Experts and Markets in Cybersecurity

On Definitional Power and the Organization of Cyber Risks

Willers, Johann Ole

COPENHAGEN BUSINESS SCHOOL
SOLBJERG PLADS 3
DK-2000 FREDERIKSBERG
DANMARK

WWW.CBS.DK

ISSN 0906-6934

Print ISBN: 978-87-7568-047-4
Online ISBN: 978-87-7568-048-1

EXPERTS AND MARKETS IN CYBERSECURITY: ON DEFINITIONAL POWER AND THE ORGANIZATION OF CYBER RISKS

PhD Series 35.2021

Johann Ole Willers

EXPERTS AND MARKETS IN CYBERSECURITY

ON DEFINITIONAL POWER AND THE ORGANIZATION OF CYBER RISKS

CBS PhD School | **PhD Series 35.2021**

CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

Experts and Markets in Cybersecurity

-

On Definitional Power and the Organization of Cyber Risks

Johann Ole Willers

Department of Organization

Copenhagen Business School

Supervisors:

Leonard Seabrooke and Ole Jacob Sending

Johann Ole Willers
Experts and Markets in Cybersecurity:
On Definitional Power and the
Organization of Cyber Risks

1st edition 2021
PhD Series 35.2021

ISSN 0906-6934

Print ISBN: 978-87-7568-047-4
Online ISBN: 978-87-7568-048-1

The CBS PhD School is an active and international research environment at Copenhagen Business School for PhD students working on theoretical and empirical research projects, including interdisciplinary ones, related to economics and the organisation and management of private businesses, as well as public and voluntary institutions, at business, industry and country level.

Abstract

As the digitalization of economies and societies has become seemingly all-encompassing, the governance of cyber risks has evolved into an issue of strategic importance across public and private organizations. Struggling to develop effective responses to this new type of risk, decision-makers operate in an environment of epistemic uncertainty and interdependence. Statements about risks that emanate through cyberspace are not simply representations of objective and observable phenomena. Instead, the diagnosis of cyber risks involves interpretations and judgments. As such, the politics of cyber risk opens the door for professional contestation and competition. How such authoritative understandings are produced is a recurrent concern throughout the separate parts of this dissertation. Concurrently, authoritative understandings of cyber risk demarcate policy options and drive the organization of cybersecurity more generally. As such, processes of diagnosis and treatment are closely entangled. Addressing the definition and organization of cyber risks as interrelated phenomena, I draw on insights from International Relations theory, the Sociology of Risk, the Sociology of Professions, and Science and Technology Studies to advance an analytical framework of embedded social action. In doing so, I highlight the critical role of private actors in shaping the parameters of cyber risk governance across jurisdictional and sectoral domains. This is not to suggest that public actors are irrelevant to these processes. Rather, I underscore how the dual condition of epistemic uncertainty and interdependence has de-monopolized public claims to authority and rendered the functional separation of actor-types on the basis of public-private dichotomies less useful. Experts act as managers of uncertainty and mobilize their claims to authority not only through formal interaction with the state, but through markets and market-like settings. I illustrate variations of this argument across four case studies. First, I emphasize the ambiguous character expert profiles through an analysis of expert committees in Denmark. Second, I document how private actors assert authority over transnational cyber risk issues through skillful framing, alliance-building, and the early mobilization of organizational resources. Third, I explore how representations of cyber risk are inscribed into calculative infrastructures. For this, I turn to an analysis of the cyber risk insurance industry. The final case zooms in on the market for surveillance and intrusion products to illustrate how private actors operate within environments that are enmeshed in geopolitical dynamics and forms of weaponized interdependence.

Dansk Resumé

I sammenspil med at digitaliseringen i stigende grad bliver altomfattende, er håndteringen af cyberrisici blevet et spørgsmål af strategisk betydning på tværs af offentlige og private organisationer. At imødekomme disse nye udfordringer er imidlertid en krævende proces. Et grundlæggende problem er, at cyberrisici er karakteriseret ved epistemisk usikkerhed og systemiske afhængigheder. Cyberrisici, modsat konkrete trusler, kan ikke observeres objektivt. Diagnostiseringen af risici kræver derimod fortolkninger og subjektive vurderinger. Hvordan risici bliver repræsenteret og hvorfor nogle aktører frem for andre opnår definitionsmagten er gentagende emner i denne afhandling. Det handler dog ikke bare om definitionsmagten som et afgrænset fænomen. Definitionen af hvad der er en risiko, reducerer samtidig det operationelle råderum og legitime handlingsmuligheder. Jeg analyserer derfor definitionsmagt og organiseringen af cyberrisici som uadskillelige fænomener. Det kræver et analyseapparat som tager sammenspillet mellem forskelligartede aktører alvorligt. Jeg konceptualiserer dette i form af åbne og gensidigt afhængige systemer, og trækker på teorier om internationale relationer, risikosociologien, professionssociologien, og teknologistudier. På denne baggrund fremhæver jeg, hvordan private aktører kan strukturere og organisere cyberrisici på tværs af sektorer og jurisdiktioner. Dette betyder dog ikke at relevansen af offentlige aktører kan underkendes. Derimod understreger jeg, hvordan epistemisk usikkerhed og indbyrdes afhængighed baner vejen for en kamp om autoritet og definitionsmagt. At forstå denne proces kræver imidlertid et opgør med separationen af offentlige og private aktører på baggrund af deres teoretisk definerede funktioner og handlemuligheder. Eksperter agerer som usikkerhedens forvaltere (’managers of uncertainty’) og mobiliserer deres krav til autoritet ikke kun igennem formelle interaktioner med staten, men ligeledes igennem markeder og markedslignende situationer. Jeg illustrerer dette argument igennem fire casestudier. I det første lægger jeg vægt på ekspert-profilernes tvetydige karakter. I det andet dokumenterer jeg, hvordan private aktører kan opnå definitionsmagten indenfor transnationale cyberrisiciemner ved at kombinere formfuldendt framing, allianceopbygning, og tidlig mobilisering af organisatoriske ressourcer. I det tredje studie udforsker jeg hvordan en midlertidig definitionsmagt kan stabiliseres igennem produktionen af kvantificeringsværktøjer. I denne sammenhæng fokuserer jeg på udviklingen af forsikringsindustrien for cyberrisici. Afsluttende illustrerer jeg, hvordan ekspertmagten varierer når vi bevæger os hen imod klassiske sikkerhedspolitiske emner. Her udfører jeg en historisk analyse af overvågningsmarkedet, som i stigende grad er blevet indlejret i geopolitiske dynamikker.

Acknowledgements

Practitioners of cybersecurity tend to emphasize the importance of partnerships to deal with digital risks, and rightly so. After all, as Bruce Schneier likes to remind us, cybersecurity is a process and not a product. To master the process, you cannot act like an island that is separated from the outside world by a vast ocean. Instead, cooperation and coordination are key. Understanding your strengths is important, and even more so to understand your vulnerabilities. This can be strenuous, and you might need help to create a sense of resilience when navigating stormy waters. At other times, you might be exposed to attack and need to bring in an emergency response team that helps you to get back on track and, most importantly, to learn from the experience. All of this, you cannot do alone. It is a team effort.

Writing a PhD is not so different in many ways, and I was very lucky to be able to draw on an incredible support system throughout the past three years. When I entered the project in the late summer of 2018, I not only entered a new world metaphorically speaking – although I certainly also did that (my prior work had not exactly touched upon issues of digitalization or cybersecurity). I entered a new place quite literally and moved to a new country and a new city. To not only manage but to enjoy this process has much to do with the support that I received from old and new friends, from my family, and above all my partner in life whose enduring support was the foundation of my resilience. For this I will forever be grateful. This dissertation would never have been possible without them.

I am equally grateful to my supervisors that not only entrusted me with a project that I knew little about, but also provided the guidance to help me navigate through the past years. Their thoughts and comments have been invaluable sources of inspiration, and their trust in me has given me strength. In more than one sense, they acted as my ‘managers of uncertainty’ throughout this process. They have been indispensable in helping me to identify my strengths and in dealing with situations of distress and doubt. At other times, they acted as my emergency response team when, for example, another article revision failed to impress the reviewers sufficiently to grant me the desired “accept” in a journal. Thank you for all this, Ole Jacob and Len.

Numerous other people deserve to be mentioned. First and foremost are Lars Gjesvik and Niels Nagelhus Schia who supported me in learning the ins and outs of cybersecurity debates, integrated me at the Center for Cybersecurity at the Norwegian Institute of International Affairs,

and time and again patiently engaged with my premature ideas. Learning about new issues can be difficult and anxiety-provoking. Patryk Pawlak was the first person who really made me belief in my own approach and trust my intuition. I am incredibly grateful to all of you!

Research is always more fun in a team, and I have been privileged to be part of an exciting research project with equally as exciting people. All members of 'The Market for Anarchy' group have at several stages of this process provided enormously helpful comments on my work and offered a temporary escape from my rabbit hole. Beyond my two supervisors and Lars Gjesvik, these people include Eleni Tsingou, Alexander Kentikelenis, Cristiana Maglia, and Elana Wilson Rowe. In this context, I also thank the Norwegian Research Council which has provided funding for this project (#274740). Further, I would like to thank all the people at my two host-organizations for their generous support throughout. In particular, I owe much to the members of the Political Economy Group at CBS and the Security and Defense Group at NUPI. Being part of both has been a source of relentless inspiration and fun. Travelling back and forth between the Norwegian Institute for International Affairs and the Department of Organization at the Copenhagen Business School has proven a great source of academic stimulation and strengthened me in the belief that the worlds of international politics and business are complementary with much to learn from either side.

Finally, I am grateful to the many people that have lent their support throughout – especially those that dedicated their time to comment on my work during the early stages. This relates especially to José Ossandón and Tobias Liebetrau who helped me bring structure to a chaotic piecemeal of loosely articulated ideas at a time when the outlook of a three-year project seemed utterly overwhelming. I also thank Maha Rafi Atal and Daniel Nexon for their invaluable comments on how to bring the individual pieces of my work into a coherent whole during a time when the idea of a three-year project seemed not so much overwhelming but first and foremost way too short. I thank all the organizers of the PhD courses and workshops that I had the privilege to attend. Among them, the memories of the SCANCOR meetings in Mannheim and the GLOBE Winter School stand out. What better way to discuss institutional theory than an evening with Woody Powell in a winery? And I thank Mark Blyth for reminding me that introductory chapters do not have to be boring. I tried.

Table of Contents

PART 1: INTRODUCTION

Experts and Markets in Cybersecurity

In cyberspace, you are only as secure as your weakest link. What is meant by this phrase is that security - or better, the minimization of cyber risk exposure - is an interdependent outcome. The practical significance of this mantra depends on the scale of analysis. At the industry level, it can be understood as an imperative to scrutinize a company's value chain for high-risk suppliers (Bures, 2018). At the level of domestic public administration, it necessitates the identification and regulation of critical infrastructures (Harašta, 2018). At the global level, the strengthening of the weakest link is a key motivation for states to support the build-up of cybersecurity capabilities in third-countries (Pawlak, 2016, p. 85). But what are cyber risks and how can we know about them? Much of the organizational response to this new risk-landscape depends on these fundamental questions and there is no easy answer (c.f. Power, 2007, p. 20). Cyber risks are a muddled category, partly driven by interpretations of evolving threats and partly derived from expectations about the future. In short, cyber risks are open to definitional contests. How these definitions are constructed and how they shape the organization of cyber risks lies at the core of this dissertation.

In addressing these questions, I propose three analytical moves: one methodological, one conceptual, and one theoretical. First, I argue for a divergence from the methodological nationalism (Callaghan, 2010; Wimmer & Glick Schiller, 2002) that has dominated cybersecurity research in the social sciences (Dunn Cavelty, 2015; Dunn Cavelty & Wenger, 2020). Second, I foreground the concepts of interdependence and authority to highlight the interpretive contests – *Deutungskämpfe* – that underlie risk work (c.f. Brettschneider, 2009; Germer, Müller-Doohm, & Thiele, 2013). Finally, I advance a theoretical framework of embedded social action to account for the meso-level politics of cyber risk control (c.f. Seabrooke & Henriksen, 2017). In doing so, I draw on insights from International Relations theory, the Sociology of Risk, the Sociology of Professions, and Science and Technology studies.

First, I move explicitly beyond the analytical fixation on the state that has characterized most of existing literature on cyber risk (Carr, 2016a, p. 50; Dunn Cavelty & Wenger, 2020). Instead, I conceptualize the arenas in which discourses and ideas about cyber risks are developed and enacted as open and interdependent systems (Scott & Davis, 2007, p. 107; see also Seabrooke & Sending, 2015). To that end, I stress the multiplicity of actor types and the loosely coupled

structure through which different aspects of cybersecurity are connected. Analytical focus is directed at private actors. This should not be understood as a rejection of the role of the state for the organization of cyber risks. Instead, it should be understood as a counterweight to the dominance of methodological nationalism in existing research.

Both structurally and operationally, private actors take on important roles within the organization of cyber risk (Eichensehr, 2017, p. 517). Critical infrastructures are largely owned and operated by private actors (Dunn Cavelty & Suter, 2009; Geers, 2009). Digital technologies – and the vulnerabilities ingrained into them - are produced by private companies (Atal, 2021), and public agencies around the world continue to struggle to attract issue-specific cybersecurity expertise (Dawson & Thomson, 2018; Maurer, 2018). Meanwhile, private companies act as entrepreneurs of international norm development (Hurel & Lobato, 2018); technical experts continue cross-border cooperation where traditional diplomacy fails (Tanczer, Brass, & Carr, 2018); and cybersecurity firms produce public attributions of cyber incidents (Egloff, 2020; Eichensehr, 2017). In short, the distinction between public and private actors on the basis of functionally different roles seems to have lost its analytical utility in cyber research (Eichensehr, 2017; Maurer, 2018, p. 152; T. Stevens, 2012). The organization of cyber risks takes place within interdependent relationships that oftentimes are portrayed through the lenses of partnerships between public and private actors (Carr, 2016a, 2016b, pp. 100–107; Eichensehr, 2017). But the significance of interdependence does not simply translate into an imperative for cooperation among various stakeholders at the domestic and global level. Instead, interdependence reshapes the relationships between actor types and offers new opportunities for non-traditional actors to assert control across institutional settings (Farrell & Newman, 2019a, pp. 170–171).

To understand the organization of cyber risks from an open systems perspective requires to take private companies and experts – alongside states, various non-state actors, and transnational professional networks – seriously and refrain from analytical reductionism in which the roles of actors are defined a priori by equating organizational types to forms of authority and agency. Yet, due to the persistent state-centrism in the cybersecurity literature, analytical focus has largely been constrained to situations of public-private engagement in which the state remains the actor *sine qua non*, and the analysis of private actors in their own right has remained a "non-issue" (Dunn Cavelty, 2015, p. 93).

The relative neglect of their roles, mechanisms of influence, and sources of authority in existing research is both curious and troubling. It is curious because their central position is uncontested even in classical International Relations accounts (e.g. Kello, 2017, p. 2), and it is troublesome because it risks turning a blind eye to the myriad of ways through which common understandings of cyber risk are established, how notions of competency are formed, and how these are translated into everyday security practices within and across communities. More generally, recent work on the 'new interdependence' of international relations has argued convincingly how non-state actors can shape global and domestic rules by engaging in processes 'cross-national layering' that impart the 'terms of interdependence' (Farrell & Newman, 2014, p. 333, 2015, p. 499; Johnson, 2016). For all these reasons, "a stronger focus on non-state actors…is now more important than ever (Maurer, 2018, p. 28) and the open systems perspective provides for the methodological foundation to address the messy and sometimes complex processes of cyber risk governance and management.

Second, I draw on conceptual discussions about the entanglements of risk, authority, and interdependence to emphasize the competitive nature of risk construction processes. Cyber risks reflect a distinct category of risk that emanate through cyberspace (Deibert & Rohozinski, 2010, p. 15).[1] These risks are diverse and can loosely be defined in rephrasing Hardy and Maguire (2013, p. 231) as "the potential for realization of unwanted, adverse consequences to human life, health, property, or the environment" on the basis of comprised confidentiality, integrity and availability of digital data and systems (Mukhopadhyay, Chatterjee, Bagchi, Kirs, & Shukla, 2019). Ontological and epistemological uncertainties over the characteristics of cyber risks invite definitional contests over what is real and what is hype, delegating the practice of cybersecurity to a response to perceived risks (T. Stevens, 2015, pp. 2, 155). Within this context, the configuration of skills and competencies that define expert profiles is highly dynamic and open to contestation (Slayton & Clark-Ginsberg, 2018, p. 117): "[Cyber]security is too important to entrust to IT alone" (Hooper & McKissack, 2016, p. 586). This dual characteristic

[1] A second category of cyber risk is concerned with risks *to* cyberspace which relate to the potential failure of the infrastructure that underpins global digital networks. This relates to submarine and fiber-optic cables and other internet 'backbones' such as Internet Service Providers (ISPs), Internet Exchange Points (IXPs). See for example Malecki (2002). This aspect of cyber risks is not addressed in this dissertation.

of epistemic uncertainty and openness, I maintain, is the enabling condition for battles of interpretation to take place.

Third, I argue that this process is best understood within a theoretical framework of embedded social action. The emphasis on embeddedness (Beckert, 2007; Granovetter, 1985) draws attention to the collective social processes through which risk definitions are produced and translated into policies at the unit level (Arena, Arnaboldi, & Azzone, 2010, p. 660). In so doing, I take a dynamic view on social structure and embrace the emerging and ambiguous environment that is characteristic of cyber risk governance (Branch, 2021; Deibert & Rohozinski, 2010, p. 20). Control over risk objects can hence not be declared unilaterally. Instead, those that pursue control projects must operate through - and actively shape - social structures by skillfully creating alliances and acting as guardians over the entanglements of diagnostic and prescriptive representations of risk. How such multi-professional control projects unfold across disparate cases of cyber risk is the main concern of this dissertation. Reflecting these considerations, the guiding research question reads as follows:

> How do experts coordinate and compete for control over the organization of cyber risks?

Throughout the requisite parts of the dissertation, the entanglements of risk, authority and interdependence provide for the undercurrents of discussion to highlight how experts and markets perform central functions in the governance and management of cyber risk. A notable extension of the above research question is therefore the proximate aspect of *who* is in control and *what* profiles are associated with these experts. I hasten to add that what follows is not a cybersecurity analysis proper. I do not make recommendations on the operational or technical level. Rather, I provide analyses about the ways in which understandings of digital risks are shaped, how these understandings structure the organization of risk work (Power, 2016), and how markets and experts play key roles within these processes.

The central argument is that the political significance of cyber risk management derives from the recursive processes through which the diagnostics of cyber risk come to be amplified through open systems of organization and shape shared understandings of what cyber risks are and what should be done about them. The construction of risk perceptions is therefore inseparable from the organizing practices through which uncertainties are managed (Power, 2007, p. 20). Through the integration of insights from International Relations, the Sociology of

Professions, the Sociology of Risk, and Science and Technology Studies, I demonstrate variations of this argument at different levels of analysis and identify the locus of action across institutional contexts, ranging from the seemingly mundane activities of cyber risk assessment practices within insurance markets to the marketization of offensive cyber capabilities.

The remainder of this introductory chapter is structured as follows: In the following section, I provide some background information on the development of digitalization and cybersecurity as interrelated phenomena. Necessarily, this historical account is incomplete and highly simplified. I focus on the sources of digital insecurity, the changing role of states in the production of cybersecurity regimes, and on the growing role of private enterprise in countering 'cyberinsecurities'. Second, I discuss the 'risk problem' of cybersecurity. Here, I provide for a selective review of the cybersecurity literature through a risk lens. From here, I verge towards a discussion of the key concepts – authority and interdependence – that motivate and underpin the analytical focus on expert power and markets. Fourth, the theoretical framework is presented. Fifth, I discuss the methodological considerations. In the final sections, the four articles that make up the main body of this dissertation are presented, and their individual contributions in relation to the research question are discussed.[2]

Case Context: A short primer of cybersecurity

> I think the potential of what the internet is going to do to society, both good and bad, is unimaginable. […] I think we're actually on the cusp of something exhilarating and terrifying.
>
> (David Bowie, 1999)

Today, digital technologies are ubiquitous. Everything – from the organization of public administrations to the configuration of global production systems – is underpinned by digital components, if not based entirely on digital systems. States communicate with citizens through digital platforms and digital technology companies have overtaken the classic industrial and manufacturing conglomerates in importance (Atal, 2021). Since 2018, the majority of the global

[2] For a quick orientation over the separate papers, please consult table 1 on page 33.

population uses the internet on a regular basis (ITU, 2019). Some 20 billion devices were connected to the internet in 2019 (Cisco, 2020). Without a doubt, we are living through another great transformation of economies and societies.

It is worth remembering the *speed* with which this transformation has come about. When David Bowie was speculating about the potential impact of the internet, the ongoing Dotcom bubble had elevated the likes of Yahoo and AOL to the first internet giants and the inflow of investments enabled the consolidation of transatlantic fiberoptic backbones, opening up for new dimensions of communication bandwidth and laying the groundwork for the digital economy (Starosielski, 2015, pp. 45–54). The opportunities seemed limitless, economically as well as socially. Three years prior to David Bowie's quote, John Perry Barlow had asserted the independence of cyberspace from the "Governments of the Industrial World" as a distinct place where privilege and domination would seize to define the terms of interaction and "anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity" (Barlow, 1996). Fittingly, Peter Steiner's cartoon published in the *New Yorker* captured the spirit of this novel social space in the depiction of a dog sitting in front of a computer, lecturing a smaller dog sitting on the floor: "On the internet, nobody knows you're a dog" (Fleishman, 2000). The shared idea, of course, was that as long as cyber*space* remained distinct and cut off from the physical world, it could be freed from the constraints that defined social life. Wealth, geography, identity – all this would not matter in cyberspace, where people finally would be set free.

It should, of course, not be long before states would reassert their dominant position in the digital domain and make the internet an extension of power and politics (Klimburg, 2017; Nye, 2010). Indeed, Barlow's manifesto was published in response to the US Telecommunications Act of 1996 that brought the internet into telecommunication regulations.[3] In the following years, international efforts multiplied to address challenges arising from this new technology. France (in 1996) and Russia (in 1998) proposed international treaties at the OECD and United Nations respectively (Lewis, 2017; Macak, 2017, p. 880). While both proposals gained a modest

[3] Earlier provisions such as the Computer Fraud and Abuse Act of 1986 had extended law enforcement competencies into digital matters but remained limited in that it criminalized the intentional alteration, damage and destruction of digital data without extending law enforcement powers to police online content (White House, 2009, pp. C–11). This was what title V of the Telecommunications Act was criticized for (Bennett, 2016).

response, the year of 1998 marked the start of recurrent and intensifying debates over cyber-related issues at the United Nations (United Nations, 1999). Perhaps more significant even, the ratification of the Convention on Cybercrime in 2001 reasserted the role of states in the digital domain, mandating amongst others the development of digital surveillance capabilities in the fight against digital crime (Council of Europe, 2001). Barlow's vision had been surpassed by reality and the state was back for good.

The reality, certainly, was that what has come to be known as *the* internet always has been a project with heavy state involvement. From the 1960s when Larry Roberts and DARPA built the ARPANET, connecting UCLA, the Stanford Research Institute, the University of California, Santa Barbara, and the University of Utah (Weinberger, 2017, p. 220; Weiss, 2014) to the development of the first internet protocols in the 1970s and 80s at MITRE and DARPA, public organizations were at the very heart of defining the underpinnings of modern connectivity (Mazzucato, 2011).

