Edinburgh University Press, Edinburgh.

Biko, S., 1981. Black consciousness & the quest for a true humanity. Ufahamu: A Journal of African Studies 11 (1). doi:10.5070/F7111017259.

Bond, D., 2018. Britain preparing to launch new cyber warfare unit. http://www.ft.com/content/eef717f2-bb6e-11e8-8274-55b72926558f.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual Res Psychol 3 (2), 77–101. doi:10.1191/1478088706qp063oa.

Braun, V., Clarke, V., 2019. Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health 11 (4), 589–597. doi:10.1080/2159676X.2019.1628806.

Brenner, S.W., Clarke, L.L., 2010. Civilians in cyberwarfare: conscripts. Vanderbilt Journal of Transnational Law 43, 1011–1076.

Bubandt, N., 2005. Vernacular security: the politics of feeling safe in global, national and local worlds. Security Dialogue 36 (3), 275–296. doi:10.1177/0967010605057015.

Burdon, M., Coles-Kemp, L., 2019. The significance of securing as a critical component of information security: an Australian narrative. Computers & Security 87, 101601. doi:10.1016/j.cose.2019.101601.

Burrell, G., Morgan, G., 1987 (1979). Sociological paradigms and organizational analysis: elements of the sociology of corporate life. Gower.

Butler, J., 2002 (1990). Gender trouble: tenth anniversary edition, 2nd ed. London: Routledge.

Carr, M., 2016. Public-private partnerships in national cyber-security strategies. Int Aff 92 (1), 43–62. doi:10.1111/1468-2346.12504.

Carver, T., 2014. Men and masculinities in international relations research. The Brown Journal of World Affairs 21 (1), 113–126.

, 2005. In: Chandler, A.D., Mazlish, B. (Eds.), Leviathans: multinational corporations and the new global history. Cambridge University Press.

Chapman, R.A., 1975. Leviathan writ small: Thomas Hobbes on the family. Am Polit Sci Rev 69 (1), 76–90. doi:10.2307/1957886.