Far from being a historical curiosity, the importance of this early work lives on today as the building blocks of the early protocols of the 1970s have endured through several updates. This is significant insofar as the protocols were designed to facilitate the speed and reliability of information flows (Carr, 2016b, pp. 48–49, 78–79). Today's glaring need for security could not be anticipated at that time. Consequently, security was not - and is neither today - an in-built feature of the networks that we collectively call the internet (Dunn Cavelty, 2015, p. 92; Singer & Friedman, 2014). As the internet expanded in scope and scale, this design flaw would increasingly take on a terrifying dimension.

The interconnectivity of the internet scaled the transmission rates of self-replicating code across operating machines. The 1988 Morris worm was the first to drive this message home. Written with an intention to showcase security flaws in the Unix mailing system, the worm spun out of control, replicating excessively and almost caused the early internet to collapse (Libicki, 2009, p. 45). Adding intent to the threat, the so-called AIDS Trojan of 1989 encrypted files on victims' computers and asked for money to undo the damage – the first known ransomware attack (Bates, 1990). During the 1990s, digital attacks on computers increased in frequency and provided a sense of urgency to address the issue (Sanger, 2018). The title of John Arquilla's and David Ronfeldt's 1993 groundbreaking report reflected this *Gestaltshift*: "Cyberwar is Coming!" (Arquilla & Ronfeldt, 1993). While the question as to the whether cyberwar indeed

was – or was not – coming remained a point of contention (Clarke & Knake, 2010; Rid, 2012), state and non-state actors started to prepare for a new reality of cyber-enabled conflict and insecurity, and in the process vibrant markets for cybersecurity ensued (Singer & Friedman, 2014, p. 162 ff.). Curiously, the rise of global cybersecurity markets was mirrored by markets for cyber*insecurity*, monetizing on vulnerabilities in digital code and developing the tools that law enforcement and intelligence agencies around the world began to rely on to probe digital systems (Deibert, 2013; Deibert & Rohozinski, 2011; Maurer, 2018; Perlroth, 2021).[4]

During the 2000s, government agencies in the United States instigated the development and acquisition of offensive cyber tools (Kaplan, 2016; Perlroth, 2021). Russia started exploring the use of cyber-enabled proxy warfare in Estonia and Georgia (Greenberg, 2019). China begun exploiting digital vulnerabilities for industrial espionage on an enormous scale (Carr, 2016b, pp. 93–95; Kaplan, 2016). And somewhere along the line, the Iranian nuclear enrichment facilities in Natanz became the target of the world's first cyberweapon. The Stuxnet worm manipulated the industrial command and control systems of the nuclear facility, causing centrifuges to rotate at harmful speeds and causing significant damage to the Iranian nuclear program (Zetter, 2015). While the operation likely prevented an armed attack by the Israeli forces, it also set a dangerous precedent for the world: digital weapons were a new reality and the US had made it clear that it was willing to make use of this new power (Sanger, 2018). Cyberspace had become the fifth domain of warfare alongside land, air, sea and space – although it should take until 2016 before the leading global military alliance NATO would officially recognize it as such (Jacobsen, 2021). In the years to come, cybersecurity simultaneously moved "upwards in the political agenda and expanding sideways as a problem area to a multitude of additional policy domains" (Dunn Cavelty & Wenger, 2020).

Throughout this development, concerns about grand scale cyberwar would gradually be replaced with constant low-level engagement that increasingly blurred the lines between public and private, crime and espionage, and offensive and defensive action (Buchanan, 2020; Jensen, Valeriano, & Maness, 2019). While seemingly everybody became less secure throughout this process, the responsibility to act became more widely dispersed. States – as the classical

[4] Article 4 of this dissertation presents a detailed historical account of these markets.

providers of security – could not prevent attacks against the privately-owned critical infrastructure and much less so against private actors in general (McCarthy, 2018).

As the societal and economic impact of cyberattacks continued to escalate, cyber-related damage has become a key business risk (Allianz, 2019; Petersen & Christensen, 2017). Cyber-attacks and large-scale data thefts have consistently ranked among the top-5 global risks in the World Economic Forum's annual Global Risk Reports between 2017 and 2020 (World Economic Forum, 2019). Yet, business leaders struggle to implement risk management processes (PwC, 2018) and public administrations are pressed to hire qualified personnel (Domscheit-Berg, 2020). Facing an opaque, complex, and highly uncertain potential danger, the crucial question became how to identify, understand and act upon digital risks (Reichborn & Friis, 2016, pp. 37-38). But what is risk in cybersecurity, and how does it relate to other issue areas for which risk has become a key organizing principle?

The (cyber) Risk Problem

> Can we know the risks we face, now or in the future? No, we cannot: but yes, we must act as if we do.
>
> (Douglas & Wildavsky, 1982, p. 49)

It is a truism that risks have become a defining factor in driving global politics (Beck, 1992) and organizational management (Power, 2007). The problem to act and organize in the face of risk is thus everything but a unique challenge to cybersecurity. "Cyberspace", Deibert and Rohozinski asserted as early as in 2010, "represents a special category of risk" (2010, p. 15). Within this line of argument, cyber risks represent an extension of wider institutional dynamics in which risks have become "more global, less readily identifiable, more problematic, less easily managed, and more anxiety-provoking" (Gephart, Van Maanen, & Oberlechner, 2009, p. 142). They are "invisible potential danger[s], the seriousness of which the layperson's unaided senses cannot judge" (MacKenzie, 2001, pp. 8–9). Because risks thus defined transgress traditional notions of controllability and calculative rationality (Hardy, Maguire, Power, & Tsoukas, 2020), "[t]he world risk society needs experts to tell it what it should fear" (Krahmann, 2011, p. 356).

This recognition of *expert authority* in the wider literature has resulted in a small but significant body of research within cybersecurity. For example, work in the tradition of securitization theory has famously described the security grammar of cybersecurity as "securitization plus technification", where "[t]he strong emphasis on the hypothetical in cyber securitizations create a particular space for technical, expert discourse" (Hansen & Nissenbaum, 2009, p. 1166). Some work highlights how the technical nature of this work shields experts from external pressures. For example, technical expert communities have been shown to facilitate international cooperation on cybersecurity and engage in 'science diplomacy' largely unconstrained from international rivalry and disputes (Tanczer et al., 2018). Others have documented how technical complexity has afforded individuals that operate through powerful organizations with significant leeway over the formulation of international norms (Kessler & Werner, 2013).

A related body of research has placed emphasis on the "hypothetical" element of professional cyber risk discourses and highlighted the propensity of cyber experts to inflate risk representations (Brito & Watkins, 2011; Lee & Rid, 2014; Quigley, Burns, & Stallard, 2015; Talesh & Cunningham, 2021). Stevens, for example, underscores the prevalence with which cybersecurity communities stress the extraordinary and revolutionary character of the current historical epoch, and concludes that cybersecurity imaginaries are "dominated by dystopian visions of the future" (T. Stevens, 2015, p. 101). In making this diagnosis, he expands on the technical and hypothetical character of risk discourses and accentuates the uniqueness of cyber risks through an exploration of the speed and acceleration that characterize digital developments. Cyber risks are "collapsing traditional notions of space and distance" (ibid., p. 74).

Technical complexity, uncertainty, and the speed of change are thus the standard characteristics that drive cyber risk work into the hands of expert communities. Understood as a specific kind of systemic risk, cyber risks resemble the structural features of global financial risks and climate change that operate within interdependent and complex environments (IRGC, 2018, p. 12). While all these risks place enormous stress on decision-makers (Dunn Cavelty, 2007, p. 18), the 'time-space compression' of cyberspace amplifies this dynamic and gives particular leeway to expert politics and risk work (c.f. Jacobsen, 2020; Malone & Malone, 2013; T. Stevens, 2015, p. 91).

As such, the cyber risk industry provides for the management of uncertainty. It would, however, be overtly simplified to describe this process as 'anything goes' in which the most blatant and inflated risk perceptions can be marketized. In following Dean, what is important is less the risk itself than the conditions – forms of knowledge and heuristics – that make risks *thinkable* (Dean, 2016, p. 25). That is, processes of risk construction rest on the successful representation of risks as real. The prime task of the risk builder is therefore to forge consensus positions through which risk objects are controlled and rationalized. "Knowledge", in Beck's words, "gains a new political significance" (Beck, 1992, p. 23). But what qualifies as cyber expert knowledge is contested (Christensen & Petersen, 2017; Shires, 2018). While recent scholarship has emphasized how experts operate in 'communities of practice' to construct common narratives (T. Stevens, 2012, 2015, p. 155) and employ distinct rhetorical techniques (Quigley et al., 2015), the construction of cybersecurity knowledge has largely remained a non-issue (C. Stevens, 2020, p. 131).

A notable exception is a body of research that has investigated the role of cybersecurity companies in publicly attributing cyberattacks and producing public knowledge about cyberinsercurities (Egloff, 2020; Eichensehr, 2017; Lupovici, 2016; Maschmeyer, Deibert, & Lindsay, 2021; Rid & Buchanan, 2015; C. Stevens, 2020). This work has significantly contributed to – albeit oftentimes implicitly - our understanding of how cyber risks are *diagnosed* and *inscribed* by private actors that operate through security markets (c.f. Krahmann, 2011). What is oftentimes missing from these accounts is a recognition of the dynamic and oftentimes contested configurations of knowledge, expertise and authority that define the political character of knowledge production (Slayton & Clark-Ginsberg, 2018, p. 117). My contention is that such work requires a conceptual and analytical framework that takes authority seriously and accounts for the interdependent processes through which cyber risks become objectified (c.f. Hilgartner, 1992). In the following sections, my attempt at such a framework will be presented.

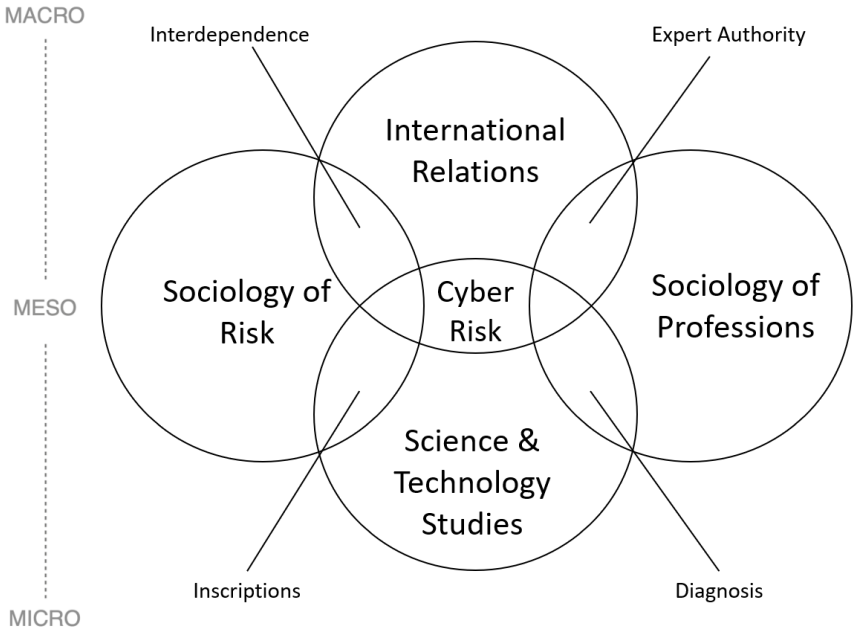


Figure 1: Analytical Framework

Conceptual Considerations

Throughout the previous sections, I have argued that the technical and inherently uncertain character of cyber risks provides a privileged position for experts to lay claims to authoritative expertise. These control projects take place within interdependent and open systems that provide for variation in terms of what types of actors matter and what strategies prove to be successful. Figure 1 illustrates this conceptual collective and locates the vantage point of risk work at the meso-level that connects macro level dynamics of interdependence and epistemic uncertainty with the micro-level activities of diagnosis and inscription. While the structural characteristics of cyber risk work in terms of interdependence (e.g. Geer, 2018; Geer, Jardine, & Leverett, 2020; Nye, 2011) and expert authority (e.g. Hansen & Nissenbaum, 2009; Quigley et al., 2015; Shires, 2018) are routinely acknowledged in the cybersecurity literature, little systematic attention has been devoted to them. My contention is that this is a mistake and that some basic conceptual clarifications have much to offer. This is what I turn to now.

Expert Authority

Authority is arguably a foundational concept to the social sciences. With its etymological origin in Roman law and Greek political philosophy, authority is sharply contrasted from coercion and pure persuasion (Arendt, 1954, pp. 8, 17–21, 29). Conceptually, it is typically understood as a form of power that is perceived to be legitimate (Hurd, 2007; Kustermans & Horemans, 2021), implying a form of "obedience in which men retain their freedom" (Arendt, 1954, p. 9). The driving force of authority is thus deference, in which the acceptance of a decision (and the decision-making process implicit to it) is derived from the characteristics associated with the source of that decision (Zürn, 2018, p. 38).

This is an important qualification for the exercise of expert control over risk objects. As I argued in the previous section, the construction of risk-perceptions around a given object naturally lends itself to contests over the authority to diagnose and treat risks. The deference view of authority stresses how these control projects are embedded within relational processes in which authority is not declared unilaterally but derived from the recognition of others (Sending, 2015, 2017). It is because of this recognition - whether it derives from tradition, charisma, or rational-legal sources (Gerth & Mills, 1977, pp. 295–300) - that the words of authoritative actors carry weight. In following Mommsen (1888, p. 1034), authoritative statements are "more than advice

and less than a command, an *advice which one may not safely ignore*"[5] (cited in Arendt, 1954, p. 18, emphasis added).

In situations of firmly established authority structures, authoritative advice may not be ignored *safely* due to the social sanctioning that follows from it and the resulting erosion of one's own social position (see also Hall, 1997, pp. 601–602; Kustermans & Horemans, 2021, p. 14). When the institutionalization of authority structure is weak, however, restrictions to participation in the decision-making process are eased and competition for authority turns into a key driver of the political process (c.f. Sending, 2015, p. 4). Not surprisingly, current conceptual debates about authority are largely concerned with transnational decision-making processes.

Famously, Haas popularized the concept of epistemic communities to draw attention to the political significance of professionals with an authoritative claim to policy-relevant knowledge (Haas, 1992). The power of epistemic communities would derive from their *control* over uncertain knowledge within a given domain. Because the issues of international and global politics are increasing both in scope and complexity, states would rely on the *epistemic authority* of expert groups for the ordering of preferences and as the providers of 'instruction sheets' to translate structural dynamics into strategic interests (Blyth, 2003; Matthijs & Blyth, 2018). The novelty in Haas' approach was a recognition of how control over contested knowledge claims can shape actor preferences and structure policy-outcomes in the international arena, but it remained rather limited in explaining how the authority of epistemic communities comes about and what mechanisms actors employ to gain control over contested knowledge claims (*see also* Sending, 2015, pp. 15-16).

Unpacking these consensus-building processes over epistemic control requires a closer investigation of the *cognitive authority* that underpins epistemic communities (Lidskog & Sundqvist, 2015, p. 5). For Broome and Seabrooke (2015), actors engage in what can be described as battles of interpretation not only based on the shared normative and causal beliefs that characterize their membership in an epistemic community in the classical sense, but equally so by drawing on professional experience and the privileged access to information that such a career entails (p. 959). Especially for emerging and ambiguous issue-fields, the ability to draw

[5] Quote in original: „In diesem Sinne ist *auctoritas* mehr als ein Rathschlag und weniger als ein Befehl, ein Rathschlag, dessen Befolgung man sich nicht füglich entziehen kann, wie ihn der Fachgelehrte dem Laien, der Führer im Parlament seinen Anhängern ertheilt".

on multi-faceted knowledge and to mediate between professional communities can serve as important explanatory mechanisms for the construction of consensus positions and the epistemic authority that follows from it (Seabrooke, 2014).

In sum, I have argued that the inherent uncertainty of risk work (Power, 2016) provides a natural extension of expert power to define, categorize and legitimate degrees of riskiness (Amoore & de Goede, 2008, p. 13) with significant effects on the organization of socio-economic systems (Fourcade & Healy, 2017). While expert power in uncertain and ambiguous environments has long been recognized (Beck, 1992; Giddens, 1991), the transnational nature of risk objects in 'late modernity' amplifies opportunities for knowledge actors to coordinate and compete for control in opaque and complex environments that provide ample opportunity to act across and beyond established hierarchies (Henriksen & Seabrooke, 2021). In Power's words, this dynamic "suggests a new kind of organizing authority for the category of risk (Power, 2007, p. 4). I identify the authority to speak about the unknown (Hansen & Nissenbaum, 2009, p. 1167) as a sought after and contested quality. Striving for the recognition of others, heterogenous actors mobilize resources and engage in 'interpretive battles'. Control over interpretations – *Deutungshoheit* - can be asserted using a wide range of resources and tools but it ultimately rests on the recognition of others and cannot be asserted unilaterally (Black, 2017). The battle for Deutungshoheit is thus a process of embedded social action that operates within open and interdependent systems.[6]

Interdependence

I have previously argued that expert struggles for control over risk definitions are best understood within a context of open systems that breaks with the methodological nationalism which has characterized much of cybersecurity scholarship. In this section I expand on this point through a conceptual discussion of interdependence.

Interdependence and digital vulnerabilities are the "twin facts" that have shaped the evolution of cybersecurity and the problems that are associated with it (Nye, 2011, p. 24). Due to the interconnective character of cyberspace, decisions taken in one place have ramifications in

[6] Importantly, I mean not to imply that expert power is the only thing that matters. Other forms of power – including political, geopolitical and military – can under certain conditions take precedence.

others. This is the basic condition of interdependence (Farrell & Newman, 2014, p. 332). For example, when cybercrime goes unpunished in one jurisdiction, it has ramification in others (Peters & Jordan, 2020). When suppliers do not have adequate security practices in place, their risk exposure reflects on the risk profile of lead firms (Windelberg, 2016). More fundamentally, interdependence derives from the underlying technologies through which global networks are pinned together, most prominently in the form of fiber-optic and submarine cables (Malecki, 2002). Control over network hubs has been associated with panopticon effects that exploit interconnectedness and extend state control beyond borders (Farrell & Newman, 2019b, p. 55; Segal, 2017, p. 153). A second perspective stresses how market concentration in the digital technology sector is both amplifying forms of interdependence and shaping it (Drezner, 2021; Geer et al., 2020).

Risk work in the context of cybersecurity therefore operates within multifaceted forms of interdependence across scales of analysis. On the one hand, it reflects broader trends towards the internationalization of domestic security that necessitate cooperation across borders and actor-types (Farrell & Newman, 2019a). On the other hand, digital vulnerabilities create (and are created by) dependencies across economic sectors as for example in the case of the cyber risk insurance industry. The cyber insurance industry both depends on and has the potential to affect the decisions of technology giants, cybersecurity companies and policyholders (Talesh, 2018). This dual characteristic of transnationality and trans-sectorality creates forms of complex interdependence (Keohane & Nye, 2012, pp. 20–21) that activate political processes of contestation, and reshape power relations between actors (Farrell & Newman, 2019a, p. 6).

While interdependence therefore can have significant ramifications for state power, it also serves as an enabling condition for state and non-state actors to shape global and domestic institutions. From this perspective, norms and rules are not the sole outcome of inter-state bargaining. Rather, interdependence creates opportunity structures through which actors can operate beyond international and domestic settings and work through transnational regulatory forums (Farrell & Newman, 2015, p. 502). Transnational organizing allows for the formation of alliances across national jurisdictions to develop consensus positions and challenge existing institutional orders.

Despite the dominant focus on established institutional arrangements within this literature, similar tendencies of transnational organizing can be observed within the organization of cyber

risk which is largely characterized by emerging and nascent institutional orders (Egloff, 2017; Eichensehr, 2015; Liebetrau & Christensen, 2020; Raymond & DeNardis, 2015). Microsoft's attempt to advocate for international cyber norms by acting through existing, and by establishing new, transnational forums is a case in point (Hurel & Lobato, 2018; Macak, 2017). The work of the Internet Governance Forum is another (Flyverbom, Deibert, & Matten, 2019), and examples abound.[7]

What is important for the purposes of this dissertation is that the global nature of cyberspace perpetuates forms of interdependence that facilitate the governance of cyber risks through open systems of organization that operate both within and across jurisdictions. Work within the literature on 'new interdependence' underscores how rules and norms that govern behavior are embedded within social systems that include, but by no means are limited to, public actors. Further, with its stress on the importance of 'collective actors' this literature provides for an important supplement to the notion of expert authority and locates expert power beyond the unitary actions of individual "professional entrepreneurs" (c.f. Stone, 2019). Finally, the perspective stresses the need to investigate variation across institutional settings, and to underscore how domestic, international and transnational organization feeds into each other (Farrell & Newman, 2015, p. 518, 2019a, p. 18). Building on these insights, the following section provides for a discussion of how the structural characteristics of interdependence and epistemic uncertainty relate to the micro-level activities of risk work. I propose that such work is defined by processes of diagnosis and inscription, and I advance an analytical framework on the basis of embedded social action to study these processes.

[7] The Cybersecurity TechAccord should be mentioned as well as the Charter of Trust for a Secure Digital World and Google's proposed legal framework for "digital security and due process". Other initiatives, such as the Paris Call or the Global Forum for Cyber Expertise operate on a mixed membership basis, including states, international organizations, private companies, civil society organizations and knowledge actors.

Analytical Framework: Diagnosing and Inscribing Cyber Risk

Because understandings of risk are produced in fragmented and uncertain environments, and because the ability of individuals and organization to act upon these risks is conditioned upon interdependent social processes, I have argued that the organizing processes underlying risk work need to be understood in terms of embedded social action. Classically, Granovetter popularized the concept of embeddedness as a critique of the 'atomized' decision-making models of mainstream economics (Granovetter, 1985, p. 486) and emphasized how the capacity of individuals to act is contingent on their network position (Callon, 1998, p. 9). For emerging and unsettled issues, stable network positions are not available. For an analysis of cyber risks, I therefore argue for a conception of embedded social action that goes beyond an explanation of social outcomes on the basis of network structures and I attune analytical focus to the question of how social structures emerge and are shaped (c.f. Beckert, 2007).

In doing so, I direct analytical focus on processes of diagnosis and inscription. For the former, I draw on Abbott's Sociology of Professions and Fligstein's Theory of Fields. For the latter, I borrow insights from Science and Technology Studies.

Diagnosing Cyber Risk

Abbott's classical work on the sociology of professions employs a systemic approach to the social organization of expert knowledge and focuses on the political character of knowledge construction (1988, p. xii). Professional turf battles over control and jurisdictions are fought within an interdependent system in which tasks do not fall naturally to any professional group (ibid., p. 122). As technological and organizational changes bring about new problems and tasks (ibid., p. 92), professional groups engage in collective struggles to lay claims to jurisdictional control. Through processes of inference, diagnosed problems are linked to treatments, providing dominating professions with the power to define the nature of problems, limit appropriate actions, and outline success criteria (ibid., p. 137).

The important contribution of Abbott's classical approach is thus less that control over knowledge implies power but rather that "control without competition is trivial" (ibid., p. 2): "Where there is advice today, there was conflict yesterday or will be conflict tomorrow" (ibid., p. 76). The vantage point for an analysis of the social organization of knowledge is therefore the

object of professional conflict (i.e. tasks) and the focus of analysis is *how* organized social actors operate within the constraints of the social system to face competitors and lay claims to jurisdictional control (ibid., 325). The approach is hence well-situated to critically approach a fundamental question about expert authority on cyber risks, namely: Who is the cyber expert? For a long time, it was assumed that cybersecurity would fall quite naturally within the profile of IT professionals, providing the underlying rationale for a security grammar of 'technification' (Dunn Cavelty & Egloff, 2021). Yet, proclamations of such a natural alignment between tasks and groups were simplified at best. Instead, the control over cybersecurity problems and risks remains contested and Abbott's classical approach provides the tools to identify the parameters of such competition.[8]

While I therefore argue for the continued relevance of this foundational approach to study expert competition on emergent issues, there are obvious weaknesses. Although professions remain important collective social actors for the organization of societies and economies, their hegemonic position as 'lords of the dance' (Scott, 2008) should not simply be asserted before the fact. The propensity of professions – defined here as exclusive occupational groups with abstract knowledge (Abbott, 1988, p. 8) – to act from a position of hegemony vis-à-vis other social actors should instead be subject to empirical evaluation. That is, organizational actors might engage in professional projects to control tasks and diagnose problems in addition to, and in competition with, formal professions within a context of *linked ecologies* (Abbott, 2005).

Linked ecologies designate shared social spaces in which control over issues is determined by the ability of actors to create alliances across previously distinct groups that share an interest in, and come to interact through, a focal object.[9] From this perspective, professions, epistemic communities and other collective actors co-exist in "a complex system of ecologies, competing and collaborating over who has jurisdiction over particular tasks and activities" (Farrell & Quiggin, 2017, p. 270). To produce settlements, actors attempt to build alliances across ecologies through *hinges* or through the colonization of competing ecologies by replicating

[8] I expand on the promises and limitations of Abbott's system of professions framework in the first article (published in Danish, "Hvem er Cybereksperten?". See also the section "Presentation of Articles" in this chapter.

[9] The linked ecologies approach is employed in the third article to study processes of inscription-building within the cyber insurance industry.

logics of diagnosis, inference and treatment into new ecologies (Abbott, 2005, p. 255). An example of the former is how macroeconomic policy has served as a hinge to build coalitions across academia and policy-makers (Seabrooke & Tsingou, 2021, p. 311). Avatar strategies, on the other hand, can be exemplified through the expansion of the economics profession into adjacent fields of business knowledge and international development policy (Fourcade & Khurana, 2013; Stone, 2013).

The diagnosis of problems within a context of linked ecologies resembles therefore an interdependent process that operates through logics of domination (avatars) and cooperation (hinges) across and within collective actors that are linked together through focal objects. Contrasting this rather narrow view of social embeddedness, the strategic action field (SAF) approach employs the metaphor of the Russian doll to emphasize how social spaces are nested within each other and thus fully embedded (Fligstein & McAdam, 2012, pp. 9, 59–61; Liu, 2021, pp. 129–130). As I document in the second article of this dissertation, the approach is well-positioned to study policy-problems that are both charged with coordination problems among heterogenous actor types and enmeshed into forms of interdependence (Fligstein, 1997, p. 398; Fligstein & McAdam, 2012, p. 58).

SAFs designate meso-level social orders that are defined by shared understandings about the purposes, power relationships, and rules of the field (Fligstein & McAdam, 2012, p. 8).[10] Social action takes place within and across fields from which actors use social skill to access resources and influence how the field operates (ibid., p. 59, 172). The SAF approach relies thus on a twofold conception of embeddedness: First, an embeddedness into the macro structure through an understanding of SAFs as variously connected to proximate and distant fields that provide for resource- and information flows (ibid., p. 18). Second, an embeddedness of social action within the meso-level in which microlevel interaction always is constrained and enabled through the social position of actors within the respective SAF (ibid., pp., 11, 48, 89).

Similar to the linked ecologies perspective, control over the diagnosis and treatment of problems is a collective endeavor in which skilled social actors seek to motivate cooperation in others (Fligstein, 1997, p. 398). Through the strategic framing of common agendas, skilled actors are

[10] The SAF approach is employed in the second article to study how global public (cyber-) policy issues emerge within nested fields and how shared understandings of problems and tasks are actively shaped through framing contests and strategic alliance-building.

pivotal for the stabilization of social orders (Fligstein, 2001, p. 116). However, because Fligstein insists on the dual role of positioning and framing as the constitutive building-blocs of social order, the approach turns a blind eye to the material underpinnings through which authority structures and social hierarchies are inscribed and stabilized. As I argue in the third article, this tends to disregard how diagnostic logics are being inscribed into calculative devices that act simultaneously as stabilization mechanisms and as strategic tools to be used for the creation and cementation of actor-coalitions.

Inscribing Cyber Risk

The intimate relationship between problematizations and inscriptions is a common observation within science and technology studies. Classically, Hilgartner proclaimed that "representations of risk get *built into* technology and shape its evolution" (Hilgartner, 1992, p. 39). The processes through which problematizations come to be represented through distinct technologies, frameworks, rankings, or benchmarks result in inscriptions of risk (Robson & Bottausci, 2018). However, because inscriptions only reflect a specific representation of risk objects, they act as much as illuminators as they conceal underlying conflicts and areas of contention (Latour, 1987, p. 246, 1999, p. 304). That is, on the one hand, inscriptions link problems to tasks and make complex problems known (c.f. Robson, 1992, p. 689), while simultaneously 'blackboxing' the politics of inscription-building (Callon, 1998). In Mackenzie's words, they act as "engines", translating abstract representations of risk objects into instruction sheets (MacKenzie, 2006).

It is precisely this tension between the performative quality of institutionalized inscriptions in prescribing action, and the competitive struggle that is characteristic of periods of inscription-building that drives my analysis. The context of inscription-building in cyber risk is asymmetrical in that the pervasiveness of risk is portrayed as universal ("everybody is at risk") while the supply of self-proclaimed and variously certified cyber experts is scant. Scripts that 'make cyber risks known' and prescribe appropriate actions are thus highly desired. I investigate this process in the context of cyber insurance underwriting and document how quantified representations of riskiness begin to define the evaluation criteria of cybersecurity practices.

The significance of inscriptions for processes of risk construction and organization is, however, not confined to their potential performative character. Rather, the process of inscription-building itself represents a crucial vector for the creation and stabilization of professional hierarchies (c.f.

Quattrone, 2009, p. 89). Not dissimilar from the multi-professional competition over professional jurisdictions and issue control within sociological work on professions, inscription-building is a process of alliance-building within embedded social spaces. In following Callon (1980, p. 198), what is at stake in these processes are not solely status battles but questions of control over the subsequent allocation of tasks. 'Inscriptors' (Qu & Cooper, 2011) strategically engage in the construction of proto-inscriptions through the creation of 'communities of interest' (Latour, 1987, p. 112). However, this is a two-way process insofar as inscription-building and alliance-building are interdependent processes. On the one hand, inscriptions reflect the interests of collective inscriptors, and on the other hand, proto-inscriptors use processes of inscription-building to forge strategic alliances across otherwise disconnected social spaces.

Throughout the subsequent articles, cyber risk diagnostics and inscriptions are addressed concurrently and represent the microlevel underpinnings of expert authority and interdependence that characterize the institutional environment through which cyber risks are defined and acted upon. The emphasis on each of these elements varies, however. Figure 2 locates the four articles in the context of these four guiding themes.

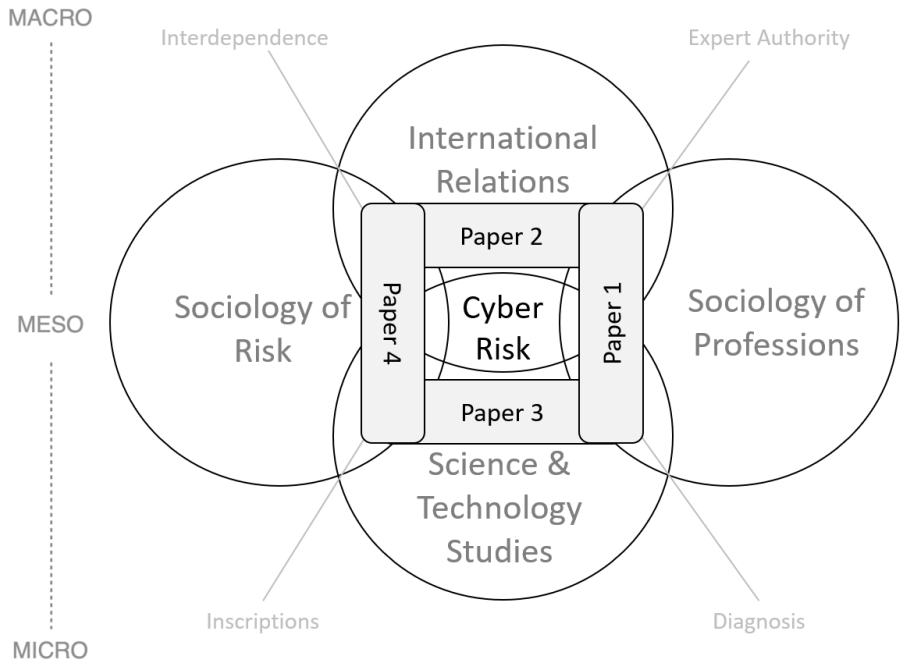


Figure 2: Locating case-studies in the analytical framework

Methodological Considerations

Throughout the previous sections, I have advanced an understanding of cyber risk that emphasizes the social construction of risk representations in a nexus of expert authority and interdependence. Because both the prefix *cyber* and the suffix *security* in cybersecurity are ambiguous concepts, and because the dangers to which cyber risks discursively are connected remain opaque, definitional contests are open to diverse stakeholders. Much of the uncertainty surrounding cyber issues is linked to its emergent qualities. This has not only to do with the relative recency with which the topic has gained widespread attention. It is equally the result of the speed and acceleration that characterize the very conjecture of digital society (T. Stevens, 2015): Cybersecurity develops at the speed of technology (Galinec, Možnik, & Guberina, 2017; Slack, 2016). This intensity translates, not surprisingly, to what might be called the 'high-paced rhythm' of cybersecurity knowledge (c.f. Abbott, 2005, p. 254): A constant need to 'stay ahead of the curve' (Talesh, 2018, p. 12) and an ever-looming threat to even the lightest of settlements. This is not simply a challenge for practitioners of the field, it equally translates into a thought-provoking task for cybersecurity research in general, and for research about cybersecurity experts in particular.

What I have been striving for is a form of 'enlightened eclecticism', allowing for pragmatic choices and the combination of diverse empirical materials while remaining conscious about how the different methods relate to each other and ensuring their methodological compatibility (Wolf, 2010, p. 151). Employing an explorative and case-driven design, I searched for variance in the Realpolitik of cyber risk representations and control. Figure 2 illustrates how the chosen cases relate to the theoretical and conceptual considerations discussed throughout the previous sections, and how they approach different loci of action.

The prime strength of an explorative research design is to approach emerging issues with an open mind and using flexible methods (Stebbins, 2001). It allows to identify and to accentuate social patterns through processes of abductive reasoning (Finnemore, 2003, p. 13), in which empirical observations and theory are in constant conversation to produce *plausible* explanations for observed phenomena (Jackson, 2011, pp. 82–84):

> Like the fictional detective, Sherlock Holmes, a researcher who uses abductive reasoning, constantly moves back and forth between new and prior data, as well as developing knowledge or theories, and makes comparisons and interpretations in the search for patterns and the best possible theoretical explanations.
>
> (Charmaz, Thornberg, & Keane, 2017, p. 734)

Rather than theory-building per se, I pursue a process of *theorizing* that is located within a 'context of discovery' (Swedberg, 2016, p. 6). Throughout my work I do not develop theory in the strict sense – that is, a theory that is context independent, complete and predictive (Flyvbjerg, 2001, p. 39). Instead, I employ a methodological framework designed to provide plausible explanations for the 'why and 'how' of expert control in cybersecurity. The resulting process of discovery unfolds not simply within the individual articles but also across them (c.f. Stebbins, 2001, pp. 2–17). The arrangement of articles in the dissertation reflects how this process unfolded. In line of succession, the articles address four different cases on the basis of new questions and insights gained from previous work.

Case studies are in-depth investigations of broader phenomena that can provide concrete and context dependent knowledge (Flyvbjerg, 2011). They are "cases of *something*" (Moses & Knutsen, 2012, p. 132). The centrality of context to case studies accommodates the examination of interdependent processes of structure and agency that span levels of analysis (Byrne & Callaghan, 2014, p. 257; Schwandt & Gates, 2018, p. 592). On a fundamental level, the selected case studies are deviant cases in that they deviate from the state-centric logic that has dominated cybersecurity research (Lijphart, 1971, p. 692). They highlight how non-state actors are important not simply because they are the ones that carry out the tasks defined by public authorities but because they can be involved in the ontologically prior processes of problem definition and preference formation. In their individual contribution, the selected cases go, however, beyond this basic premise and address critical issues within their respective domain (Flyvbjerg, 2011, p. 307). The following section expands on this point and discusses the selection of cases as presented in figure 2 in more detail.

Operationalization and Case Selection

Cyber risks are vast, almost ubiquitous. Approaching the research question of how risk representations are created and disseminated through markets and market-like settings necessitated the identification of sub-areas that promised interesting insights into mechanisms of expert control. This process evolved over time in light of data gathered and new issues emerging (Schwandt & Gates, 2018, p. 593).

The first case concerned the relationship between expert authority and processes of cyber risk diagnosis. A fundamental issue in this context has to do with the nature of cyber experts. If it is true that expert profiles remain as opaque as the risk work of cybersecurity itself (c.f. Shires, 2018), a closer investigation was warranted. Expert committees provide a direct link between the work of experts at the micro-level and the macro-level phenomenon of expert authority (Stone, 2003, p. 50). Abbott's classical sociology of professions suggests that control over new tasks comes to be absorbed by individual professions that claim exclusive jurisdiction over the diagnosis, inference and treatment of problems (Abbott, 1988). To test whether such jurisdictional claims could be deduced from occupational values as Abbott's work would suggest, I analyzed the composition of expert groups as a proxy to identify patterns of expert control. For the empirical setting, I chose Danish expert committees. Because Denmark is among the most digitized countries in the world and also among the most "cyber safe" (e.g. Bischoff, 2021), the analysis of Danish elite cyber experts is likely to reflect key dynamics in other high-capacity countries (Flyvbjerg, 2001, p. 74).

The second case moves away from a simple depiction of expert profiles and verges towards an investigation of how actors assert control over cyber risk issues in a context of interdependence. Research on transnational governance indicates that expert control tends to be the most pronounced in 'thin' institutional environments that are characterized by weak and overlapping formal mandates (Faulconbridge & Muzio, 2012; Henriksen & Seabrooke, 2016; Quack, 2007; Seabrooke & Tsingou, 2015). Concurrently, research that focuses on new forms of interdependence within International Relations scholarship points towards how rule overlap equally can operate as a constraint for actors with limited access to transnational forums (Farrell & Newman, 2015). Given this ambiguous character, an investigation of cyber risk governance at the transnational level promised some interesting variation in how multi-professional *Deutungskämpfe* unfold. The case of cybersecurity capacity building (CCB) presented itself as

an obvious choice. Here, global cyber risks are addressed through the transfer to, and build-up of, capabilities in low-capacity countries. But which risks should be addressed, how these risks are distributed, and what exactly should be done about them is subject to continuous negotiation. Because the process of CCB is actively encouraged by donor countries and international organizations in order to address the macro-variant of the weakest-link problem outlined in the opening to this introductory chapter, private actors operate within a field of heavy state-involvement and must navigate the politics of interdependence (Pawlak & Barmpaliou, 2017). As I show in the article, this constraining condition does not negate the possibility for private actors to achieve diagnostic authority and shape the formation of best practices and routines through careful alliance-building and strategic investments during periods of field formation.

Third, I address processes of diagnosis and inscription-building as interrelated phenomena. This theme emerged tacitly in the analysis of the previous case and warranted further exploration. A rich tradition within science and technology studies suggests that inscriptions act as stabilizers of uncertainty and ordering-mechanisms (Jordan, Mitterhofer, & Jørgensen, 2018; MacKenzie, 2006; Muniesa, Millo, & Callon, 2007; Themsen & Skærbæk, 2018). An issue of particular salience in the management of cyber risk is the development of quantified risk statements (Jones, 2019). To understand how the development of such calculative devices hinges upon professional settlements, the cyber insurance industry was chosen. With a long history of quantifying risks (Callon & Muniesa, 2005; Jordan et al., 2018) and an urgent need to develop technologies for the valuation and categorization of cyber risks (Biener, Eling, & Wirfs, 2015), the industry seemed ideal to delve into the politics of inscription-building (Power, 2015; Qu & Cooper, 2011).

While the previous cases provided ample evidence that markets and experts are critical to the definition of and response to cyber risks, their analytical focus remained on areas that only qualify as security issues in a broad sense. That is, they apply to aspects of societal security and transnational cooperation. For the fourth and final case, I turn to an empirical investigation of how private actors and their perceptions of risk operate within environments that are deeply enmeshed into forms of weaponized interdependence (Farrell & Newman, 2019b). The objective, therefore, was to illustrate the perspective in the context of a case that lies at the core of international security concerns: The proliferation of offensive cyber capabilities. As such this final article builds upon the insights gained from previous articles and applies them to the

market for ‘cyber*insecurity*’ through which offensive cyber capabilities are disseminated worldwide.

For the practical operationalization of the research, the cases were addressed individually. While the respective methods and data-sources were chosen in response to the specific context of the individual cases, all articles relied on combinations of multiple methods including interviews, document analysis, participant observations and descriptive quantitative analysis. This openness to a variety of data sources is one of the main strengths of a case-driven research design. It requires, however, a careful approach to data analysis. Triangulation is a way to deal with this challenge. In its basic form, triangulation refers to “the combination of methodologies in the study of the same phenomenon” (Norman K Denzin, 1970, p. 291; Flick, 2018, p. 765). In navigating qualitative multi-method research, data triangulation is a way to learn from different empirical sources to gain a deeper knowledge about the object of interest. It involves a pragmatic combination of methods to identify emerging patterns and areas of contestation including reflections about how to explore these issues further (Flick, 2018, p. 773).

Methods

When I entered the project in late summer of 2018, I approached the topic of cybersecurity with a blank slate. The early phase of the doctoral project was thus dedicated to learning the ins and outs of cybersecurity debates, trying to identify areas of contention and always with an eye to the profiles of those who led the debates. Within this context, the early empirical strategy should be understood as a reflection of this learning process. Data collection during this phase was focused on building a foundation to prepare me for the subsequent phases of systematic data collections on specific issues and topics within the wider research environment. The most important sources of information during this early stage were the ‘classics’ of the field. That is, the books and research articles that had gained extraordinary standing as signified by, for example, their number of citations and the social position of the author. I also visited cybersecurity conferences of various types including technical and more policy-oriented ones. This proved helpful to gain an initial impression of what kind of ‘actor communities’ existed within the field, how they related to each other, and what issues stood out as important.

As I began to identify issues for further exploration, I adapted more strategic data collection strategies. Despite some variation across the individual articles of this dissertation, the approach

usually revolved around the sourcing of information from written materials, interviews, and participant observations. A close reading of the literature would typically be the first step, followed by an initial sampling of interview candidates and selection of possible venues for participant observations. Once I would feel confident to move on from the initial round of desktop research, the use of data sources would become more integrated. Interviews would for example at times result in the identification of new and hitherto overlooked documents. At other times, participation in conferences or online events would point me to new interviewees. Concurrently, triangulation was also a means to ensure the robustness of my work in that it allowed to test initial findings and to subject emerging explanations to repeated trials of strengths (c.f. Latour, 1987, p. 79). This integration of research methods in the practical operationalization of the research strategy is important to keep in mind when I discuss the methods individually in the subsequent sections. For all primary data gathered, important aspects considered were: who is speaking, what audience are they speaking, what position are they advocating, and what is the context of the utterances.[11]

Documents, literature, and other written sources

The reading of relevant literature is a common and oftentimes trivialized first entry into new fields of study. Its critical position in shaping research questions and subsequent selections of appropriate methods should, however, not be underestimated. As such, close readings of the academic literature, official documents, industry reports, and newspaper articles were a central aspect of my 'polymorphous engagement' with issues of interest (Gusterson, 1997, p. 116). This centrality was not limited to initial phases of desktop research. Rather, the continuous reading and re-reading of documents served as a critical component for the contextualization and critical assessment of new insights gathered elsewhere (Hinchman & Moore, 2013).

The sampling of 'relevant' literature followed a structured and intuitive approach, starting with a sourcing of academic literature through inter alia the Web of Science on the basis of keywords. Academic work was ordered according to two criteria: number of citations and date of publication with an inverse relationship between the two. That is, the more recent the

[11] A similar approach can be found within process-tracing (George & Bennett, 2005).

publication, the less citations necessary to qualify for the initial sampling (Liñán & Fayolle, 2015). After this structured entry-point to sampling, I would allow for some intuition in expanding the 'relevance' category on the basis of emerging points of contention and frequent referrals to individual practitioners or organizations within the texts. During later stages, this broadening would equally be informed by information gathered during interviews.

Interviews

Qualitative semi-structured interviews have taken a central role throughout the research process to explore how interview partners experience issues of interest, what opinions they have, and how they perceive their own roles in the constitution of certain phenomena (Kvale, 2007, pp. 7–9). Three aspects are important in this respect: First, the sampling of interviewees. Second, the types and purposes of conducted interviews, and finally the approach to data analysis.

First, interviewees were generally sampled in a purposive manner to ensure that the central actors are included (Tansey, 2007, p. 769). The selection of interviewees was thus the result of prior analysis. For initial rounds of interviews, the analysis of documents was used to identify informants. This would include authors of central reports from international-, industry-, and other organizations, and individuals that would be referred to in these documents. During later stages of the data collection process, the sampling would allow for the incorporation of insights from participant observations and referrals from prior interviews in the form of snowballing techniques, which oftentimes proved helpful to gain access to otherwise unreachable interview partners and to compensate for limited information derived from participant observations and document readings (Davies, 2001).

Second, given the interest in expert dynamics and control, interviews were conducted with high-ranking individuals within their respective organizations or the wider field. Such elite interviews require that the researcher must enter the conversation with a certain level of knowledge about the status-quo and current debates within the community (Kvale, 2007, p. 70). Consequently, I often opted for an initial round of informative and factual interviews with local informants (Kvale, 2007, pp. 71–72). The purpose of these interviews was to establish the accuracy of basic understandings and to prepare me for subsequent stages of elite interviews. As I moved up the 'packing order', focus was increasingly placed on the narratives that interview partners would advance and the oral history and recollection of key events (Bornat, 2004).

Third, the nature of elite interviewing is that the interviewee typically occupies a social position that far exceeds that of the interviewer. This is particularly pressing when the interviewer occupies a junior position, as is the case for every doctoral student. In such a situation, the establishment of trust was the primary precondition to gain useful and novel information. Partly, this could be achieved through meticulous preparation. I, however, quickly learnt that recorded interviews resulted in less useful information and I opted therefore for an alternative strategy in which I would take detailed handwritten notes during the conversation and transform these into memos as soon as the interview had ended (Roulston, 2014). In the memos, I recorded the main elements of the conversation and, using a separate section, reflections on what new topics emerged and how these could be incorporated into further analysis. Whenever I encountered particularly interesting remarks during conversations, I would try to write them down immediately and intervene after the interviewee had finished his/her thoughts to ask whether this could be used as a quote. As a general rule, potential quotes were subsequently sent by mail to the interviewee to provide consent for further use. In practice, I conducted 46 formal interviews that directly informed the four articles and numerous background interviews that were not directly used for the article writings. Oftentimes, follow-up mails were exchanged to clarify statements and reflect on new findings.