Chilcote, R.H., 2002. Globalization or imperialism? Lat Am Perspect 29 (6), 80–84.
Claassen, R., 2020. Hobbes meets the modern business corporation. Polity 53 (1), 101–131. doi:10.1086/712231.
Coles-Kemp, L., Ashenden, D., O'Hara, K., 2018. Why should I? Cybersecurity, the security of the state and the insecurity of the citizen. Politics and Governance 6 (2), 41–48. doi:10.17645/pag.v6i2.1333.
Coles-Kemp, L., Zugenmaier, A., Lewis, M., 2014. Watching you watching me: the art of playing the panopticon. Stand Alone 147–162. doi:10.3233/978-1-61499-450-3-147.
Connell, R.W., Wood, J., 2005. Globalization and business masculinities. Men Masc 7 (4), 347–364. doi:10.1177/1097184X03260969.
Corera, G., 2017. NHS cyber-attack 'came from N Korea'. https://www.bbc.com/news/technology-40297493.
Cormack, P., 2004. Sociology and Mass Culture: Durkheim, Mills, and Baudrillard. University of Toronto Press.
Council, F. R., 2018. UK Corporate Governance Code. https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf.
Companies and Securities - London Stock Exchange, 2021. https://www.londonstockexchange.com/statistics/companies-and-issuers/companies-and-issuers.htm.
Dawson, J., Thomson, R., 2018. The future cybersecurity workforce: going beyond technical skills for successful cyber performance. Front Psychol 9. doi:10.3389/fpsyg.2018.00744.
Deibert, R.J., Rohozinski, R., 2010. Risking security: policies and paradoxes of cyberspace security. International Political Sociology 4 (1), 15–32. doi:10.1111/j.1749-5687.2009.00088.x.
Dhillon, G., Backhouse, J., 2001. Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal 11 (2), 127–153. doi:10.1046/j.1365-2575.2001.00099.x.
Di Stefano, C., 1983. Masculinity as ideology in political theory: Hobbesian man considered. Womens Stud Int Forum 6 (6), 633–644. doi:10.1016/0277-5395(83)90024-9.
Ehrlicher, D., 2021. Council Post: The Evolution Of Cybersecurity In 2021. https://www.forbes.com/sites/forbestechcouncil/2021/03/05/the-evolution-of-cybersecurity-in-2021/.
Eichensehr, K.E., 2017. Public-private cybersecurity. Tex Law Rev 95 (3), 467–538.
Esposito, R., 2008. Bíos: Biopolitics and Philosophy. University of Minnesota Press.
Farley, A.P., 2001. Amusing monsters. Cardozo L. Rev. 23, 1493.
Flechais, I., Riegelsberger, J., Sasse, M.A., 2005. Divide and conquer: The role of trust and assurance in the design of secure socio-technical systems. In: Proceedings of the 2005 Workshop on New Security Paradigms. Association for Computing Machinery, New York, NY, USA, pp. 33–41. doi:10.1145/1146269.1146280.
Foucault, M., 1991 (1977). Discipline and Punish. Penguin Books.
Foucault, M., 2004. Society Must Be Defended. Penguin Books.
Foucault, M., 2009. Security, Territory, Population. Palgrave Macmillan.
Friedrich, C.J., Brzezinski, Z.K., 1961 (1956). Totalitarian Dictatorship and Autocracy. Praeger, New York.
Furedi, F., 2006. Culture of Fear Revisited : Risk-taking and the Morality of Low Expectation, 4th ed. London : Continuum, London.
Gasser, U., Gertner, N., Goldsmith, J.L., Landau, S., Nye, J.S., O'Brien, D., Olsen, M.G., Renan, D., Sanchez, J., Schneider, B., Schwartzol, L., Zittrain, J.L., 2016. Don't Panic: Making Progress on the "Going Dark" Debate. Berkman Center Research Publication.
Geppert, M., Dörrenbächer, C., 2014. Politics and power within multinational corporations: mainstream studies, emerging critical approaches and suggestions for future research. International Journal of Management Reviews 16 (2), 226–244. doi:10.1111/ijmr.12018.
Gert, B., 2001. Hobbes on reason. Pacific Philosophical Quarterly 82 (3–4), 243–257. doi:10.1111/1468-0114.00127.
Giddens, A., 1990. The Consequences of Modernity. Stanford University Press.
Google, Apple criticise GCHQ snooping tech, 2019. BBC News.
Government, U., 2000. Regulation of Investigatory Powers Act 2000.
Government, U., 2006. Terrorism Act 2006.
Government, U., 2016. National Cyber Security Strategy 2016 to 2021. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.
Hall, P., Heath, C., Coles-Kemp, L., 2015. Critical visualization: a case for rethinking how we visualize risk and security. Journal of Cybersecurity 1 (1), 93–108. doi:10.1093/cybsec/tyv004.
Hall, S., 2014. Entanglements between finance, corporate power and state sovereignty. Geopolitics 19 (3), 740–745. doi:10.1080/14650045.2014.899016.
Hammersley, M., Atkinson, P., 1995. Ethnography Principles in Practice (Second Edition). Routledge.
Havakhor, T., Zhang, T., Hammer, B., 2019. Cybersecurity Talents and the Value of IT Security Investments. SSRN Scholarly Paper. Social Science Research Network, Rochester, NY.
Heath, J., Moriarty, J., Norman, W., 2010. Business ethics and (or as) political philosophy. Business Ethics Quarterly 20 (3), 427–452.
Heraclides, A., 2012. 'What will become of us without barbarians?' the enduring Greek–Turkish rivalry as an identity-based conflict. Southeast European and Black Sea Studies 12 (1), 115–134. doi:10.1080/14683857.2012.661944.
Hermanowicz, J.C., 2002. The great interview: 25 strategies for studying people in bed. Qual Sociol 25 (4), 479–499. doi:10.1023/A:1021062932081.
Hermanowicz, J.C., 2007. Argument and outline for the sociology of scientific (and other) careers. Soc Stud Sci 37 (4), 625–646. doi:10.1177/0306312706075337.
Hobbes, T., 1985. [1651] Leviathan. Penguin Books, London.