Participant observations

Participant observations allow the researcher to "participate[..] in the daily life of the people under study, either openly in the role of researcher or covertly in some disguised role" (Becker & Geer, 1957, p. 28; Richardson, 2003, p. 259). As such, it is an exciting method to escape from the cleaned and carefully crafted sterility of published documents and experience the "vicissitudes of translation" first-hand (Richardson, 2003, p. 123). Here, the community can be experienced 'in action' across dispersed sites (Gusterson, 1997, p. 116). Three issues need to be addressed in the context of participant observations: Venue selection, form of participation, and data utilization.

First, two forms of participant observation were conducted. As mentioned above, I participated in conferences during the early stages of the doctoral training to gain an overall impression of different cybersecurity communities. These observations did not require much preparation. They were solely designed to gain experiences, explore and, if possible, identify interesting people

and issues. In short, these observations served as familiarization (Nicholls, Mills, & Kotecha, 2013). The second form of participant observations was more strategic and conducted in the context of concrete research projects. These typically followed initial rounds of desktop research and represented a second round of data gathering during which information from interviews, documents, and participant observations would come into conversation with each other. The venues would typically resemble conferences and sometimes (especially during travel restrictions) online seminars and workshops. Venues were selected using one or more of the following three strategies: First, venues emerged from interviews. This happened either in the context of interview preparations where the interviewee was listed as a keynote speaker or discussant for upcoming events, or the information emerged during the interview itself. Second, conferences and workshops would be held by organizations that emerged as central during initial rounds of desktop research. Third, and more rarely, new venues of interest would emerge during the participant observation itself.

The second issue to discuss is the form of participation. This is unusual but necessary given the implications of the corona pandemic that have defined large parts of the dissertation-writing. Because of prolonged travel restrictions, in-person participant observations were limited to the first one and a half years of research. For the remaining part, observations were limited to online conferences, workshops, seminars etc. Obviously, this limits the utility of the approach because large parts of information are derived from the informal mingling and conversations that happen outside of the main venue hall. On the other hand, many conferences moved online, and the number of seminars and workshops exploded, providing otherwise unimaginable access to expert discussions across the world.

Naturally, the implications of online versus in-person participations had ramifications for the gathering and utilization of data. For in-person events, I would take handwritten notes during the day and sometimes record thoughts on the phone. During evenings, I would translate these notes and audio files into detailed memos. Importantly, reflections that resulted from the memo-writing could oftentimes be followed up on during the next day. This was of course not possible for online events. However, online events also have advantageous. Oftentimes, sessions would be recorded so that I could note interesting sequences and go back later to re-watch them. Further, many events allowed for Q&A sessions that proved very useful to test initial findings and explore issues of interest further.

In total, in-person participant observations have taken me to several countries, including Poland, the Netherlands, Norway and Ethiopia, with a further trip to South Africa being canceled last minute due to the beginning pandemic. Online events allowed for participation in events held in the U.S., U.K., Belgium, Canada, Germany and more. While the effects of the pandemic therefore clearly had some drawbacks, they also allowed for far broader participant observations than initially planned.

To sum up, the methodological framework reflects core conceptual concerns about the contested nature of risk representations and accommodates the analytical focus on embedded social action which derived from the theoretical framework. Employing a case-driven exploratory research design, I attend to the contextual and temporal factors that are crucial for investigations of diagnostic and inscription-building processes. The multi-method approach to data collection reflects the oftentimes emerging and opaque social structures that characterize the organization of cyber risk, and it proved critical in the process of bringing empirics and theory into conversation.

#	Title	Key Concern	Setting & Methods	Key argument	Theory	Target Journal
1	Who is the Cyber Expert? Expertise and professions in cybersecurity (Single-authored)	What types of expert profiles are associated with elite cyber risk professionals, and how do these profiles reflect dominant perceptions of risk?	Expert Committees. Analysis of 176 professional backgrounds and careers, and review of industry reports	Elite cyber experts tend to be characterized by hybrid profiles that allow for the translation of technical knowledge into policy- and business-relevant domains. This reflects the rise of a resilience logic and the demise of preventive security logics.	Sociology of Professions (Abbott, 1988)	***Økonomi & Politik*** (published)
2	Seeding the Cloud: Consultancy Services in the Nascent Field of Cyber Capacity Building (Single-authored)	How is expert authority negotiated in transnational cyber forums?	Transnational admin-istration of cyber capacity building. Participant obser-vations, interviews	Although transnational cyber risks are enmeshed in interdependent structures, private actors play decisive roles as managers of uncertainty and architects of diagnostic consensus positions.	Global Public Policy; Strategic Action Fields	***Public Administration*** (published)
3	Linked ecologies for inscription-building in unstable markets: The emergence of cyber risk insurance (Co-authored)	How are inscriptions of cyber risk constructed and stabilized?	Cyber risk insurance industry. Interviews, Participant Observations	Inscription-building is a fragile recursive process that hinges on professional settlements. Because cyber risks are not controlled by any one professional group, settlements are negotiated between ecologies.	Linked Ecologies; Science and Technology Studies	***Accounting, Organizations and Society*** (Under revision)
4	The Globalization of the Surveillance Industry (Co-authored)	How are cyber risks monetized in markets for cyber*insecurity*?	Historical analysis of digital surveillance and interception markets. Interviews.	States have little choice but to rely on private actors for the provision of intrusion and interception tools. But the largely intangible products defy traditional mechanisms of control. The result is a globally operating market that is simultaneously enmeshed in forms of weaponized interdependence and acts as a key vector for the proliferation of cyber weapons.	Historical Analysis; International Relations	***International Security*** (Submitted and rejected after first round of reviews). Currently under revision for resubmission at ***International Studies Quarterly***

Table 1: Dissertation Papers

Outlook of the Dissertation

The four articles of this dissertation reflect variations of expert control across empirical settings that span different loci of action. The first article focuses on the relation between micro-level professional profiles and institutionalizations of expert authority. The second article focuses on the organization of cyber risk governance at the transnational level. The third article zooms in on processes of multi-professional coordination at the industry level, and the final article illustrates the perspective through an investigation of how industry-level dynamics defy jurisdictional boundaries. As such, the four articles can either be read individually in light of their individual contribution to cybersecurity research or collectively in light of how they successively build on each other.

Article 1: Professions and expertise in cybersecurity

Informed by the classical work in the sociology of professions, the first paper of this dissertation provides for an investigation of expert profiles in public and private Danish cybersecurity expert committees. Based on an analysis of 176 professional backgrounds and a close reading of the relevant literature, it is argued that the profile of cybersecurity experts has moved away from a purely technical focus to a process orientation which is both broader in scope and closer to the decision-making level. The new expert profile is positioned at the intersection of technical, organizational and economic rationality, reflecting a move away from preventive security logics and towards resilience paradigms (Dunn Cavelty, Kaufmann, & Søby Kristensen, 2015). The organization of cyber risks within such an approach requires a holistic and continuous approach to risk mitigation. Cyber risks are presented as opaque and evasive. Everybody is constantly at risk and the best response is to elevate cyber risk management to a strategic level that is tightly integrated into all aspects of organization. Consequently, authority over cyber risks has dispersed from the *techne* of IT professionals and is increasingly bound up with the recognized ability to generate and operationalize processes around permanent cybersecurity risk (c.f. Amoore & de Goede, 2008). This recognition, I argue, hinges critically on the ability to bridge between professional ecologies. These findings add to, and are in line with, existing research on the changing role of corporate cybersecurity information officers and highlight the rising importance of effective communication in asserting expert authority over cyber risks (Hooper & McKissack, 2016).

Article 2: Framing contests and the temporality of authority structures

The second article builds upon the previous findings and expands on the communicative underpinnings of expert authority. Bringing the sociology of risk and sociology of professions into conversation, this article investigates multi-professional coordination at the transnational level and asks how authority structures are discursively constructed and maintained through framing contests. Based on an analysis of the nascent field of cybersecurity capacity building, I document how emerging institutional structures provide rich opportunity for strategic actors to advance particular framings of risks and assert their own competency as indispensable for the resolution of governance problems. While the social skill perspective emphasizes how prevailing actors employ superior communicative strategies, the findings of this paper equally document how such processes cannot be understood detached from a resource perspective of organizational mobilization.

Although the strategic framing of risks is a core component of alliance-building between disparate actors that operate in contexts of interdependence, authoritative actors draw on organizational resources to link theoretical assertations of knowledge claims with strategic and forward-looking action. To do so effectively, I argue, private actors invest into the production of global claims to best practice and link these with a claim to competency 'on the ground'. This linkage between the global and the local is subsequently employed to not only mediate interests of interdependent actors but to actively shape them. To do so during periods of field emergence requires, however, a distinct organizational form that provides for the ability to operate with relatively long investment horizons. Such investments include a range of pro-bono work and the deployment of manpower across geographies to identify gaps and to act on opportunity structures. Global professional service firms, I argue, are in an advantageous position to navigate this institutional environment and act early on emerging opportunities. They 'seed the cloud' to benefit from the field as it matures.

Article 3: Stabilizing risk representations through inscription-building

While the second article focused on the emergence of authority structures, this third article asks how authoritative representations of cyber risk become institutionalized. The previous analysis showcased how best practice guides stabilized actor positions and linked risk definitions to appropriate mitigation strategies. In this article, I reflect on these processes through the lenses of

science and technology studies and zoom in on the production of ‘calculative infrastructures’. Because the effective communication of cyber risks oftentimes is impeded by the difficulty to navigate across disparate knowledge actors, a particularly salient issue in cyber risk governance is the challenge to find a common language through which risks can be communicated effectively. This process, I theorize, relies fundamentally on the identification of common risk definitions and the translation thereof into widely recognized metrics. That is, the process of inscription-building is at its core about the standardization of risk representations and turning what is fluid and ambiguous into stable and concrete forms. This translation, I argue, not only stabilizes representations of risk. It equally stabilizes jurisdictional claims and professional hierarchies.

Through an analysis of the cyber risk insurance sector, I highlight how the inscription of cyber risks into standardized and seemingly objective evaluative infrastructures is a recursive process that hinges on professional settlements and is subject to continuous re-calibration. Such professional settlements are, however, also subject to what I elsewhere have referred to as the ‘high-paced rhythm of cybersecurity knowledge’. That is, the dynamic and fast-moving cybersecurity threat landscape creates continuous ‘trials of strength’ (Latour, 1987, p. 79) that probe the objective character of risk representations and spark recursive cycles of professional coordination and contention. This tension intensifies as new inscriptions prioritize the lightness of communication over the complexity of the inscribed phenomenon. The quantification of cyber risk is the epitome of this process and illustrates the dual character of inscription-building for cyber risk, being both highly desired and fragile.

Article 4: Cyber risk markets and the new interdependence

The final article builds upon two insights from the previous articles and locates private authority within dynamics of international security. First, the second article highlighted that private actors can assert authority in fields that are marked by high levels of interdependence and strong state involvement. Second, the previous article indicated the close entanglement of risk representations and organizational responses to risk. Crucially, such dynamics were documented to operate across jurisdiction with the potential to disseminate risk management practices through the market rather than through legislation. Through a historical analysis of the market for surveillance and intrusion products, this final article investigates how these processes operate

when private actors are entangled into forms of weaponized interdependence. That is, how do dynamics of private authority change when the locus of action is reversed? Contrary to the cyber risk insurance industry and the wider markets for cybersecurity capacity building, the effects of private authority over the dissemination of offensive cyber capabilities threaten to undermine the global security landscape through escalating proliferation dynamics. Drawing on extensive historical data, interviews, and an empirical analysis of 5973 product demonstrations, trainings and seminars, the article documents the emergence, consolidation and globalization of private authority over the provision of digital surveillance and intrusion products. It is documented how private actors initially gained authority because states saw no alternative to the private provision of digital surveillance and intrusion technology. As the market became more profitable, firms invested into product innovation and tried to shield themselves from competitive pressures. The result was a form of private authority over the provision of cyber*insecurity* products that is increasingly undermining the security objectives of leading states. While regulative efforts have been initiated to reassert public authority, the market proves resilient, indicating how private authority structures are difficult to challenge once they are institutionalized.

Discussion and Contributions

Addressing the critical issue of private authority over the definition and organization of cyber risks, I make three overarching contributions: First, drawing on insights across academic disciplines and spanning the sociology of risk, international relations, the sociology of professions, and science and technology studies, I introduce a new analytical framework to the study of cybersecurity issues within open and multifaceted environments. Second, I introduce the concept of *Deutungskämpfe* to account for the emergence of authority structures in the context of risk work, and I foreground how this process is underpinned by struggles over the diagnosis and inscription of risk objects. Third, the thus introduced perspective has opened for important empirical and practical contributions that provide new insights into administrative and organizational aspects of cyber risks across levels of analysis. I quickly expand on each of them in the following section before I conclude.

Cybersecurity has evolved into an issue of strategic importance for individuals, organizations, and states alike. The organization of cyber risks responds, however, not simply to objective and observable dynamics against which actors weigh their interests and develop rational responses.

The diagnosis of cyber risks involves interpretations and judgements. Cyber risk experts manage uncertainty and this process is open to professional contestation. Because cybersecurity has not, and likely will not, become provided by the state, the organization of cyber risks operates within open systems. Within open systems of organization, multiple actor-types navigate loosely coupled structures through which cybersecurity issues are connected. Crucially, the shape and form of connections are subject to constant re-negotiation and contestation. The institutional environment within which the organization of cyber risk takes place is therefore defined by openness and interdependence with the latter deriving from the systemic character of cyber risk in which actions in one place have ramifications for others. Given this context of actor-multiplicity and interdependence, it is appropriate to speak of the politics of cyber risk governance, implying contestations over the identification and organization of cyber risks.

The centrality of private actors in these political struggles remains underspecified in existing research for at least two reasons. First, a sizeable tradition of cybersecurity research locates the politics of cyber risk solely within and across nation states (Dunn Cavelty, 2015; Liebetrau & Christensen, 2020). Within these perspectives, it is states that respond to the opportunities and dangers of a new interconnectedness by organizing risks through the development of national strategies and capacities. While these processes oftentimes involve cooperation and coordination with the private sector, the perspective remains centered on the primacy of the state to define both the means and ends of such cooperative action. This is what I have referred to as methodological nationalism. Second, a related body of research has emphasized how cyber risks are organized within models of multistakeholderism. While this work explicitly recognizes the structurally and operationally central role of private actors to deliver on the mitigation of cyber risks, it systematically underplays the political character of multi-stakeholder interaction. Relying on a Habermasian conception of communicative action as necessarily consensus seeking (Flyvbjerg, 2001, p. 92), work in this tradition has neglected political struggles among disparate actors whose interests might not align (Raymond & Denardis, 2015).

I therefore contribute to cybersecurity research by advancing an analytical framework that is grounded within an open systems perspective and places center-stage processes of authority construction among interdependent actors. In doing so, I locate cyber risk work at the meso-level and emphasize how the politics of cyber risk are embedded within wider social processes. From this perspective, the definition and organization of cyber risk is shaped by the collective

actions of individuals and organizations that coordinate and compete over shared notions of competency and jurisdictional control.

As a second contribution, I introduce the concept of *Deutungskämpfe* to unpack how such collective struggles unfold in the nexus between risk and professional control.[12] Deutungskämpfe roughly translate to "battles of interpretations" and allude to the social processes through which uncertainties are discursively objectified (Brettschneider, 2009, p. 192). While the term oftentimes is used in the context of heated public debates, I maintain that the currency of interpretative battles is deference and that the 'battle' metaphor alludes more to the political meaning of the word than to full-blown civil war.[13] As such, I use the concept to highlight the specific dynamics of authority structures in the context of risk work and emphasize the critical position of definitional power for the organization of risk objects. Because participation in the Deutungskampf is not confined to actors with formal mandates, it is equally well-positioned to account for the contested nature of expert authority that I have argued to be typical for risk work. I document how such authority derives from a mediating capacity in which the translation of technical knowledge into policy- and business-relevant domains is valued highly. Further, I document how the discursive formation of authoritative risk representations is underpinned by acts of alliance-building that hinge both on social skill and the mobilization of organizational resources. Brokerage between sparsely connected social spaces is in this context a more effective strategy to gain interpretative authority than guardianship that seeks to shield risk work in one domain from the dynamics in the wider environment.

Finally, I make several practical and empirical contributions. Among these, I draw attention to the mechanisms through which cyber risks are organized and document the meso-level politics that drive these processes. At the transnational level, I document how the multi-stakeholder approach to cyber risk governance is embedded within structures in which states and private actors not only interact on the premise of 'partnerships'. Instead, I contend that the social space of interaction increasingly resembles market-like characteristics for which the functional separation of actor-types into public and private categories becomes less useful. The

[12] The salience of the concept in the subsequent chapters varies, but it has been central to the overall thinking and development of the individual articles.

[13] Habermas (1979, p. 21) famously referred to such interpretative battles as the "paramilitary operations at the frontlines of semantic civil-wars" (quoted in Germer et al., 2013, own translation)

significance of this dynamic stems from the constraints that it places on the regulative capacity of states to unilaterally dictate rules and norms about cybersecurity practices. However, the same dynamic allows states to 'punch above their weight' when they embrace the new opportunity structures and skillfully build alliances across public and private actors to develop norms and standards of appropriate behavior. For private actors, this dynamic equally represents opportunity and constraint simultaneously. While those with access to transnational forums, recognized expertise and global networks have ample opportunity to monetize on cyber risks and create new markets, those that lack these qualities are less likely to move beyond the role of rule-takers.

Concluding Remarks

This dissertation emphasizes the centrality of experts and markets for the definition and organization of cyber risks. The subsequent contributions should therefore be understood as both counterweight to the hitherto dominance of state-centric approaches and as illustrations of a new methodological and analytical framework. In no way do I mean to imply that the importance of nation states should be disregarded. Instead, I hope to make compelling arguments for a perspective that does not prioritize the power and authority of individual actor types a priori. The following four articles foreground how cyber risks can, under certain circumstances, empower non-traditional actors to define the parameters of organization in the face of cyber risk and how these practices can shape the wider cybersecurity landscape across domains. The four corresponding cases were chosen to illustrate this perspective. Without a doubt the results might change for other aspects of cyber risk. This dissertation is therefore necessarily incomplete. Further research is needed to systematically locate patterns of variation in the degree of expert authority on issues of cyber risk. Nonetheless, I hope that this dissertation can serve as useful inspiration for further research.

References

Abbott, A. (1988). *The System of Professions - An Essay on the Division of Expert Labor*. Chicago: The University of Chicago Press.

Abbott, A. (2005). Linked ecologies: States and universities as environments for professions. *Sociological Theory*, Vol. 23, pp. 245–274. https://doi.org/10.1111/j.0735-2751.2005.00253.x

Allianz. (2019). *Allianz Risk Barometer - Top Business Risks for 2019*. Retrieved from https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf

Amoore, L., & de Goede, M. (2008). *Risk and the War on Terror*. London: Routledge.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society*, *35*(7), 659–675. https://doi.org/10.1016/j.aos.2010.07.003

Arendt, H. (1954). What is authority? In *Between Past and Future* (pp. 91–141). New York: The Viking Press.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141–165. https://doi.org/10.1080/01495939308402915

Atal, M. R. (2021). The Janus faces of Silicon Valley The Janus faces of Silicon Valley. *Review of International Political Economy*, *28*(2), 336–350. https://doi.org/10.1080/09692290.2020.1830830

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace | Electronic Frontier Foundation*. Retrieved from https://www.eff.org/cyberspace-independence

Bates, J. (1990). Trojan horse: AIDS information introductory diskette version 2.0. *Virus Bulletin*, 3–6. Retrieved from https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf

Beck, U. (1992). *Risk society: Towards a new modernity*. London: SAGE.

Becker, H., & Geer, B. (1957). Participant observation and interviewing: A comparison. *Human Organization*, *16*(3), 28–32.

Beckert, J. (2007). The Great Transformation of Embeddedness - Karl Polanyi and the New Economic Sociology. *MPIfG Discussion Paper*, *07*(1), 1–25.

Bennett, R. (2016, February 10). The legacy of Barlow's cyberspace declaration of independence | American Enterprise Institute - AEI. Retrieved September 21, 2021, from AEIdeas website: https://www.aei.org/technology-and-innovation/telecommunications/legacy-barlows-cyberspace-declaration-independence/

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *Geneva Papers on Risk and Insurance: Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Bischoff, P. (2021, March 24). Which countries have the worst (and best) cybersecurity? Retrieved August 20, 2021, from Comparitech's Annual Report: Which countries have the worst (and best) cybersecurity? website: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

Black, J. (2017). "Says who?" liquid authority and interpretive control in transnational regulatory regimes. *International Theory*, *9*(2), 286–310. https://doi.org/10.1017/S1752971916000294

Blyth, M. (2003). Structures Do Not Come with an Instruction Sheet: Interests, Ideas, and Progress in Political Science. *Perspectives on Politics*, *1*(04), 695–706. https://doi.org/10.1017/S1537592703000471

Bornat, J. (2004). Oral history. In C. Seale, G. Gobo, J. F. Gubrium, & D. Silverman (Eds.), *Qualitative research practice* (pp. 34–47). London: SAGE.

Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization*, *75*(1), 39–70. https://doi.org/10.1017/S002081832000051X

Brettschneider, A. (2009). Paradigmenwechsel als Deutungskampf: Diskursstrategien im Umbau der deutschen Alterssicherung Author(s): *Sozialer Fortschritt*, *58*(9/10), 189–199.

Brito, J., & Watkins, T. (2011). *Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy* (No. 11–24). Retrieved from http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-

Broome, A., & Seabrooke, L. (2015). Shaping policy curves: Cognitive authority in

transnational capacity building. *Public Administration*, *93*(4), 956–972. https://doi.org/10.1111/padm.12179

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

Bures, O. (2018). Contributions of private businesses to the provision of security in the EU: Beyond public-private partnerships. In O. Bures & H. Carrapico (Eds.), *Security privatization: How non-security-related private businesses shape security governance* (pp. 23–49). Cham, Switzerland: Springer.

Byrne, D., & Callaghan, G. (2014). *Complexity Theory and the Social Sciences*. https://doi.org/10.4324/9780203519585

Callaghan, H. (2010). Beyond methodological nationalism: How multilevel governance affects the clash of capitalisms. *Journal of European Public Policy*, *17*(4), 564–580. https://doi.org/10.1080/13501761003673351

Callon, M. (1980). Struggles and Negotiations to Define What is Problematic and What is Not: The Sociologic Translation. In W. A. Schwartz, K. D. Knorr, R. Krohn, & R. Whitley (Eds.), *The Social Process of Scientific Investigation* (pp. 197–220). https://doi.org/10.2307/2068551

Callon, M. (1998). Introduction: The Embeddedness of Economic Markets in Economics. *The Sociological Review*, *46*, 1–57. https://doi.org/10.1111/j.1467-954x.1998.tb03468.x

Callon, M., & Muniesa, F. (2005). Economic markets as calculative collective devices. *Organization Studies*, *26*(8), 1229–1250. https://doi.org/10.1177/0170840605056393

Carr, M. (2016a). Public – private partnerships in national cyber-security strategies. *International Affairs*, *1*(February), 190–209. https://doi.org/10.1111/1468-2346.12504

Carr, M. (2016b). *US power and the Internet in international relations: The irony of the information age*. New York: Palgrave Macmillan.

Charmaz, K., Thornberg, R., & Keane, E. (2017). Evolving grounded theory and social justice inquiry. In Noman K. Denzin & Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research* (pp. 705–760). Thousand Oaks, CA: Sage Publications.

Christensen, K. K., & Petersen, K. L. (2017). Public-private partnerships on cyber security: A practice of loyalty. *International Affairs*, *93*(6), 1435–1452. https://doi.org/10.1093/ia/iix189

Cisco. (2020). *Cisco Annual Internet Report (2018-2023)*. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: the next threat to national security and what to do about it*. New York: Harper Collins.