Hobbes, T., 1839. The English Works of Thomas Hobbes of Malmesbury; now first collected and edited by Sir William Molesworth, Bart, Vol. 6. John Bohn, London.
Hobbes, T., 2009 (1642). De Cive. Dodo Press.
Hobbes's Leviathan, 2021. https://www.bl.uk/collection-items/hobbess-leviathan.
Hobson, J.A., 1900. Capitalism and Imperialism in South Africa. The Tucker Publishing Co., New York.
Hoeksma, J., 2017. NHS cyberattack may prove to be a valuable wake up call. BMJ: British Medical Journal 357.
Hofmann, W., Wisneski, D.C., Brandt, M.J., Skitka, L.J., 2014. Morality in everyday life. Science 345 (6202), 1340–1343.
Hooper, V., McKissack, J., 2016. The emerging role of the CISO. Bus Horiz 59 (6), 585–591. doi:10.1016/j.bushor.2016.07.004.
Hughes, R., 2010. A treaty for cyberspace. International Affairs (Royal Institute of International Affairs 1944-) 86 (2), 523–541.
Industry Classification Benchmark (ICB), 2018. https://www.ftserussell.com/data/industry-classification-benchmark-icb.
Jessen, M.H., 2012. The state of the company: corporations, colonies and companies in Leviathan. Journal of Intellectual History and Political Thought 1 (1), 56–85.
Joshi, A., Bollen, L., Hassink, H., De Haes, S., Van Grembergen, W., 2018. Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. Information & Management 55 (3), 368–380. doi:10.1016/j.im.2017.09.003.
Kaminski, R.T., 2010. Escaping the cyber state of nature: cyber deterrence and international institutions. In: Czosseck, C., Podins, K. (Eds.), Conference on Cyber Conflict Proceedings 2010. CCD COE Publications, Tallinn, pp. 79–94.
Kangas, A., Kujala, J., Heikkinen, A., Lönnqvist, A., Laihonen, H., Bethwaite, J., 2019. Leading Change in a Complex World: Transdisciplinary Perspectives. Tampere University Press.
Kanniainen, V., 2019. Cyber technology and the arms race. German Economic Review 20 (4), e523–e544. doi:10.1111/geer.12181.
Krahmann, E., 2018. The market for ontological security. European Security 27 (3), 356–373. doi:10.1080/09662839.2018.1497983.
Lanz, J., 2017. The chief information security officer: the new CFO of information security. CPA Journal 87 (6), 52–57.
Limnéll, J., 2016. The cyber arms race is accelerating – what are the consequences? Journal of Cyber Policy 1 (1), 50–60. doi:10.1080/23738871.2016.1158304.
Lloyd, S.A., 2009. Morality in the Philosophy of Thomas Hobbes: Cases in the Law of Nature. Cambridge University Press, Cambridge doi:10.1017/CBO9780511596759.
Lloyd, S.A., Sreedhar, S., 2020. Hobbes's moral and political philosophy. In: Zalta, E.N. (Ed.), The Stanford Encyclopedia of Philosophy, Fall 2020. Metaphysics Research Lab, Stanford University.
Locke, J., 1997. [1690] An essay concerning human understanding. Penguin Books, London [Eng.].
Macpherson, C.B., 1985. Introduction. Leviathan. Penguin Books, London.
McClure, C.S., 2013. War, madness, and death: the paradox of honor in Hobbes's Leviathan. J Polit 76 (1), 114–125. doi:10.1017/s0022381613001072.
Merriam, C.E., 1906. Hobbes's doctrine of the state of nature. Proceedings of the American Political Science Association 3, 151–157. doi:10.2307/3038543.
Mintzberg, H., 1979. The Structuring of Organizations. Prentice-Hall.
Mitzen, J., 2006. Ontological security in world politics: state identity and the security dilemma. European Journal of International Relations 12 (3), 341–370. doi:10.1177/1354066106067346.
Moore, T., Dynes, S., Chang, F.R., 2015. Identifying How Firms Manage Cybersecurity Investment. Working Paper. Southern Methodist University, Dallas, Texas.
Neocleous, M., 2008. Critique of Security. Edinburgh : Edinburgh University Press, Edinburgh.
Nissenbaum, H., 2005. Where computer security meets national security. Ethics Inf Technol 7 (2), 61–73. doi:10.1007/s10676-005-4582-3.
Noonan, L., 2021. Bank of England-backed cyber security war game opens to more companies. Financial Times.
O'Reilly, M., Parker, N., 2013. 'Unsatisfactory saturation': a critical exploration of the notion of saturated sample sizes in qualitative research. Qualitative Research 13 (2), 190–197. doi:10.1177/1468794112446106.
Pasquino, P., 1991. Theatrum Politicum: The Genealogy of Capital - Police and the State of Prosperity. Chicago : University of Chicago Press, Chicago.
Peacock, D., Irons, A., 2017. Gender inequality in cybersecurity: exploring the gender gap in opportunities and progression. International Journal of Gender, Science and Technology 9 (1), 25–44.
Peacock, M., 2010. Obligation and advantage in Hobbes' "Leviathan". Can J Philos 40 (3), 433–458.
Pearlson, K., Thorson, B., Madnick, S., Coden, M., 2021. Cyberattacks are inevitable. is your company prepared? Harv Bus Rev.
Qualitative Data Analysis Software | NVivo, 2021. https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home.
Rai, S., Chukwuma, P., 2019. Ciso – career is surely over? EDPACS 59 (6), 1–4. doi:10.1080/07366981.2019.1617270.
Roach, B., 2005. A primer on multinational corporations. In: Chandler, A.D., Mazlish, B. (Eds.), Leviathans: Multinational Corporations and the New Global History. Cambridge University Press, pp. 19–44.
Rousseau, J.-J., 1968 (1762). The social contract. Penguin Books.
Saldaña, J., 2016. The coding manual for qualitative researchers, 3rd SAGE Publications Ltd.
Shires, J., 2018. Enacting expertise: ritual and risk in cybersecurity. Politics and Governance 6 (2), 31–40. doi:10.17645/pag.v6i2.1329.