Council of Europe. (2001). *Convention on Cybercrime*. Retrieved from https://rm.coe.int/1680081561

David Bowie. (1999). *David Bowie speaks to Jeremy Paxman on BBC Newsnight (1999) - YouTube*. Retrieved from https://www.youtube.com/watch?v=FiK7s_0tGsg

Davies, P. H. J. (2001). Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services. *Politics*, *21*(1), 73–80.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*(JUN), 1–12. https://doi.org/10.3389/fpsyg.2018.00744

Dean, M. (2016). Risk, Calculable and Incalculable. *Soziale Welt*, *49*(1), 25–42.

Deibert, R. J. (2013). *Black code: Surveillance, Privacy, and the Dark Side of the Internet*. Oxford: Signal.

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*, 15–32. Retrieved from https://academic.oup.com/ips/article-abstract/4/1/15/1917052

Deibert, R. J., & Rohozinski, R. (2011). The new cyber military-industrial complex. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/opinion/the-new-cyber-military-industrial-complex/article573990/

Denzin, Norman K. (1970). *The Research Act: A Theoretical Introduction to Sociological*

Methods. Chicago: Aldine Publishing.

Domscheit-Berg, A. (2020). Bundesregierung nimmt das Problem der IT-Sicherheit nicht ernst – Anke Domscheit-Berg. Retrieved May 15, 2020, from https://mdb.anke.domscheit-berg.de/2020/02/bundesregierung-nimmt-das-problem-der-it-sicherheit-nicht-ernst/

Douglas, M., & Wildavsky, A. (1982). How Can We Know the Risks We Face? Why Risk Selection Is a Social Process. *Risk Analysis, 2*(2), 49–58. https://doi.org/10.1111/j.1539-6924.1982.tb01365.x

Drezner, D. W. (2021). Introduction. In D. W. Drezner, H. Farrell, & A. L. Newman (Eds.), *The Uses and Abuses of Weaponized Interdependence*. Brookings Institution Press.

Dunn Cavelty, M. (2007). *Cyber Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge.

Dunn Cavelty, M. (2015). Cyber-Security and Private Actors. In *Routledge Handbook of Private Security Studies* (pp. 89–99). https://doi.org/10.4324/9781315850986-10

Dunn Cavelty, M., & Egloff, F. J. (2021). Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland. *Swiss Political Science Review, 27*(1), 139–149. https://doi.org/10.1111/spsr.12433

Dunn Cavelty, M., Kaufmann, M., & Søby Kristensen, K. (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue, 46*(1), 3–14. https://doi.org/10.1177/0967010614559637

Dunn Cavelty, M., & Suter, M. (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection, 2*(4), 179–187. https://doi.org/10.1016/j.ijcip.2009.08.006

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Egloff, F. J. (2017). Cybersecurity and the Age of Privateering. In G. Perkovich & A. E. Levite (Eds.), *Understanding Cyber Conflict: Fourteen Analogies* (pp. 231–247). Washington D.C.: Georgetown University Press.

Egloff, F. J. (2020). Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy*, *41*(1), 55–81. https://doi.org/10.1080/13523260.2019.1677324

Eichensehr, K. E. (2015). The Cyber-Law of Nations. *Georgetown Law Journal*, *103*(2), 317–380.

Eichensehr, K. E. (2017). Public-Private Cybersecurity. *Texas Law Review*, *95*, 467–538.

Farrell, H., & Newman, A. L. (2014). Domestic institutions beyond the nation-state: Charting the new interdependence approach. *World Politics*, *66*(2), 331–363. https://doi.org/10.1017/S0043887114000057

Farrell, H., & Newman, A. L. (2015). The New Politics of Interdependence: Cross-National Layering in Trans-Atlantic Regulatory Disputes. *Comparative Political Studies*, *48*(4), 497–526. https://doi.org/10.1177/0010414014542330

Farrell, H., & Newman, A. L. (2019a). *Of Privacy and Power - The Transatlantic Struggle over Freedom and Security*. Princeton: Princeton University Press.

Farrell, H., & Newman, A. L. (2019b). Weaponized interdependence. *International Security*, *44*(1), 42–79.

Farrell, H., & Quiggin, J. (2017). Consensus, dissensus, and economic ideas: Economic crisis and the rise and fall of Keynesianism. *International Studies Quarterly*, *61*(2), 269–283. https://doi.org/10.1093/isq/sqx010

Faulconbridge, J. R., & Muzio, D. (2012). Professions in a globalizing world: Towards a transnational sociology of the professions. *International Sociology*, *27*(1), 136–152. https://doi.org/10.1177/0268580911423059

Finnemore, M. (2003). *The Purpose of Intervention - Changing Beliefs about the Use of Force*. https://doi.org/10.7591/9780801467073

Fleishman, G. (2000, December 14). Cartoon Captures Spirit of the Internet. *New York Times*. Retrieved from https://web.archive.org/web/20171229172420/http:/www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html

Flick, U. (2018). Triangulation in data collection. In Norman K. Denzin & Y. S. Lincoln (Eds.), *The SAGE handbook of qualitative data collection* (pp. 761–791). Thousand Oaks, CA: SAGE.

Fligstein, N. (1997). Social Skill and Institutional Theory. *American Behavioral Scientist*, *40*(4), 397–405. https://doi.org/10.1177/07399863870092005

Fligstein, N. (2001). Social Skill and the Theory of Fields. *Sociological Theory*, *19*(2), 105–125.

Fligstein, N., & McAdam, D. (2012). *A Theory of Fields*. Oxford: Oxford University Press.

Flyvbjerg, B. (2001). *Making Social Science Matter -Why social inquiry fails and how it can succeed again*. Cambridge: Cambridge University Press.

Flyvbjerg, B. (2011). Case Study. In Norman K. Denzin & Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research* (4th ed., pp. 301–316). https://doi.org/10.1057/9780230348158.0012

Flyverbom, M., Deibert, R., & Matten, D. (2019). The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business. *Business and Society*, *58*(1), 3–19. https://doi.org/10.1177/0007650317727540

Fourcade, M., & Healy, K. (2017). Classification situations: Life-chances in the Neoliberal Era. *Historical Social Research*, *42*(1), 23–51. https://doi.org/10.12759/hsr.42.2017.1.23-51

Fourcade, M., & Khurana, R. (2013). From social control to financial economics: the linked ecologies of economics and business in twentieth century America. *Theory and Society*, *42*(2), 121–159. https://doi.org/10.1007/sl

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika*, *58*(3), 273–286. https://doi.org/10.1080/00051144.2017.1407022

Geer, D. E. (2018). A Rubicon. *A Hoover Institution Essay*, (Aegis Series Paper No. 1801), 1–20. Retrieved from https://www.hoover.org/research/rubicon%0Apapers3://publication/uuid/5BB794C3-0DCB-4E6E-A19F-9E647A9B8A77

Geer, D. E., Jardine, E., & Leverett, E. (2020). On market concentration and cybersecurity risk.

Journal of Cyber Policy, *5*(1), 9–29. https://doi.org/10.1080/23738871.2020.1728355

Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. *Information Security Journal*, *18*(1), 1–7. https://doi.org/10.1080/19393550802676097

George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

Gephart, R. P., Van Maanen, J., & Oberlechner, T. (2009). Organizations and risk in late modernity. *Organization Studies*, *30*(2–3), 141–155. https://doi.org/10.1177/0170840608101474

Germer, H., Müller-Doohm, S., & Thiele, F. (2013). Intellektuelle Deutungskämpfe im Raum publizistischer Öffentlichkeit. *Berliner Journal Fur Soziologie*, *23*(3–4), 511–520. https://doi.org/10.1007/s11609-013-0230-7

Gerth, H. H., & Mills, C. W. (1977). *From Max Weber: Essays in Sociology*. London: Routledge & Kegan Pail Ltd.

Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Redwood City, CA: Stanford University Press.

Granovetter, M. (1985). Economic Action and Social Structure: The Problem of Embeddedness. *American Journal of Sociology*, *91*(3), 481–510.

Greenberg, A. (2019). *Sandworm - A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Random House USA.

Gusterson, H. (1997). Studying Up Revisited. *PoLAR: Political and Legal Anthropology Review*, *20*(1), 114–119.

Haas, P. (1992). Epistemic Communities and International Policy Coordination. *International Organization*, *46*(1), 1–35. https://doi.org/10.1017/S0020818300001442

Habermas, J. (1979). *Stichworte zur »Geistigen Situation der Zeit«*. Berlin: Suhrkamp.

Hall, R. B. (1997). Moral Authority as a Power Resource. *International Organization*, *51*(4), 591–622.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-

2478.2009.00572.x

Harašta, J. (2018). Legally critical: Defining critical infrastructure in an interconnected world. *International Journal of Critical Infrastructure Protection*, *21*, 47–56. https://doi.org/10.1016/j.ijcip.2018.05.007

Hardy, C., Maguire, S., Power, M., & Tsoukas, H. (2020). Organizing risk: Organization and management theory for the risk society. *Academy of Management Annals*, *14*(2), 1032–1066. https://doi.org/10.5465/annals.2018.0110

Henriksen, L. F., & Seabrooke, L. (2016). Transnational organizing: Issue professionals in environmental sustainability networks. *Organization*, *23*(5), 722–741. https://doi.org/10.1177/1350508415609140

Henriksen, L. F., & Seabrooke, L. (2021). Elites in Transnational Policy Networks. *Global Networks*, *21*, 217–237. https://doi.org/10.1111/glob.12301

Hilgartner, S. (1992). The Social Construction of Risk Objects: Or, How to Pry Open Networks of Risk. In J. F. Short & L. Clarke (Eds.), *Organizations, uncertainties, and risk* (pp. 39–53). Boulder: Westview Press.

Hinchman, K. A., & Moore, D. W. (2013). Close Reading. *Journal of Adolescent & Adult Literacy*, *56*(6), 441–450. https://doi.org/10.1002/JAAL.163

Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, *59*(6), 585–591. https://doi.org/10.1016/j.bushor.2016.07.004

Hurd, I. (2007). *After Anarchy: Legitimacy and Power in the United Nations Security Council*. Princeton: Princeton University Press.

Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: private companies as norm entrepreneurs. *Journal of Cyber Policy*, *3*(1), 61–76. https://doi.org/10.1080/23738871.2018.1467942

IRGC. (2018). *Guidelines for the Governance of Systemic Risks*. Lausanne: Inteernational Risk Governance Center (IRGC).

ITU. (2019). *Measuring Digital Development: Facts and Figures*. Retrieved from https://news.itu.int/measuring-digital-development-facts-figures-2019/

Jackson, P. T. (2011). *The Conduct of Inquiry in International Relations*. Retrieved from http://www.tandfebooks.com/isbn/9780203843321

Jacobsen, J. T. (2020). From neurotic citizen to hysteric security expert: a Lacanian reading of the perpetual demand for US cyber defence. *Critical Studies on Security*, *8*(1), 46–58. https://doi.org/10.1080/21624887.2020.1735830

Jacobsen, J. T. (2021). Cyber offense in NATO: challenges and opportunities. *International Affairs*, *97*(3), 703–720. https://doi.org/10.1093/ia/iiab010

Jensen, B., Valeriano, B., & Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, *42*(2), 212–234. https://doi.org/10.1080/01402390.2018.1559152

Johnson, T. (2016). Cooperation, co-optation, competition, conflict: international bureaucracies and non-governmental organizations in an interdependent world. *Review of International Political Economy*, *23*(5), 737–767. https://doi.org/10.1080/09692290.2016.1217902

Jones, J. (2019). *Understanding Cyber Risk Quantification A Buyer's Guide*. FAIR Institute.

Jordan, S., Mitterhofer, H., & Jørgensen, L. (2018). The interdiscursive appeal of risk matrices: Collective symbols, flexibility normalism and the interplay of 'risk' and 'uncertainty.' *Accounting, Organizations and Society*, *67*, 34–55. https://doi.org/10.1016/j.aos.2016.04.003

Kaplan, F. (2016). *Dark Territory - The Secret History of Cyber War*. New York: Simon & Schuster Paperbacks.

Kello, L. (2017). *The Virtual Weapon and International Order*. New Haven: Yale University Press.

Keohane, R. O., & Nye, J. S. (2012). *Power and Interdependence* (4th Editio). Boston: Longman.

Kessler, O., & Werner, W. (2013). Expertise, uncertainty, and international law: A study of the Tallinn manual on cyberwarfare. *Leiden Journal of International Law*, *26*(4), 793–810. https://doi.org/10.1017/S0922156513000410031

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace*. London: Penguin.

Krahmann, E. (2011). Beck and beyond: Selling security in the world risk society. *Review of International Studies*, *37*(1), 349–372. https://doi.org/10.1017/S0260210510000264

Kustermans, J., & Horemans, R. (2021). Four Conceptions of Authority in International Relations. *International Organization*, 1–25. https://doi.org/10.1017/S0020818321000230

Kvale, S. (2007). *Doing Interviews*. London: SAGE Publications Ltd.

Latour, B. (1987). *Science in Action* (11th ed.). Cambridge, MA: Harvard University Press.

Latour, B. (1999). *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge, MA: Harvard University Press.

Lee, R. M., & Rid, T. (2014). OMG Cyber!: Thirteen Reasons Why Hype Makes for Bad Policy. *RUSI Journal*, *159*(5), 4–12. https://doi.org/10.1080/03071847.2014.969932

Lewis, J. A. (2017). *Sustaining Progress in International Negotiations on Cybersecurity*. Retrieved from https://www.csis.org/analysis/sustaining-progress-international-negotiations-cybersecurity

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Lidskog, R., & Sundqvist, G. (2015). When Does Science Matter? International Relations Meets Science and Technology Studies. *Global Environmental Politics*, *15*(1), 1–20.

Liebetrau, T., & Christensen, K. K. (2020). The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European Journal of International Security*, *1*, 74–89. https://doi.org/10.1017/eis.2020.10

Lijphart, A. (1971). Comparative Politics and the Comparative Method. *The American Political Science Review*, *65*(3), 682–693.

Liñán, F., & Fayolle, A. (2015). A systematic literature review on entrepreneurial intentions: citation, thematic analyses, and research agenda. *International Entrepreneurship and Management Journal*, *11*(4), 907–933. https://doi.org/10.1007/s11365-015-0356-5

Liu, S. (2021). Between social spaces. *European Journal of Social Theory*, *24*(1), 123–139. https://doi.org/10.1177/1368431020905258

Lupovici, A. (2016). The"Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward. *International Studies Perspectives*, *17*,

322–342. https://doi.org/10.1111/insp.12082

Macak, K. (2017). From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers. *Leiden Journal of International Law*, *30*, 877–899. https://doi.org/10.1017/s0922156517000358

MacKenzie, D. (2001). *Mechanizing Proof: Computing, Risk, and Trust*. https://doi.org/10.1353/tech.2004.0209

MacKenzie, D. (2006). *An Engine, Not A Camera: How financial models shape markets*. Cambridge, MA: MIT Press.

Maguire, S., & Hardy, C. (2013). Organizing Processes and the Construction of Risk: A Discursive Approach. *The Academy of Management Journal*, *56*(1), 231–255.

Malecki, E. J. (2002). The economic geography of the internet's infrastructure. *Economic Geography*, *78*(4), 399–424. https://doi.org/10.1111/j.1944-8287.2002.tb00193.x

Malone, E. F., & Malone, M. J. (2013). The "wicked problem" of cybersecurity policy: analysis of United States and Canadian policy response. *Canadian Foreign Policy Journal*, *19*(2), 158–177. https://doi.org/10.1080/11926422.2013.805152

Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2021). A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology and Politics*, *18*(1), 1–20. https://doi.org/10.1080/19331681.2020.1776658

Matthijs, M., & Blyth, M. (2018). When Is It Rational to Learn the Wrong Lessons? Technocratic Authority, Social Learning, and Euro Fragility. *Perspectives on Politics*, *16*(1), 110–126. https://doi.org/10.1017/S1537592717002171

Maurer, T. (2018). *Cyber Mercenaries - The State, Hackers, and Power*. Cambridge: Cambridge University Press.

Mazzucato, M. (2011). *The Entrepreneurial State*. London: Demos.

McCarthy, D. R. (2018). Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

Mommsen, T. (1888). *Römisches Staatsrecht: Dritter Band*. Retrieved from https://archive.org/details/handbuchderrmis09mommgoog/page/n8/mode/2up

Moses, J. W., & Knutsen, T. L. (2012). *Ways of knowing: Competing methodologies in social and political research* (2nd ed.). Houndmills, UK: Palgrave Macmillan.

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*, *21*(5), 997–1018. https://doi.org/10.1007/s10796-017-9808-5

Muniesa, F., Millo, Y., & Callon, M. (2007). An introduction to market devices. *Sociological Review*, *55*(SUPPL. 2), 1–12. https://doi.org/10.1111/j.1467-954X.2007.00727.x

Nicholls, C. M., Mills, L., & Kotecha, M. (2013). Observation. In J. Ritchie, J. Lewis, C. M. Nicholls, & R. Ormston (Eds.), *Qualitative research practice: A guide for social science students and researchers* (pp. 243–268). London: SAGE.

Nye, J. S. (2010). Cyber Power. *Belfer Center for Science and International Affairs*, (May), 1–31. Retrieved from http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

Nye, J. S. (2011). Nuclear Lessons for Cyber Security ? *Strategic Studies Quarterly*, *5*(4), 18–38.

Pawlak, P. (2016). Capacity Building in Cyberspace as an Instrument of Foreign Policy. *Global Policy*, *7*(1), 83–92. https://doi.org/10.1111/1758-5899.12298

Pawlak, P., & Barmpaliou, P.-N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy*, *2*(1), 123–144. https://doi.org/10.1080/23738871.2017.1294610

Perlroth, N. (2021). *This Is How They Tell Me the World Ends - The Cyberweapons Arms Race*. London: Bloomsbury Publishing Plc.

Peters, A., & Jordan, A. (2020). Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime. *Journal of National Security Law and Policy*, *10*(3), 487–524.

Petersen, K. L., & Christensen, K. K. (2017). *Cyber Security: Complexity that Requires Responsibility*. Copenhagen.

Power, M. (2007). Organized Uncertainty: An Introduction. In *Organized Uncertainty: Designing a World of Risk Management.* (pp. 1–33). Oxford: Oxford University Press.

Power, M. (2015). How accounting begins: Object formation and the accretion of infrastructure. *Accounting, Organizations and Society*, *47*, 43–55. https://doi.org/10.1016/j.aos.2015.10.005

Power, M. (2016). Postscript - On Riskwork and Auditwork. In *Riskwork: Essays on the Organizational Life of Risk Management* (pp. 583–605). https://doi.org/10.1093/acprof:oso/9780198753223.003.0014 Abstract

PwC. (2018). *The Global State of Information Security Survey 2018: Strengthening digital society against cyber shocks*. Retrieved from https://www.pwc.com/us/en/cybersecurity/information-security-survey.html

Qu, S. Q., & Cooper, D. J. (2011). The role of inscriptions in producing a balanced scorecard. *Accounting, Organizations and Society*, *36*(6), 344–362. https://doi.org/10.1016/j.aos.2011.06.002

Quack, S. (2007). Legal Professionals and Transnational Law-Making: A Case of Distributed Agency. *Organization*, *14*(5), 643–666. https://doi.org/10.1177/1350508407080313

Quattrone, P. (2009). Books to be practiced: Memory, the power of the visual, and the success of accounting. *Accounting, Organizations and Society*, *34*(1), 85–118. https://doi.org/10.1016/j.aos.2008.03.001

Quigley, K., Burns, C., & Stallard, K. (2015). "Cyber Gurus": A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, *32*(2), 108–117. https://doi.org/10.1016/j.giq.2015.02.001

Raymond, M., & Denardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory*, *7*(3), 572–616. https://doi.org/10.1017/S1752971915000081

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory*, *7*(3), 572–616. https://doi.org/10.1017/S1752971915000081

Reichborn, E., & Friis, K. (2016). From Cyber Threats to Cyber Risks. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (pp. 27–44). London: Routledge.

Richardson, L. (2003). Writing: A Method of Inquiry. In Y. S. Lincoln & N. K. Denzin (Eds.), *Turning Points in Qualitative Research - Tying Knots in a Handkerchief* (pp. 379–396). Walnut Creek, CA: AltaMira Press.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Robson, K. (1992). Accounting numbers as "inscription": Action at a distance and the development of accounting. *Accounting, Organizations and Society*, *17*(7), 685–708. https://doi.org/10.1016/0361-3682(92)90019-O

Robson, K., & Bottausci, C. (2018). The sociology of translation and accounting inscriptions: Reflections on Latour and Accounting Research. *Critical Perspectives on Accounting*, *54*(June 2017), 60–75. https://doi.org/10.1016/j.cpa.2017.11.003

Roulston, K. (2014). Analysing interviews. In U. Flick (Ed.), *The SAGE Handbook of Qualitative Data Analysis* (pp. 297–312). London: SAGE.

Sanger, D. E. (2018). *The Perfect Weapon*. London: Scribe Publications.

Schwandt, T. A., & Gates, E. F. (2018). Case study methodology. In Norman K. Denzin & Y. S. Lincoln (Eds.), *The Sage Handbook of Qualitative Research* (pp. 590–619). Thousand Oaks, CA: SAGE Publications Inc.

Scott, W. R. (2008). Lords of the dance: Professionals as institutional agents. *Organization Studies*, *29*(2), 219–238. https://doi.org/10.1177/0170840607088151

Scott, W. R., & Davis, G. F. (2007). *Organizations and Organizing - Rational, Natural, and Open System Perspectives* (Vol. 148). New York: Routledge.

Seabrooke, L. (2014). Epistemic Arbitrage: Transnational Professional Knowledge in Action. *Journal of Professions and Organization*, *1*(1), 49–64. https://doi.org/10.1093/jpo/jot005

Seabrooke, L., & Henriksen, L. F. (2017). Issue control in transnational professional and organizational network. In L. Seabrooke & L. F. Henriksen (Eds.), *Professional Networks in Transnational Governance* (pp. 3–24). https://doi.org/10.1017/9781316855508.001

Seabrooke, L., & Sending, O. J. (2015). Open Systems of International Organization. *GR:EEN Working Paper No. 51*.

Seabrooke, L., & Tsingou, E. (2015). Professional emergence on transnational issues: Linked ecologies on demographic change. *Journal of Professions and Organization*, *2*(1), 1–18. https://doi.org/10.1093/jpo/jou006

Seabrooke, L., & Tsingou, E. (2021). Revolving doors in international financial governance. *Global Networks*, *21*(2), 294–319. https://doi.org/10.1111/glob.12286

Segal, A. (2017). Chinese Cyber Diplomacy in a New Era of Uncertainty. *Aegis Paper Series*, (1703).

Sending, O. J. (2015). *The Politics of Expertise. Competing for Authority in Global Governance*. Ann Arbor: University of Michigan Press.

Sending, O. J. (2017). Recognition and liquid authority. *International Theory*, *9*(2), 311–328. https://doi.org/10.1017/S1752971916000282

Shires, J. (2018). Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance*, *6*(2), 31–40. https://doi.org/10.17645/pag.v6i2.1329

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar - What Everybody Needs to Know*. New York: Oxford University Press.

Slack, C. (2016). Wired yet Disconnected: The Governance of International Cyber Relations. *Global Policy*, *7*(1), 69–78. https://doi.org/10.1111/1758-5899.12268

Slayton, R., & Clark-Ginsberg, A. (2018). Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. *Regulation and Governance*, *12*(1), 115–130. https://doi.org/10.1111/rego.12168

Starosielski, N. (2015). *The undersea network*. Durham: Duke University Press.

Stebbins, R. A. (2001). *Exploratory research in the social sciences*. Thousand Oaks, Calif. London.

Stevens, C. (2020). Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*, *41*(1), 129–152. https://doi.org/10.1080/13523260.2019.1675258

Stevens, T. (2012). Norms, Epistemic Communities and the Global Cyber Security Assemblage. *E-International Relations*. Retrieved from https://www.e-ir.info/2012/03/27/norms-epistemic-communities-and-the-global-cyber-security-assemblage/

Stevens, T. (2015). *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.

Stone, D. (2003). The "knowledge bank" and the global development network. *Global Governance*, *9*(1), 43–61. https://doi.org/10.1163/19426720-00901005

Stone, D. (2013). "Shades of grey": The World Bank, knowledge networks and linked ecologies of academic engagement. *Global Networks*, *13*(2), 241–260. https://doi.org/10.1111/glob.12007

Stone, D. (2019). Transnational policy entrepreneurs and the cultivation of influence: individuals, organizations and their networks. *Globalizations*, *16*(7), 1128–1144. https://doi.org/10.1080/14747731.2019.1567976

Swedberg, R. (2016). Before theory comes theorizing or how to make social science more interesting. *British Journal of Sociology*, *67*(1), 5–22. https://doi.org/10.1111/1468-4446.12184

Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. *Law and Social Inquiry*, *43*(2), 417–440. https://doi.org/10.1111/lsi.12303

Talesh, S. A., & Cunningham, B. (2021). The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy. *Utah Law Review*, *0*(0), 1–72.

Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, *9*(November), 60–66. https://doi.org/10.1111/1758-5899.12625

Tansey, O. (2007). Process tracing and elite interviewing: A case for non-probability sampling.

PS - Political Science and Politics, *40*(4), 765–772. https://doi.org/10.1017/S1049096507071211

Themsen, T. N., & Skærbæk, P. (2018). The performativity of risk management frameworks and technologies: The translation of uncertainties into pure and impure risks. *Accounting, Organizations and Society*, *67*, 20–33. https://doi.org/10.1016/j.aos.2018.01.001

United Nations. (1999). *A/RES/54/49*. New York.

Weinberger, S. (2017). *The imagineers of war: the untold history of DARPA, the Pentagon agency that changed the world*. New York: Knopf.

Weiss, L. (2014). *America Inc.?: innovation and enterprise in the national security state*. Ithaca: Cornell University Press.

White House. (2009). *Cyberspace Policy Review*. Retrieved from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Wimmer, A., & Glick Schiller, N. (2002). Methodological nationalism and beyond: nation-state building, migration and the social sciences. *Global Networks*, *2*(4), 301–334. https://doi.org/10.1111/1471-0374.00043

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, *12*, 4–11. https://doi.org/10.1016/j.ijcip.2015.11.003

Wolf, F. (2010). Enlightened eclecticism or hazardous hotchpotch? Mixed methods and triangulation strategies in comparative public policy research. *Journal of Mixed Methods Research*, *4*(2), 144–167. https://doi.org/10.1177/1558689810364987

World Economic Forum. (2019). *The Global Risks Report 2019* (14th ed.). https://doi.org/978-1-944835-15-6

Zetter, K. (2015). *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*. New York: Broadway Books.

Zürn, M. (2018). *A Theory of Global Governance: Authority, Legitimacy, and Contestation*. Oxford: Oxford University Press.

PART 2: ARTICLES

ARTICLE 1: Who is the Cyber Expert? Expertise and Professions within Cybersecurity

Who is the Cyber Expert? Expertise and Professions within Cybersecurity

Originally published in Danish for "Økonomi & Politik", available at Willers, J. O. (2020) "Hvem er cybereksperten? Ekspertise og professioner i cybersikkerhedsfeltet", Økonomi & Politik, 93(3), s. 59–75. doi: 10.7146/okonomi-og-politik.v93iOktober.122528.
Translated with minor additions for the purposes of this dissertation only.

Abstract

Cybersecurity experts play an important role in identifying and managing digital risks. Yet, little is known about the defining features of these individuals. This article employs insights from the sociology of professions to highlight competing epistemic rationalities in the organization of cyber risk. Drawing on a review of industry reports and a novel dataset of elite expert profiles in Danish cybersecurity committees, it is argued that the profile of cybersecurity experts has moved away from a purely technical focus. The new expert profile is both broader in scope and closer to the decision-making level. As such, it is positioned at the intersection of technical, organizational, and economic rationality. This indicates a metamorphosis of expert roles within cybersecurity: Cyber experts are no longer mundane digital security guards located in IT departments. Instead, they have become cyber risk managers. This has both elevated the standing of cyber risk experts to one of strategic importance, and it reflects a new security understanding structured around resilience logics.

Keywords: Cybersecurity, Cyber experts, Cybersecurity professions, Expert Power

Introduction

Experts have without a doubt become central actors within contemporary security debates (Berling & Bueger, 2015). Concurrently, increasing dependencies on digital technologies have redirected security debates towards issues of digital vulnerabilities and risks (Nye, 2011). Today, cybersecurity is both a strategic goal and a coveted competency.

But who is the cyber expert? Classically, Lene Hansen and Helen Nissenbaum argued that the technical complexity of cybersecurity and the speed of technological change would cement the expert's central role in driving cybersecurity as an issue of security policy (Hansen & Nissenbaum, 2009, p. 1166). In this context, it has been documented how cybersecurity experts occupy strategically important positions within public-private partnerships (Petersen & Christensen, 2017) and engage in diplomatic efforts (Segal, 2017). Yet, there is surprisingly little consensus about the competencies that define cybersecurity experts (Shires, 2018, p. 32). In this article, I address this question and zoom in on the profiles of elite cybersecurity experts. Drawing on the sociology of professions, I advance a new analytical framework to the study of cybersecurity knowledge, a topic that lately has begun to attract academic interest (c.f. Dunn Cavelty & Wenger, 2020).

Underlying this approach is a recognition of the political character of cyber risk. Cyber risks do not automatically translate into organizational responses. Instead, mitigation strategies are open to multiple interpretations with significant leeway for expert judgement. I argue that the ideas that underlie such expert judgements do not develop in a vacuum. Rather, ideas are being developed, tested, and disseminated among experts across institutional boundaries. Whether these ideas follow economic, technical, or geopolitical logics is of critical importance for the ordering of priorities and allocation of responsibilities (Kremer, 2014). It is therefore vital to understand how cybersecurity knowledge is organized, and what types of knowledge and competencies come to be associated with elite cybersecurity experts.

I draw inspiration from recent contributions to the cybersecurity literature that have highlighted the transformative character of cybersecurity governance in challenging existing institutional orders (McCarthy, 2018, p. 6). This literature has typically drawn on Actor-Network Theory and Science and Technology Studies to study the relations between technical and sociopolitical objects (Dunn Cavelty, 2018; T. Stevens, 2018). Others have integrated insights from 'assemblage theory' to highlight how cybersecurity issues are constituted through networks of

material and non-material actors (Collier, 2018). Common to these approaches is an analytical focus that prioritizes the entanglements of humans, objects, and ideas, arguing that the resulting socio-technical networks are constitutive of cybersecurity practices and discourses (Dunn Cavelty & Wenger, 2020). Building upon work in the tradition of the sociology of professions, I contribute to these debates by focusing on the political character of expert knowledge and highlight how expert status is underpinned by struggles for recognition (Reed, 1996; Sending, 2015). Further, I draw specifically on Andrew Abbott's classical work to locate the organization of cybersecurity knowledge within a nexus of economic, political, and technical logics (Abbott, 1988, 2005). Crucially, this approach is well-positioned to highlight how expert profiles correspond to competing approaches to the diagnosis and organization of cyber risks (see also T. Stevens, 2012).

The following section discusses the entanglements of knowledge and expert power. I also provide examples of expert authority in the shaping of cybersecurity regulations and norms. This is followed by a conceptual discussion about professions. I focus here on the relationship between functional debates about the merits of professionalization, and the systemic analysis of expert knowledge through multi-professional control projects. Subsequently, the perspective is illustrated. Here, I analyze expert profiles in central Danish expert committees. I conclude with a discussion about the implications of a new expert profile that is both broader in focus and closer to the decision-making level than the earlier technical profile.

Expertise in Focus

The social production of knowledge has long been a cornerstone of sociologically inspired scholarship within security studies. A central topic within this work is the entanglement of knowledge and power (Allan, 2018; Bueger, 2014; CASE Collective, 2006). Within this literature, experts are usually defined by a special set of competencies within the confines of a particular issue area. We know, however, from areas as diverse as economics and security-policy that expert knowledge rarely is uncontested (e.g. Eyal & Pok, 2015; Fourcade, 2010). To the contrary, professional contestation is a defining feature of the 'politics of expertise' (Reed, 1996; Sending, 2015). These struggles, it is argued, take the form of ongoing "conflicts over the exclusionary jurisdictional domains arising out of the contested monopolization of abstract knowledge and technique" (Reed, 1996, p. 582). Put differently, the politics of expertise refer to

struggles through which organized professional groups compete over definitional control. Such control affords professional groups to link diagnostics to treatments and claim jurisdiction over tasks (Abbott, 1988). In short, the politics of expertise are about definitional authority. The German term *Deutungshoheit* fittingly describes this process, referring to the exclusive authority to interpret problems and define appropriate means to address the problem (c.f. Krentz, 2014). In this context, epistemic (Haas, 1992) and cognitive (Broome & Seabrooke, 2015) authority are crucial vectors for the social organization of cyber risks.

But why is this significant? Security is not self-explanatory. As McCarthy highlights, security is first and foremost a question about "security for whom?" (2018, p. 8). Cybersecurity is itself a contested term (Shires & Smeets, 2017). Central aspects, such as the definition of security problems and the allocation of responsibilities, are subject to continuous renegotiation (Christensen & Liebetrau, 2019, p. 396). How security is conceptualized is therefore critical for the definition of security problems, including related questions of who is in charge, and what should be done. Expert knowledge, in this context, is embedded in relations to the social and political institutions that define the cultural framework through which knowledge is produced (Slayton & Clark-Ginsberg, 2018, p. 117). This provides for the breeding ground of conflicts between expert communities that claim jurisdiction over the same issue areas. Elsewhere, it has been documented that cybersecurity communities differ in their approach to emerging problems. Kremer uses the concept "security mindsets" to distinguish between distinct ways of thinking about cybersecurity issues. Whether dominant security mindsets reflect liberal or military logics has had serious implications for the U.S. approach to cybersecurity policy. Crucially, he argues, these mindsets reflect the professional and institutional backgrounds of cybersecurity experts (Kremer, 2014). In a similar vein, it has been documented how changes to the regulation of critical infrastructures in the U.S. were a direct result of professional conflicts between information technology experts and operational technology experts respectively (Slayton & Clark-Ginsberg, 2018). What type of professional group emerges victorious has stark implications for the organization of cyber risks.

This ability to promote different – and oftentimes competing – approaches to cybersecurity is one of the foundations of expert power. In this sense expert knowledge can both function as a legitimizing factor in the political decision-making process, and it can shape the means and ends of regulation itself (Bueger, 2014). While this is true for many security issues, there are several structural characteristics that facilitate processes of expert control in the cybersecurity domain.

The technical complexity and the speed of change are two factors that were already mentioned in the introductory section. The global shortage of qualified personnel is another.

Stevens argues that the dual character of technical complexity and rapid technological development creates a fundamental sense of uncertainty. This epistemological uncertainty translates into what he terms the "persistent core of cyber security narratives", namely "confusion over what is real and what is not" (T. Stevens, 2015, p. 155). Hansen and Nissenbaum, in turn, speculate that uncertainty sparks dynamics of technocratic policy-making "requiring an expertise that the public (and most politicians) do not have and this in turn allows "experts" to become securitizing actors" (2009, p. 1167). Similar dynamics of 'technification' and expert control are well-known from other issue areas that exhibit high degrees of technical complexity (Gracia & Oats, 2012; Thistlethwaite & Paterson, 2016; Tsingou, 2014).

Adding to the technical complexity and pace of change, cybersecurity work is characterized by a marked shortage of qualified personnel on a global scale (Vogel, 2016). The international organization of IT professionals, ISACA, estimates this shortage to be in the realm of two million globally (ISACA, 2019). Consequently, many organizations have neither the opportunity nor the means to hire qualified practitioners. By the early 2010s, the dependence of the U.S. administration on private cybersecurity consultants had reached such heights that several observers feared the development of a persistent and structural imbalance that would allow cybersecurity experts to define both the demand and the supply of cybersecurity solutions (Deibert, 2013; Deibert & Rohozinski, 2011; Lee & Rid, 2014).

Many public actors are still experiencing major problems when it comes to hiring cybersecurity experts. In Germany, one in four public cybersecurity positions remained vacant in 2020 (Domscheit-Berg, 2020). We lack corresponding figures from the Danish public sector, but there is no indication of a significantly better situation. A recent study from the Danish Digitization Agency concludes, for example, that the areas of "resources, competencies and awareness" are among the most pressing within the Danish administration when it comes to cybersecurity (Digitaliseringsstyrelsen, 2019, p. 5).

Many countries have elevated the training of cybersecurity experts to a level of strategic importance. In the United States, for example, the Obama administration unveiled the first national "Cybersecurity Workforce Strategy" in 2016, allocating $62 million annually to support the training of new practitioners (White House, 2016). Donald Trump followed up on this

promise and declared cybersecurity experts "*a strategic asset that protects the American people, the homeland, and the American way of life*" (Trump, 2019). In Denmark, the first dedicated Master's program in cybersecurity was established at Aalborg University earlier this year (Aalborg Universitet, 2020), and the Danish cyber- and IT strategy has identified the improvement of cybersecurity knowledge across educational programs as a key priority (Finansministeriet, 2018, p. 32). The United Kingdom has even gone as far as to announce that it aspires to create a fully-fledged cybersecurity profession in the near future (Government of the United Kingdom, 2016, 2018).

In summary, I argue that cybersecurity is particularly prone to expert power. I link this dependence to persistent epistemic uncertainties about the nature of cyber risks and a global shortage of practitioners. Epistemic uncertainty derives from the combination of technical complexity and the "high-paced rhythm" of technological development (c.f. Abbott, 2005). The mismatch between supply and demand makes cyber risk management an asymmetrical process, with cyber risks being portrayed as ubiquitous, while practitioners remain scant. This has created a field that exhibits all the characteristics to produce outcomes of expert power, privileging the elite discourses of authoritative individuals and undermining the possibilities for public debate. This opens an important question: What makes an expert in cybersecurity, and how can we know? In the subsequent section, I discuss the relationship between professions and professionalization to shine a light on these questions.

Professions and professionalization

Whether a professionalization of the cybersecurity industry is a desirable development has long been a controversial issue (Burley, Eisenberg, & Goodman, 2014; Dawson & Thomson, 2018; National Research Council, 2013). In this debate, professionalization is conceptualized as a functional process with the aim of ensuring minimum quality standards through the use of, among other things, certifications, licenses, common trainings, and ethical standards (Ford & Gibbs, 1996, p. 5). The debate is focused on whether a professionalization will create a positive societal effect or exacerbate the shortage of qualified experts. Abbott's approach, which forms the background the this article's analysis, breaks with this functional focus and directs attention to the organization of expert knowledge within a system of professions that is characterized by struggles over control and recognition (Abbott, 1988, p. 98). In the subsequent sections, I

discuss first the industry debate about the merits of professionalization from a functional perspective, before turning to a discussion of Abbott's systemic approach to the organization of expert knowledge.

From a functional perspective, there can be clear benefits to professionalization. Customers are guaranteed a minimum standard; public recognition of the work is increased; and the profession might find it easier to attract young talents through the establishment of clear career paths and secure working conditions. Processes of professionalization create, however, also new obstacles to practitioners. Compulsory training courses create barriers to entry and can lead to an unnecessary reduction in the available pool of practitioners (Burley et al., 2014). Reflecting on this aspect, the American National Research Council concluded in 2013 that "*some organizations may find that professionalization provides a useful degree of "quality control" for those who work in the field, but professionalization also imposes barriers to those who wish to enter the field at a time when demand for cybersecurity workers exceeds supply*" (National Research Council, 2013, p. 2). Professionalization is thus a process that involves a delimiting and a homogenizing element: a recognition of having the right tools to address a known problem, and enforcement mechanisms to ensure that these tools are common to all within the profession (c.f. Abbott, 1988, p. 60). Typical characteristics of mature professions are dedicated university degrees, professional associations, certifications and a common code of ethics (Ford og Gibbs, 1996). An organic development of these dimensions takes time and professionalization is therefore typically a long historical process (see for example Fourcade, 2010).

Cybersecurity is in many ways an immature profession. The first antivirus programs were developed in the late 1980s and the development of flourishing cybersecurity markets only fully transpired in the early 2010s when attacks became more destructive and widespread (Denning & Frailey, 2011). Further, the meaning of what cybersecurity work implies has changed dramatically since the early 2000s, and the classification of work roles remains ambiguous to this day (National Research Council, 2013). In a foundational text, Peter Denning identified 'system security' as one of 15 IT disciplines, alluding to a logic in which the management of digital vulnerabilities would naturally fall within the jurisdiction of IT experts (Denning, 2001). As the digital threat landscape evolved and digital systems increasingly became all-encompassing, the tasks associated with cybersecurity changed and required new competencies (Dawson og Thomson, 2018). The 2017 version of NIST's "Cybersecurity Workforce

Framework", for example, listed system security as only one among 62 work roles within cybersecurity (NIST, 2017). In many ways, cybersecurity resembles more of a loosely coupled field than a coherent profession (c.f. T. Stevens, 2012).

In practice, this means that the management of digital risks takes place within and across organizational environments and issue fields (Dawson & Thomson, 2018). Is cybersecurity a technical, organizational, financial, or cultural issue? Abbott's approach emphasizes how the answer to this question revolves around the competitive dynamics of professional claims to jurisdiction control (Abbott, 1988, p. 98). The advantage of such an approach is that it accounts for the multiplicity of cybersecurity work and it provides the tools to ask how fragmentation transpires into professional claims to jurisdictional control: "Cybersecurity is no longer the remit only of private or corporate practitioners but has become a complex site of interaction between a very wide range of people, organizations and technologies" (C. Stevens, 2020, p. 133). Control, in this perspective, originates from the relations between professions and allows for the exercise of definitional power by linking processes of diagnosis, inference and treatment. That is, dominant professions control problematizations, define courses of action, and – perhaps most importantly – determine evaluative success criteria (Abbott, 1988, p. 137).

From this perspective, a profession is characterized by control over tasks (ibid., pp. 8, 53). Classical examples are the medical professions, lawyers, and auditors. Some professions, such as economists, have significantly expanded their jurisdictional control over time and colonized ever more tasks (Fourcade, Ollion, & Algan, 2015). Such expansionary dynamics have also been documented for cybersecurity professionals, albeit on a much smaller scale. Tanczer and colleagues document, for example, how technical cybersecurity experts are taking on roles in adjacent fields. Their analysis shows that Cybersecurity Incidence Response Teams (CIRTs/CSIRTs) have a unique ability to navigate transnational networks and maintain open lines of communication even in situations of geopolitical conflict. In doing so, the authors argue, cybersecurity experts take on diplomatic roles (Tanczer, Brass, & Carr, 2018). Further, Clare Stevens shows how private cybersecurity companies operate in a nexus of political and technical considerations when analyzing and attributing cyberattacks. In conclusion to her analysis, she highlights how technical work tasks became "entangled in the politics of nuclear proliferation, diplomacy, international law, and the mechanisms of global cybersecurity governance" (C. Stevens, 2020, p. 130). For cybersecurity as much as for information technology more broadly,

“governments and their executives…no longer enjoy a monopoly over diplomatic interactions” (Farrell & Newman, 2019, p. 170).

By redirecting focus away from the structural characteristics of professionalization, Abbott’s systemic account places the concrete work of professions centerstage and opens the analysis to questions of authority and definitional power. Elsewhere, it has been argued that, owing to the technical complexity and speed of technological change, professional struggles for control operate in a depoliticized and technocratic context: ”[T]he epistemic authority which computer and information scientists hold allow them the privileged role as those who have the authority to speak about the unknown” (Hansen & Nissenbaum, 2009, pp. 1166–1167). My contention is that such questions of jurisdictional control should not be answered deductively. Instead, it should be the subject of empirical analysis. Public and private councils and expert committees can serve as important indicators of professional control. They are gathering places for elite professionals and critical venues for the deliberation of problematizations and best practices (Reed, 1996; van Apeldoorn og Graaff, 2014). The next section turns to an analysis of such forums.

Danish cybersecurity experts

To illustrate the above theoretical considerations, I turn now to an illustrative analysis of Danish elite cybersecurity experts. The empirical material is based on a collection of prominent public and private expert committees with cybersecurity as the sole focus area. Expert groups have previously been found to play important roles in structuring professional work and reflecting control projects. As such, they are well-positioned to shed light on professional dynamics in ambiguous issue-fields (Reed, 1996; Seabrooke & Tsingou, 2014). The dataset covers 195 positions across 176 practitioners. Some committees are established by public decree (Cybersikkerhedsråd og Erhvervsministeriets IT Sikkerhed Virksomhedsråd). One has an independent status, two are affiliated with industry organizations and another covers the cybersecurity officers from the largest 25 Danish companies (C25 companies). The selection of committees was based on their position in the institutional ecology of cybersecurity discourse in Denmark. The sampling strategy was therefore purposive and subsequently discussed with trusted industry insiders (Tansey, 2007). The analysis is strictly illustrative and does not aim to provide a representative picture of the entire population of cybersecurity experts in Denmark.

Given the clear limitations of the dataset, none of the conclusions that appear from the subsequent analysis are definitive. However, given the focus on elite practitioners, the analysis nevertheless promises to provide interesting insights into the profiles of authoritative cybersecurity experts. Throughout, I expand on the empirical results and link them to broader debates in the academic and professional literature. Finally, it is important to emphasize that the analysis focuses exclusively on expert groups and committees. Formal organizations such as the "Center for Cybersecurity" or the 'Digitaliseringsstyrelsen's "Office for Cyber- and Information Security" are thus excluded from the analysis.

Table1: Overview over select expert committees.

Name	*# Members*	*Public/private*
Cybersikkerhedsråd	19	Public, Center for Cybersikkerhed
IT-Branchens Sikkerhedsudvalg	53	Private, IT Branchen
Rådet for Digital Sikkerhed	63	Independent Organization
Erhvervsministeriets IT Sikkerhed Virksomhedsråd	14	Public, Erhvervsministeriet
Dansk Industri's Udvalg for Informationssikkerhed	16	Private, Dansk Industri
C25 Danske Virksomheders CISOs eller tilsvarende	30	Private, not formally constituted

I collected professional and educational backgrounds on all thence identified elite experts through publicly available sources such as conference brochures and LinkedIn. The results indicate a heterogenous population of individuals. Two overarching trends show elite experts to be predominantly men and to work in the private sector. 86% are currently employed by private companies while 6% and 5% are affiliated with research- and public institutions respectively. Female cyber experts account for only 12% of the sample, indicating a rather strong gender imbalance. While these results partially reflect the selection of expert committees, studies from other countries show similar results. According to the International Information System Security Certification Consortium's (ISC^2) *Cybersecurity Workforce Survey,* only 30% of respondents identified as female (ISC^2, 2019). The 2017 *'Global Information Security Workforce Stud*y'

from business consulting firm Frost and Sullivan estimates that almost 90% of cybersecurity experts are men (Frost & Sullivan, 2017, p. 5). Finding reference data on the proportion of publicly employed cyber experts is more difficult (c.f. Bate, 2018, p. 9). A UK Government study from 2020 shows that public organizations in the United Kingdom are 50% more likely than private companies to outsource cybersecurity tasks to external actors (Pedley et al., 2020). This is another indication of the challenges that public organizations face in attracting qualified cybersecurity practitioners, a condition that oftentimes is linked to the difficulties in competing with private sector wage levels (Pollitt, 2010).