Shrobe, H., Shrier, D.L., Pentland, A., 2018. Conclusion. In: New Solutions for Cybersecurity. MIT Press, pp. 477–482.
Silverman, D., 1970. The Theory of Organisations : A Sociological Framework. London : Heinemann Educational, London.
Sims, D., 2005. You bastard: a narrative exploration of the experience of indignation within organizations. Organization Studies 26 (11), 1625–1640. doi:10.1177/0170840605054625.
Singh, A.N., Picot, A., Kranz, J., Gupta, M.P., Ojha, A., 2013. Information security management (ISM) practices: lessons from select cases from india and germany. Global Journal of Flexible Systems Management 14 (4), 225–239. doi:10.1007/s40171-013-0047-4.
Siroli, G.P., 2018. Considerations on the cyber domain as the new worldwide battlefield. The International Spectator 53 (2), 111–123. doi:10.1080/03932729.2018.1453583.
Smith, B., Sparkes, A.C., 2008. Contrasting perspectives on narrating selves and identities: an invitation to dialogue. Qualitative Research 8 (1), 5–35. doi:10.1177/1468794107085221.
Smith, G.M., 2005. Into Cerberus' lair: bringing the idea of security to light. The British Journal of Politics and International Relations 7 (4), 485–507. doi:10.1111/j.1467-856x.2005.00204.x.
Stevens, T., 2016. Cyber Security and the Politics of Time. Cambridge University Press.
Symon, G., Chamakiotis, P., Whiting, R., Roby, H., 2014. Identity work across boundaries in a digital world. In: BAM2014 Conference Proceedings. British Academy of Management, Belfast.
Taylor, J., 2019. Australia's anti-encryption laws being used to bypass journalist protections, expert says. The Guardian.
Thomson, I., 2019. Low Barr: Don't give me that crap about security, just put the backdoors in the encryption, roars US Attorney General. https://www.theregister.co.uk/2019/07/23/us_encryption_backdoor/.
TalkTalk CISO given carte blanche over security investments, 2021. https://www.totaltele.com/492027/TalkTalk-CISO-given-carte-blanche-over-security-investments.
USA PATRIOT Act 2001, 2001.
von Clausewitz, C., 1873. On War. N. Trübner & Company, London.
Walker, C., 2006. Cyber-terrorism: legal principle and the law in the united kingdom. Penn State Law Review 110, 625–665.
Walker, R.B.J., 1993. Inside/outside: international relations as political theory. Cambridge University Press.
Warf, B., Fekete, E., 2016. Relational geographies of cyberterrorism and cyberwar. Space and Polity 20 (2), 143–157. doi:10.1080/13562576.2015.1112113.
Williams, M.C., 1996. Hobbes and international relations: a reconsideration. Int Organ 50 (2), 213–236.
Wolin, S.S., 1970. Hobbes and the Epic Tradition of Political Theory. Los Angeles : William Andrews Clark Memorial Library, University of California, Los Angeles.
Woodward, J., 1965. Industrial Organization: Theory and Practice. Oxford University Press.
Zimmerman, M.J., 2006. Is moral obligation objective or subjective? Utilitas 18 (4), 329–361.
Zmud, R.W., Shaft, T., Zheng, W., Croes, H., 2010. Systematic differences in firm's information technology signaling: implications for research design. Journal of the Association for Information Systems 11 (3), 150–181.

Joseph Da Silva is a part-time Ph.D. researcher within the Information Security Group at Royal Holloway, University of London and is performing multidisciplinary research into the purpose of cyber-security functions within commercial organisations. He works full-time as a Chief Information Security Officer (CISO).