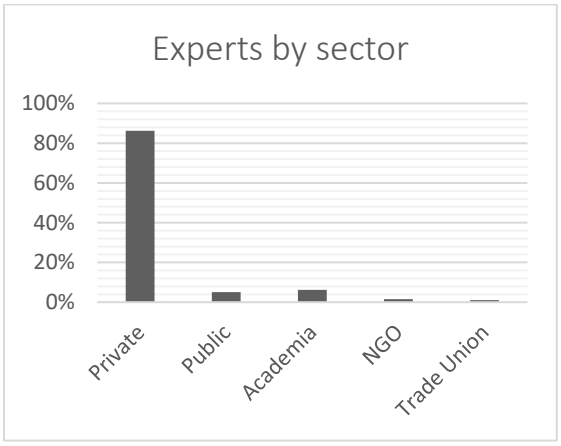


Figure1: Elite experts by affiliated sector

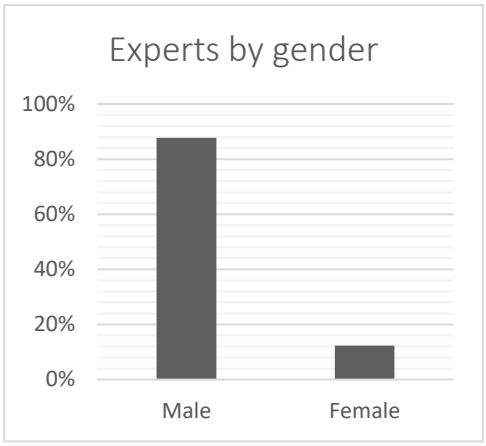


Figure 2: Elite experts by gender

In terms of the educational background of elite experts, the results are mixed. For each person in the dataset, the two most recent degrees within higher education were recorded. To qualify as such, I set a threshold for full degrees and excluded individual courses. The rationale for this decision was to gather data that would indicate coherent trainings and allow for statements of the sort: If a person has taken this programme, s/he is likely to be primarily an expert in area a/b/c (c.f. Young, 2012). For 19 individuals, no data were available and another 26 had only listed their most recent degree. Together, these two groups account for the 22% of missing values ("n/a") in the dataset. In order to provide an overall overview, it was necessary to categorize the educational backgrounds. This was especially important for the computer science category. For the purposes of this analysis, I included all degrees that were primarily focused on computer- and data-science, and those that were labelled IT or encryption. In turn, hybrid

degrees that only included computer sciences as a minor were labelled in accordance to the major part of the degree. “Business and ICT management”, for example, was coded as “business”. The results should, therefore, be taken as indicative rather than definitive.

As shown in Figure 3, computer science is the most frequent type of education among the 390 registered degrees (19%). Business administration (13%) and political science (11%) take second and third places. Considering the classical assertion that cybersecurity experts derive their authority from mastering complex technical knowledge, these results are surprising. However, the results still indicate a central position for such *techne* in expert profiles. Almost a third (32%) of the individuals have completed at least one IT-specific degree at university level. A similar trend can be observed in the US workforce, which indicates a continuing, albeit shrinking, dominance of computer science and engineering backgrounds among cybersecurity professionals (Frost & Sullivan, 2017, p. 5).

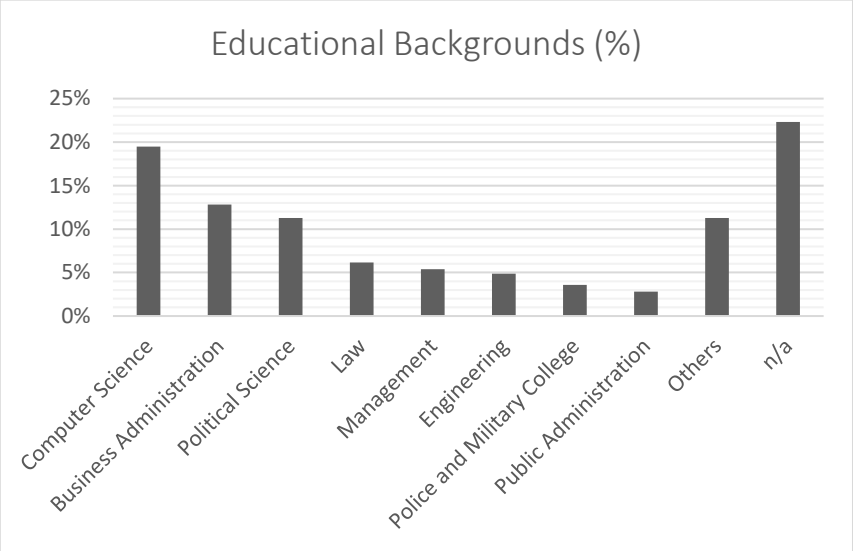


Figure 3: Elite experts by education background

It is equally interesting to take a closer look at the less classical educations. At least 19% have taken a degree in business administration. When combining business administration, political science, management, finance, and public administration into a single category, we can see that almost half (44%) of the experts have completed non-traditional degrees in areas that are associated with management and administrative jobs (“Djøf-uddannelser”). As far as possible, certifications were also considered for the analysis. Given the high number of missing values

(122), the results of this analysis remain, however, prone to sampling errors. Two trends stand out. The "$(ISC)^2$" and CISSP (25) certificates dominate among elite experts together with ISACA's CISM, CISA and CRISC (combined 35) certificates. The "Certified Information Systems Security Professionals" (CISSP) certificate is issued by the world's largest member association of professional cybersecurity experts with over 150,000 certified members worldwide (ISC^2, 2020). According to industry insiders, holding a CISSP certificate is an important signifier of professional competency, but it is only available for experienced professionals, and does therefore not offer a license to enter the profession. CISSP is often characterized as the most recognized accreditation for cybersecurity experts and signals a broad knowledge across cybersecurity work tasks (Pedley et al., 2020, p. 14). ISACA is an association with a broader scope and issues certificates across IT-relevant working areas, including cybersecurity (ISACA, 2020).

In summary, the illustrative analysis has indicated that elite cybersecurity experts overwhelmingly are men and operate from within the private sector. These results are in line with comparable research from the United States and the United Kingdom. Technical IT-specific degrees are frequent, but the analysis indicates that elite experts tend to have a more diverse educational background. The technical aspect is oftentimes balanced with degrees within business administration, strategic management, and political science. Certificates are primarily issued by private transnational associations.

A new Expert Profile? From techne to process-orientation.

The previous section has indicated that we are dealing with more than one expert profile when it comes to cybersecurity. Concurrently, however, there seems to be a clear trend that locates expert profiles between fields (c.f. Eyal, 2013). The location of experts within purely technical confines – the *techne* (Flyvbjerg, 2001) – has shifted and is today complemented by corporate-organizational and political rationalities. Consequently, cybersecurity seems no longer to be regarded as a purely technical matter. To make cybersecurity operational, it seems, requires both a technical foundation and bridge-building competences to mediate between epistemes. From an organizational perspective such a change implies a reconceptualization of cybersecurity itself, elevating it from a delimited and clearly defined task within IT operations to an integrated role with a clear process orientation across organizational entities (c.f. Ferdinand, 2015). Whereas

the classical cybersecurity expert was part of the IT department (Denning, 2001), the new profile is both broader in focus and closer to the executive level.

Additionally, this process orientation also reflects a more proactive approach to cybersecurity. An expert profile grounded in *techne* corresponds to an understanding of cyber problems in terms of threats. From this perspective, the main task of the cybersecurity expert is to defend against cyber threats by effectively improving digital defenses and keeping costs low. In short, the cyber expert is a *digital security guard*. The new profile, on the other hand, seems to be part of an organization's development. Located in the nexus between governance and strategy, the new cyber expert is concerned with the development of processes around the organization's risk profile, segmenting the 'crown-jewels' from non-essential data and designing appropriate responses to the thence defined categories (EY, 2019, pp. 7, 25). The new cyber expert is a *risk manager*.

This requires a new expert profile across three dimensions. First, it requires intimate understanding of an organization's structure and operations. The previously identified prominence of degrees in business administration can be understood as testament to this development. The second requirement is a partial reorientation to external developments. Among those, the external threat landscape is the most important to monitor. Who are potential adversaries and what are the global trends in the cybersecurity arena? Political science degrees and military backgrounds align with this aspect of the new expert profile. Finally, the third dimension relates to the continued importance of the technical foundation of experts. For the new cyber *risk* expert, the crucial competency is to translate operational and strategic considerations into technical solutions, and, concurrently, to translate technical developments into organizational processes. In short, the new profile as risk manager elevates the cybersecurity expert to a strategic position. A similar development was documented for security experts in private American companies, where the position "corporate security officer" moved from a technical to a strategic role (Petersen, 2013, p. 225).

At the same time, this development intersects with, and it reflects, a new ontology of cybersecurity. Where the preoccupation with technical solutions reflected a preventive security logic, the new profile signifies the unattainability of absolute security in cyberspace (Reichborn & Friis, 2016). To accommodate such a permanent state of latent insecurity, it is necessary to create processes that ensure the organization's ability to withstand attacks. In security jargon,

this reflects a move away from preventive and towards resilience strategies (Lasconjarias, 2017). That is, in a world where dedicated hackers always will find a way in (given that they have both the will and the resources), purely defensive action is no longer deemed viable. The resilience strategy, on the other hand, prioritizes the identification of an organization's essential assets - so-called crown jewels - and works to either completely separate them from the rest of the network or to build special security processes around them (ENISA, 2019, p. 16).

The new hybrid profile is, therefore, both broader in focus and closer to the decision-making level. As such, it strengthens the position of the cyber expert to define risks and assign appropriate mediating strategies. The sociological analysis of professions emphasizes how cybersecurity work is embedded in an institutional arena in which the contours of cyber risk work are continuously re-negotiated among professionals that operate in a nexus between economic, political, and technical considerations. From a societal perspective, such a development raises new political, democratic, and economic questions. To address such questions, it will be necessary to create a basis for public discussions and to strengthen overall levels of knowledge and awareness of digital risks among societal actors. Cybersecurity questions are increasingly enmeshed in broader social questions about the balancing of security and liberty. As such, these discussions require public debates. In this context, it is crucial to create a framework that strengthens the ability of civil society organizations to translate expert-driven debate to a wide audience. The state can support this process by, among others, offering free trainings in cybersecurity. This is not without precedence. The UK, for example, offers free courses for young adults with an interest in cybersecurity (UK Cyber First, 2020; UK Cyber Skills Immediate Impact Fund, 2020). Such a mechanism could also help to correct the gender gap and motivate more women to enter the cybersecurity workforce. The overarching goal, however, must be to lift cybersecurity discourses out of the confines of expert debates and to provide the precondition for an inclusive debate that recognizes the politics of cyber risk governance (Dunn Cavelty & Wenger, 2020).

From an economic perspective, cybersecurity is an issue that will only grow in importance and the management of digital risks is expensive. A successful process orientation can minimize the cost of cyberattacks. As discussed, this requires a new expert profile, that can bridge technical, organizational, and strategic considerations. However, there can be no doubt that the technical element remains the basis of cyber risk governance. Therefore, extra efforts must be made to raise the awareness of senior-decision makers. Not unlike the broader socio-political discussion,

this does not imply that everyone should become an expert. Rather, it requires a recognition of digital risks as fundamental components of digital societies and economies.

Conclusions

This article has argued for a stronger focus on knowledge formation and expert profiles in cybersecurity research. The organization and structure of expert knowledge in mature and immature professions can be an important factor in shaping security understandings across public and private organizations. A variety of approaches can be applied to study these dynamics. Here, I have focused on the contested nature of knowledge production inspired by Andrew Abbott's classical work on the sociology of professions. With an emphasis on the political character of expert control, I have focused on the location of expert knowledge within a system of professions that is defined by competitive struggles among professional groups to assert exclusive control over tasks through processes of risk diagnosis, inference, and treatment. The illustrative analysis of Danish elite cyber experts indicates that political and business-administrative logics have become important reference points for the otherwise technical cybersecurity profile.

This development, I have argued, can be understood in terms of a new security understanding that revolves around resilience logics. Cybersecurity is no longer a cost factor first and foremost but a strategic priority. As such, the new expert profile operates in the context of organizational *development* and is characterized by a managerial focus on the segmentation of essential from non-essential assets and processes. As cyber experts are becoming managers of risk and uncertainty more broadly, expert power over questions of cyber risk should be balanced by a democratic and inclusive debate. Such democratic debates are particularly crucial at a time when fundamental issues such as the use of encryption, surveillance, and the use of offensive military cyber capabilities are being renegotiated.

References

(ISC)2. (2019). Strategies for Building and Growing Strong Cybersecurity Teams. In *(ISC)2 Cybersecurity Workforce Study* (Vol. 2019).

Aalborg Universitet. (2020, January 29). Danmarks første uddannelse i cybersikkerhed. Retrieved May 15, 2020, from https://www.nyheder.aau.dk/2019/nyhed/danmarks-foerste-uddannelse-i-cybersikkerhed.cid447828

Abbott, A. (1988). *The System of Professions - An Essay on the Division of Expert Labor*. Chicago: The University of Chicago Press.

Abbott, A. (2005). Linked ecologies: States and universities as environments for professions. *Sociological Theory*, Vol. 23, pp. 245–274. https://doi.org/10.1111/j.0735-2751.2005.00253.x

Allan, B. B. (2018). From subjects to objects: Knowledge in International Relations theory. *European Journal of International Relations*, *24*(4), 841–864. https://doi.org/10.1177/1354066117741529

Bate, L. (2018). *Cybersecurity Workforce Development: A Primer*. Retrieved from https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_Workforce_Development_A_Primer_2018-10-31_175830_YMwa3ZJ.pdf

Berling, T. V., & Bueger, C. (2015). *Security expertise: practice, power, responsibility*. London: Routledge.

Broome, A., & Seabrooke, L. (2015). Shaping policy curves: Cognitive authority in transnational capacity building. *Public Administration*, *93*(4), 956–972. https://doi.org/10.1111/padm.12179

Bueger, C. (2014). From Expert Communities to Epistemic Arrangements: Situating Expertise in International Relations. In *International Relations and the Global Politics of Science and Technology* (pp. 39–54). https://doi.org/10.1007/978-3-642-55010-2

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Privacy and security: Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM*, *57*(2), 24–27. https://doi.org/10.1145/2556936

CASE Collective. (2006). Critical Approaches to Security in Europe: A Networked Manifesto. *Security Dialogue*, *37*(4), 443–487. https://doi.org/10.1177/0967010606073085

Christensen, K. K., & Liebetrau, T. (2019). A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry. *Intelligence and National Security*, *34*(3), 395–408. https://doi.org/10.1080/02684527.2019.1553704

Collier, J. (2018). Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision. *Politics and Governance*, *6*(2), 13–21. https://doi.org/10.17645/pag.v6i2.1324

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*(JUN), 1–12. https://doi.org/10.3389/fpsyg.2018.00744

Deibert, R. J. (2013). *Black code: Surveillance, Privacy, and the Dark Side of the Internet*. Oxford: Signal.

Deibert, R. J., & Rohozinski, R. (2011). The new cyber military-industrial complex. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/opinion/the-new-cyber-military-industrial-complex/article573990/

Denning, P. J. (2001). Who Are We? *Communications of the ACM*, *44*(2), 15–19.

Denning, P. J., & Frailey, D. J. (2011). The profession of IT: Who are we - now? *Communications of the ACM*, *54*(6), 25–27. https://doi.org/10.1145/1953122.1953133

Digitaliseringsstyrelsen. (2019). *ISO 27001-modenhed i staten*. Retrieved from https://digst.dk/media/21873/iso-modenhed-i-staten-nov-2019.pdf

Domscheit-Berg, A. (2020). Bundesregierung nimmt das Problem der IT-Sicherheit nicht ernst – Anke Domscheit-Berg. Retrieved May 15, 2020, from https://mdb.anke.domscheit-berg.de/2020/02/bundesregierung-nimmt-das-problem-der-it-sicherheit-nicht-ernst/

Dunn Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance*, *6*(2), 22. https://doi.org/10.17645/pag.v6i2.1385

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*,

41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

ENISA. (2019). *Threat Landscape Report 2018 15 Top Cyberthreats and Trends*. https://doi.org/10.2824/622757

EY. (2019). *Global Bank Risk Management Survey*. Retrieved from https://www.ey.com/Publication/vwLUAssets/ey-global-risk-survey-2019/$FILE/ey-global-risk-survey-2019.pdf

Eyal, G. (2013). Spaces Between Fields. In P. S. Gorski (Ed.), *Bourdieu and Historical Analysis* (pp. 158–182). Durham: Duke University Press.

Eyal, G., & Pok, G. (2015). What is security expertise ? From the sociology of professions to the analysis of networks of expertise. In T. Villumsen Berling & C. Bueger (Eds.), *Security Expertise* (pp. 53–75). London: Routledge.

Farrell, H., & Newman, A. L. (2019). *Of Privacy and Power - The Transatlantic Struggle over Freedom and Security*. Princeton: Princeton University Press.

Ferdinand, J. (2015). Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. *Journal of Business Continuity & Emergency Planning*, *9*(2), 185–195.

Finansministeriet. (2018). National strategi for cyber- og informationssikerhed. In *Center for Cybersikkerhed*. Retrieved from https://fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed-2018.pdf

Flyvbjerg, B. (2001). *Making Social Science Matter -Why social inquiry fails and how it can succeed again*. Cambridge: Cambridge University Press.

Ford, G., & Gibbs, N. E. (1996). *A Mature Profession of Software Engineering*.

Fourcade, M. (2010). *Economists and Societies*. Princeton University Press.

Fourcade, M., Ollion, E., & Algan, Y. (2015). The Superiority of Economists. *Journal of Economic Perspectives*, *29*(1), 89–114. https://doi.org/10.1257/jep.29.1.89

Frost & Sullivan. (2017). *The 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk*.

Government of the United Kingdom. (2016). National Cyber Security Strategy 2016-2021. In

National Cyber Security Strategy. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Government of the United Kingdom. (2018). *Implementing the National Cyber Security Strategy - Developing the Cyber Security Profession in the Uk*. Retrieved from https://extranet.cranfield.ac.uk/government/uploads/system/uploads/attachment_data/file/767427/,DanaInfo=assets.publishing.service.gov.uk,SSL+Government_Response_to_Consultation_on_Developing_the_Cyber_Security_Profession_in_the_UK_-_21_December_2018.pdf

Gracia, L., & Oats, L. (2012). Boundary work and tax regulation: A Bourdieusian view. *Accounting, Organizations and Society*, *37*(5), 304–321. https://doi.org/10.1016/j.aos.2012.03.004

Haas, P. (1992). Epistemic Communities and International Policy Coordination. *International Organization*, *46*(1), 1–35. https://doi.org/10.1017/S0020818300001442

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

ISACA. (2019). *State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development*. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2019-part-1_res_eng_0319.pdf?regnum=500542

ISACA. (2020). IT Certification Programs | Information Technology Certifications | ISACA. Retrieved May 19, 2020, from https://www.isaca.org/credentialing

ISC^2. (2020). Cybersecurity Certification and Training | (ISC)^2. Retrieved May 18, 2020, from https://www.isc2.org/about

Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information and Communications Technology Law*, *23*(3), 220–237. https://doi.org/10.1080/13600834.2014.970432

Krentz, N. (2014). *Ritualwandel und Deutungshoheit: Die frühe Reformation in der Residenzstadt Wittenberg (1500-1533)*. Mohr Siebeck.

Lasconjarias, G. (2017). Deterrence Through Resilience Nato, the Nations and the Challenges of Being Prepared. In *Eisenhower Paper, Research Division*.

Lee, R. M., & Rid, T. (2014). OMG Cyber!: Thirteen Reasons Why Hype Makes for Bad Policy. *RUSI Journal*, *159*(5), 4–12. https://doi.org/10.1080/03071847.2014.969932

McCarthy, D. R. (2018). Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

National Research Council. (2013). *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*. https://doi.org/10.17226/18446

NIST. (2017). *National Initiative for Cybersecurity Education (NICE) - Cybersecurity Workforce Framework.*

Nye, J. S. (2011). Nuclear Lessons for Cyber Security ? *Strategic Studies Quarterly*, *5*(4), 18–38.

Pedley, D., Borges, T., Bollen, A., Shah, J. N., Donaldson, S., Furnell, S., & Crozier, D. (2020). *Cyber security skills in the UK labour market 2020 Findings report*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869506/Cyber_security_skills_report_in_the_UK_labour_market_2020.pdf

Petersen, K. L. (2013). The corporate security professional: A hybrid agent between corporate and national security. *Security Journal*, *26*(3), 222–235. https://doi.org/10.1057/sj.2013.13

Petersen, K. L., & Christensen, K. K. (2017). *Cyber Security: Complexity that Requires Responsibility*. Copenhagen.

Pollitt, C. (2010). Technological Change: A Central yet Neglected Feature of Public Administration. *NISPAcee Journal of Public Administration and Policy*, *3*(2), 31–53. https://doi.org/10.2478/v10110-010-0003-z

Reed, M. I. (1996). Expert power and control in late modernity: An empirical review and theoretical synthesis. *Organization Studies*, *17*(4), 573–597. https://doi.org/10.1177/017084069601700402

Reichborn, E., & Friis, K. (2016). From Cyber Threats to Cyber Risks. In K. Friis & J.

Ringsmose (Eds.), *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (pp. 27–44). London: Routledge.

Seabrooke, L., & Tsingou, E. (2014). Distinctions, affiliations, and professional knowledge in financial reform expert groups. *Journal of European Public Policy*, *21*(3), 389–407. https://doi.org/10.1080/13501763.2014.882967

Segal, A. (2017). Chinese Cyber Diplomacy in a New Era of Uncertainty. *Aegis Paper Series*, (1703).

Sending, O. J. (2015). *The Politics of Expertise. Competing for Authority in Global Governance*. Ann Arbor: University of Michigan Press.

Shires, J. (2018). Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance*, *6*(2), 31–40. https://doi.org/10.17645/pag.v6i2.1329

Shires, J., & Smeets, M. (2017). Contesting Cyber. *New America Foundation*. Retrieved from https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/contesting-cyber/

Slayton, R., & Clark-Ginsberg, A. (2018). Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. *Regulation and Governance*, *12*(1), 115–130. https://doi.org/10.1111/rego.12168

Stevens, C. (2020). Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*, *41*(1), 129–152. https://doi.org/10.1080/13523260.2019.1675258

Stevens, T. (2012). Norms, Epistemic Communities and the Global Cyber Security Assemblage. *E-International Relations*. Retrieved from https://www.e-ir.info/2012/03/27/norms-epistemic-communities-and-the-global-cyber-security-assemblage/

Stevens, T. (2015). *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.

Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance*, *6*(2), 1–4. https://doi.org/10.17645/pag.v6i2.1569

Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, *9*(3), 60–66.

https://doi.org/10.1111/1758-5899.12625

Tansey, O. (2007). Process tracing and elite interviewing: A case for non-probability sampling. *PS - Political Science and Politics*, *40*(4), 765–772. https://doi.org/10.1017/S1049096507071211

Thistlethwaite, J., & Paterson, M. (2016). Private governance and accounting for sustainability networks. *Environment and Planning C: Government and Policy*, *34*(7), 1197–1221. https://doi.org/10.1177/0263774X15604841

Trump, D. J. (2019, May 2). Executive Order on America's Cybersecurity Workforce | The White House. Retrieved May 15, 2020, from https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

Tsingou, E. (2014). Club governance and the making of global financial rules. *Review of International Political Economy*, *22*(2), 225–256. https://doi.org/10.1080/09692290.2014.890952

van Apeldoorn, B., & Graaff, N. De. (2014). Corporate Elite Networks and us Post-Cold war Grand Strategies From Clinton to Obama. *European Journal of International Relations*, *20*(1), 29–55. https://doi.org/10.1177/1354066111433895

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32–46.

White House. (2016). *Federal cybersecurity workforce strategy*. Retrieved from https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf

Young, K. L. (2012). Transnational regulatory capture? An empirical examination of the transnational lobbying of the Basel Committee on Banking Supervision. *Review of International Political Economy*, *19*(4), 663–688. https://doi.org/10.1080/09692290.2011.624976

ARTICLE 2: Seeding the Cloud: Consultancy Services in the Nascent Field of Cyber Capacity Building

Symposium Article

Seeding the Cloud: Consultancy Services in the Nascent Field of Cyber Capacity Building

Published article: Willers, J. O. (2021). Seeding the Cloud: Consultancy services in the nascent field of cyber capacity building. Public Administration, 1–16.
https://doi.org/10.1111/padm.12773

Abstract

Transnational issues in public administration are charged with coordination problems between public and private actors. This is especially true for nascent issue fields. The mitigation of global cyber risks represents one such emerging issue. International organizations have encouraged the development of cybersecurity strategies as an integral part of national security regimes and to strengthen the global security environment. Cyber Capacity Building (CCB) efforts respond to these calls and disseminate digital risk management to recipient states. At a time where public administrations have not determined a position on CCB, Global Professional Service Firms (GPSFs) have affirmed the importance of external third-party knowledge on cybersecurity issues. They are 'seeding the cloud' to benefit from the field as it matures. Through the application of the Strategic Action Field framework, I highlight how field dynamics are shaped through framing contests and reflected in the practices of policy production.

Keywords: Nascent fields; framing; strategic action fields; cyber capacity building; Deloitte

Introduction

The notion of emerging issues in transnational public administration has recently begun to attract interest in public administration scholarship (Stone & Ladi, 2015). Coordination on these issues often occurs in multi-actor and multi-level policy fields with overlapping or ambiguous mandates (Bryson, Crosby, & Stone, 2015). For nascent issues, it has been suggested that the institutional environment resembles a marketplace for ideas inhibited by a transnational policy community (Brütsch & Lehmkuhl, 2007; Stone, 2008). Public sector officials, international civil servants and transnational policy professionals occupy this "global agora" (Stone, 2013). Consultancies are an important part of this policy community (Bouteligier, 2011; Linovski, 2019; Stone & Ladi, 2015), but their role remains underspecified. This paper highlights framing and positioning as crucial strategies of global consultancies when engaging in emerging policy issues.

Research on the role of consultants in public administration has typically focused on the role of consultancies in domestic public administration and often in the context of new public management reforms, highlighting a power shift from public administrations to private professional service firms (Arnaboldi, 2013; Gunter, Hall, & Mills, 2015; Martin, 1998; Saint-Martin, 1998; Ylönen & Kuusela, 2019). More recently, research has highlighted the "market-making" role of Global Professional Service Firms (GPSFs), combining management consultancy with other professional services. These firms construct nascent policy fields by advancing established practices into new jurisdiction or creating demand for solutions to previously not treated problems (Beaverstock, Faulconbridge, & Hall, 2010; Brès & Gond, 2014; Faulconbridge & Muzio, 2017; O'Mahoney & Sturdy, 2016).

Adding to these accounts, this paper advances a strategic action field understanding of how GPSFs engage in the framing and shaping of nascent transnational issues (Fligstein & McAdam, 2012). The strategic action field approach has recently attracted interest among scholars of public administration (Ingold, 2018; Moulton & Sandfort, 2017; Sandfort, 2018). It advances a view of embedded action in which strategic actors compete and cooperate for control over shared meanings (Fligstein, 1996). The ability of actors to successfully engage in such meaning-making projects is conditioned by political opportunity structures at the field level and the social skill to enlist others into coalitions (Fligstein, 2001).

In nascent fields, definitional struggles over rules, resources and actor roles are "front and center" (Fligstein & McAdam, 2012, p. 27). Skillful actors engage in these struggles by translating rules and resources from proximate fields and build coalitions around these frames (Fligstein & Dauter, 2007). Framing has been a prominent concept within public administration scholarship (Baekkeskov, 2011; Boin, 't Hart, & McConnell, 2009; McCann, 2013; Vogel, 2012; Wilkinson, Lowe, & Donaldson, 2010) and refers to discursive acts that "lay the ground for proposing and justifying change measures" (McCann, 2013, p. 5, *see also* Boin et al., 2009). Timing is important and framing during the early stages of field formation weighs heavily on the future development of the field, defining legitimate means and desirable ends (Benford & Snow, 2000; Bryson et al., 2015).

Within public administration scholarship, framing contests are typically initiated by public officials during periods of crisis ('t Hart & Tindall, 2009; 't Hart, 2013; Boin et al., 2009). In this paper, I show how GPSFs engage in the strategic construction of a nascent transnational policy field by exploiting opportunity structures, skillfully offering their resources while maintaining a notion of neutrality and building alliances. This strategic action is not one of domination, as a conventional 'market makers' narrative would suggest (c.f. Beaverstock et al., 2010; Faulconbridge & Muzio, 2017). Rather, they 'seed the cloud' and intervene strategically to shape a consensus on norms about routine practices and appropriate behavior.

To illustrate this process, the case of cyber capacity building (CCB) is presented. Located at the nexus between cybersecurity and development aid, CCB refers to efforts aimed at improving the ability of recipient constituencies to reduce digital risks in the global South (Pawlak, 2014, 2018). Officially recognized by the United Nations in 2010, the field remains in the early stages of coordinating actors for an open, safe and secure cyber space. CCB is a central component to allow developing nations to reap the "digital dividends" from rapidly spreading digital technologies around the globe (DfID, 2018; OECD, 2012; Principles for Digital Development, 2019; United Nations, 2013; World Bank, 2016). Meanwhile, GPSFs have identified CCB as an opportunity to invest in the formation of a future market opportunity.

Empirically, the paper employs an abductive approach and draws on participant observations during conferences and workshops of the Global Forum of Cyber Expertise (GFCE), a close reading of the literature, and semi-structured interviews with key actors. Grounded in an exploratory design, the activities of Deloitte emerged as a crucial case (Gerring, 2007). This paper

is structured as follows: In the first two sections, I provide an overview of the literature on consultancies within nascent fields and introduce the strategic action field approach. Third, methods and data collection are discussed. Fourth, the case is presented. In the subsequent sections, I provide an analysis of the strategic engagement of Deloitte in the field of CCB. In the final section, the link between framing strategies and field development is discussed.

Global Professional Service Firms in Nascent Fields

Diane Stone introduced the *global agora* as a metaphor for the market of ideas found in transnational administration, which is populated by a transnational policy community that spans international civil servants, public officials and transnational policy professionals (Stone, 2013, p. 28). In the global agora, actor roles are highly dynamic. Private actors can engage in public policy design negotiations, drawing on soft forms of authority to steer the governance process – sometimes against the will of public sector officials (Meier & García, 2015).
Previous research on consultancies within transnational administration provides evidence that global consultancies have taken on key tasks within these processes (Boussebaa & Faulconbridge, 2018; Momani, 2017; Seabrooke & Sending, 2020). Similarly, it has been recognized that GPSFs are expanding activities into new markets as the profitability of core services are decreasing (Greenwood, Suddaby, & Hinings, 2002; Kipping, Bu, & David, 2019; Suddaby & Greenwood 2001). With recognized expertise across policy, management, and technical fields, these firms are uniquely positioned to participate in the global agora and engage in agenda-setting exercises for complex policy problems at the transnational level. The ability to draw upon multifaceted expertise places GPSFs as the "obligatory passage points" for public administrations to inform decision-making processes when uncertainty over appropriate courses of action prevails (Editor's introduction to this symposium).

Complementing economies of knowledge, GPSFs control global networks spanning business, political, and civil society communities. These networks provide access to situated knowledge that links global expertise and local networks (Momani, 2017), affording GPSFs to exercise "design power" over institutional arrangements (Boussebaa & Faulconbridge, 2018) and to act as "staging posts" for political and economic transformations (Faulconbridge & Muzio, 2017, p. 222). Prince (2012) highlights the horizontal diffusion of policies through networks that are

maintained by consultancies, which he depicts as “the often unheralded foot soldiers of changing governance structures” (p. 200).

The ability to leverage expertise across geographies and issue areas allows GPSFs to act as knowledge brokers (Brès & Gond, 2014). The global operations of GPSFs provide unique opportunities to identify the ‘big picture’, acting as early-movers on emerging issue fields (Momani, 2017, p. 248). Dense networks to political, business, and civil society actors can be leveraged to shape perceptions and set the agenda for future courses of action (David, Sine, & Haveman, 2013; O’Mahoney & Sturdy, 2016).

While this literature has greatly added to our understanding about the resources employed by GPSFs, there has been a tendency to focus on outcomes of ‘consultocracy’ (Ylönen & Kuusela, 2019) with little attention to the underlying processes that allowed GPSFs to arrive in central positions. However, GPSFs cannot drive issues alone. Research on the effect of consultants on urban policy developments suggests that transnational consultancies aim to foster a position as neutral observers to the political process, operating at ‘modest witnesses’ (Hurl, 2018). From this position, consultancies broker alliances and organize consensus positions through active framing of contentious issues, oftentimes relying on pro-bono work to create future contracting opportunities (Canata & Giangreco, 2011; Linovski, 2017; Vogelpohl & Klemp, 2018).

In the transnational arena, this implies a focus on the strategies employed to enroll state, IO and non-state actors into alliances, and a deeper appreciation of the institutional context in which such actions take place. The agora metaphor suggests that such processes operate both in the transnational context as well as along ‘imperial’ lines, in which knowledge creation and policy options are shaped in imperial centers and transferred to former colonies (Stone, de Oliveira & Pal, 2020, p. 3). Shared conceptual frames and language facilitate this process, especially in the Anglosphere, as has been noted in public administration scholarship (Legrand, 2015; Broome and Seabrooke 2015). Similarly, the ability of global consultancies to operate across transnational and imperial networks has been extensively documented (Boussebaa, Morgan & Sturdy, 2012; Poullaos & Sian, 2010; Sian, 2011). Accounting for organizing processes in such multi-actor and multi-level environments, recent scholarship has turned to the strategic action field framework (Canzler, Engels, Rogge, Simon, & Wentland, 2017; David et al., 2013; Kauppinen, Cantwell, & Slaughter, 2017).

Field Emergence and Framing Contests

Within the strategic action field framework, fields are embedded social spaces of interdependent relationships, from which actors use social skill to access resources and influence how the field operates (Fligstein & McAdam, 2012, p. 59). In the context of global public policy, this perspective directs analytical focus away from the unitary action of policy entrepreneurs and emphasizes instead the interplay of resources, networks and interdependent action to shape the rules of the field (Fligstein, 1996; Santos & Eisenhardt, 2009).

The process of field emergence is a period of contention and uncertainty (Fligstein & McAdam, 2012). In the absence of institutional settlements, proximate fields can serve as yard sticks for importing rules and norms governing behavior (Fligstein & Dauter, 2007; Fligstein & McAdam, 2012, p. 86). Actors with the ability to bridge fields can exert a lasting influence on the development of shared meanings and rules (Bryson et al., 2015; Fligstein, 2001).

Skilled social actors exploit openings at the field-level to "motivate cooperation in other actors by providing those actors with common meanings and identities in which actions can be undertaken and justified" (Fligstein, 1997, p. 398). Fundamentally, the challenge for strategic actors is to frame their preferred line of action to induce the cooperation of others (Fligstein, 2001, p. 113). For emerging fields, frames are used to create alliances and confer legitimacy to a preferred course of action (Freeman & Peck, 2007; Heimstädt & Dobusch, 2018; Vogel, 2012).

Because nascent fields lack a shared understanding over rules, framing contests are significant for the definition of what types of resources are important, how best practices are established, and what actions are good and legitimate (Cornelissen & Werner, 2014, pp. 197–198; Kaplan, 2008). In doing so, strategic actors charge narratives with persuasiveness and can draw upon positive messaging, turning problems into opportunities and opening new courses of action (Crosby, 't Hart, & Torfing, 2017; Kennedy & Fiss, 2009, Vogel, 2012, p. 373).

As the field settles, previously contested processes become normalized. Framing can thus become an effective strategy to define solutions and working processes, placing oneself at the center of institutional settlements. Hence, an investigation of framing processes in nascent fields provides for an explanation of how the foundations for institutional outcomes such as 'consultocracy' are being laid.

Data and Approach

Empirically, this paper relies on an exploratory design of *polymorphus engagement* (Gusterson, 1997) informed by a close reading of documents, participant observations at key sites and semi-structured interviews with key informants. Nascent fields in transnational policy processes can be challenging to study as actors, sites and issues are dispersed globally and oftentimes only loosely connected. Exploratory research is a useful approach to identify emerging structures of the field and avenues for further data gathering (Stebbins, 2001, p. 6). An overview over the full data is provided in table 1.

As an initial step, documents on cyber capacity building were sourced. Specialized academic writings were identified through 'Web of Science' based on the key words "Cybersecurity Capacity Building", "Cyber Security Capacity Building" and "Cyber Capacity Building". Organizational reports from public and private organizations were identified based on references in the academic literature. Due to the novelty of the issue and the limited specialized academic literature available, additional material was sourced by conducting a Google News Search on the same key words as for the initial specialized literature in the Web of Science, yielding another five relevant articles. In total, this resulted in 51 documents. A close reading of this literature was conducted to gain an initial understanding of central concepts and concerns. Coordinative challenges, a shortage of funding, a lack of integration with traditional development actors, and a scarcity of qualified personnel emerged as central concerns (e.g. Hohmann, Pirang & Benner, 2017; Klimburg & Zylberberg, 2015; Morgus, 2018; Pawlak, 2018).

The Global Forum for Cyber Expertise was quickly identified as the central coordinating body of the field, being referenced in 8 of the 11 specialized articles and in the official strategies on cybersecurity and digitalization of the Netherlands, Norway and the United Kingdom. In-person participant observations were conducted at the 2019 Working Group Meetings in the Hague and the 2019 Annual Conference in Addis Ababa in Ethiopia over a total of six days. Further twelve hours of observations were made during virtual meetings in April-June 2020. At the physical gatherings, I attended all meetings and took extensive notes, which were transformed into memos. The in-person meetings were also used for informal background conversations with practitioners. These data were used to critically assess the results from the initial analysis, and to gain insights on dominant discourses and actors within the community (Mintrom & Luetjens, 2016).

This abductive approach proved valuable to uncover emerging patterns and dynamics of the field, which were not visible from a reading of the literature alone (Davies, 2001, p. 75). During the first round of participant observations at the working group meetings in 2019, Deloitte was identified as a *crucial case* (Gerring, 2007) due to its centrality in discussions. While single-case studies only allow for limited insights into market effects more generally (Leander, 2005), they are a viable approach for understanding nascent fields and open up for subsequent comparative approaches (Heimstädt & Dobusch, 2018).

Finally, eight formal interviews with key informants have been conducted. All interviews were conducted in a semi-structured manner with the aim to identify and confirm framing strategies and actor roles. Interview partners were sampled in a purposive manner based on a close reading of the literature and observations at key events. All interviewees were granted full anonymity. Due to the small-N character of interviews, no coding strategy was applied. In this way, the interviews were used to triangulate between data sources and increase the credibility of findings (Tansey, 2007).

Table 1: Empirical Materials and Data Sources

Data	*Sub-types*	*Count*
Documents	Specialist articles on cyber-capacity building	11
	Think-tank/research institute reports	8
	National Strategies	9
	IO Reports/Guidance	18
	Newspaper/other media	5
	Total	51
Participant observations	2019 GFCE Working Group Meetings, the Hague	3 days
	2019 Annual Meeting, Addis Ababa, Ethiopia	3 days
	2020 Virtual Working Group Meetings	12 hours
Interviews	A1: Gesellschaft für Internationale Zusammenarbeit (GIZ), *Senior Official*	26.11.2018
	A2: Independent Development Consultant	23.09.2019
	A3: European Union Institute for Security Studies (EUISS), *Senior Researcher*	24.02.2020
	A4: World Bank, *Senior Official*	27.02.2020
	A5: Deloitte, *Partner*	06.02.2020 04.12.2020
	A6: Deloitte, *Consultant*	09.09.2020
	A7: Small Consultancy, *CEO*	26.08.2020

Cyber Capacity Building as a Nascent Field

CCB refers to a range of activities collectively aimed at improving the ability of individuals, communities, and governments to reduce digital risks through the development of appropriate institutional, legal, and human capacities (Pawlak, 2018). Notwithstanding the importance of capacity building across the globe, the concept of CCB refers explicitly to a donor-recipient relationship in the context of development aid (Hohmann, Pirang, & Benner, 2017; Schia, 2018). Although the earliest CCB projects can be traced back to the mid-2000s (Collett, 2019), the concept became formally constituted by the group of governmental experts within the United Nations (UN GGE) in the 2010 report and reiterated through the 2013 and 2015 reports (United Nations, 2010, 2013, 2015).

Digital technologies are a key driver of economic growth in the global South (World Bank, 2008, p. 2) and development institutions across the board have incorporated digital solutions into their strategies (DfID, 2018; Sida, 2003, 2005; Utenriksdepartementet, 2018). The World Bank estimates that at least 80% of its projects have digital components (Sargent, 2017). Without adequate safeguards to address digital risks, the positive impact of digital technologies on development might be offset or even reversed (World Bank, 2016, pp. 3–4). Against this rise of "the dark side of ICT" (Deibert, 2013; Tarafdar, Gupta, & Turel, 2015), the OECD emphasized "a need for better alliances and partnerships with like-minded countries or allies, including facilitating capacity building of less developed countries" (2012, p. 13), and the Principles for Digital Development recognize privacy and security as fundamental building blocks of digital development projects (Principles for Digital Development, 2019).

CCB is, however, more than a new feature of development policy (Schia & Willers, 2020). It pursues a threefold aim of economic and societal growth, global risk mitigation and geopolitical ambition: First, to provide a foundation for developing countries to reap digital dividends. Second, to strengthen the global security landscape as exposure in one country easily spills-over into other – including developed – countries. And third, to advance and promote a model of digital governance rooted in the notions of openness, freedom, and security (Klimburg & Zylberberg, 2015; *see also* Pawlak & Barmpaliou, 2017).

Whereas renowned experts imagined CCB growing into "one of the most important activities within the security/development nexus" (Klimburg & Zylberberg, 2015, p. 5; see also Pawlak, 2016, p. 85), annual funding remains on the margins of the US$ 153 billion market for official development aid (OECD, 2019). Estimations fluctuate between US$ 50 million and 1 billion

annually, with a mean between 100 and 300 million US-dollars (Morgus, 2018, pp. 29, 70). If the market for CCB has not yet lived up to early expectations, it is due to three major challenges: a lack of expertise, a lack of funding, and organizational complexity. First, the digital skills gap puts pressure on traditional recruitment channels (Berger & Frey, 2015, p. 77), as public and private organizations compete for a limited pool of talents, and private actors typically outspend public institutions (Andrews, 2018, p. 7). With a global shortage of two million cybersecurity experts (ISACA, 2019), practitioners with deep technical knowledge are rare and expensive (Shires, 2018). Second, the hybrid character of CCB projects – being both development and security projects – creates uncertainty as to its qualification as official development assistance in conjunction with the ODA guidelines (Klimburg & Zylberberg, 2015; Pawlak, 2018, p. 49). If development projects cannot be classified as ODA, donor countries are less likely to allocate funding.

Finally, the coordinative challenge to navigate organizational complexity has led to duplications of efforts, constrained the efficient delivery of projects and spurred uncertainty as to the impact of initiatives (Dutton, Creese, Shillair, & Bada, 2019). Building capacity in developing countries requires the participation of actors from the technical, development, security, and diplomatic communities to produce coherent programs and frameworks (c.f. Pawlak & Barmpaliou, 2017). Working across these communities requires boundary-spanning skills and the development of brokerage knowledge (Pollitt, 2010). Silo-structured bureaucratic organizations are especially constrained by this condition (Klimburg, 2017). Critically, mediating between security and development communities has proven difficult (Hohmann et al., 2017; Klimburg & Zylberberg, 2015; Morgus, 2018). Without the enrolment of the development community, CCB projects often lack access to local networks in recipient states (Pawlak, 2014; Pijnenburg Muller, 2015, p. 14) and suffer from supply- rather than demand driven project designs (Pawlak, 2018, p. 100). CCB therefore risks to repeat the mistakes of early digital development projects (Heeks, 2008).

In 2015, acknowledgement of this coordinative challenge induced the United Kingdom and the Netherlands to launch the Global Forum for Cyber Expertise (GFCE). This multi-stakeholder platform brings together public officials, international organizations, development actors, research institutes, and private companies to advance a global agenda for CCB and avoid duplications of efforts (GFCE, 2015). Within the few years of its existence, it has developed into the key global coordinative body for CCB issues.

In sum, CCB has developed from a loosely articulated recommendation at the level of the United Nations into a nascent global policy field. Coordination among the relevant communities remains the biggest challenge for effective policy implementation. Coordinative platforms, such as the GFCE, tend to be dominated by actors from the security and foreign policy community. Without access to the local networks and capacity building expertise of the development community, CCB projects risk to be short-lived as local ownership is lacking (c.f. Eade, 1997).

The Strategic Action Field in Cyber Capacity Building

The GFCE functions as the main coordinating platform in the nascent field (c.f. Netherlands Ministry of Justice, 2018; UK Cabinet Office, 2016; Utenriksdepartementet, 2018). As of early 2020, its members include 54 countries, 14 international organizations, 12 research institutes/think tanks, 17 for-profit companies, four non-profits and eight other organizations from around the world. These can be roughly clustered around donors, recipients and implementing actors. Within each of these categories, we see both private and public actors, mirroring Diane Stone's observation of the transnational sphere as penetrating dichotomies, where "policy activity does not conform to the standard distinction of simply public or private, but occurs across them" (Stone & Ladi, 2015, p. 843). For example, Microsoft is a key investor into CCB activities (GFCE, 2020b; *see also* Pijnenburg Muller, 2015) and academic organizations like the Oxford University's Global Cyber Security Capacity Centre are active in project implementation and assessments (GCSCC, 2016).

Consultancies are, however, the main implementing agents (Interview, A4 & A7; see also Morgus, 2018, p. 53; Pawlak & Barmpaliou, 2017). The GFCE member consultancies are of three types: smaller and specialized consultancies; medium-sized thematic consultancies with a regional focus; and GPSFs. The difference in size and function corresponds to public administration scholarship on smaller consultancies providing technical fixes, mid-size consultancies policy changes for a community, and large consultancies a shift in frames (van den Berg et al., 2019). Smaller and specialized technical companies are typically contracted for the implementation of specialized aspects of larger projects, such as the development of national computer emergency response teams (Interview, A7). Mid-sized consultancy firms like the consultancy arm of the Commonwealth Telecommunication Organisation (CTO) tend to have a broader portfolio and a regional focus area. Created in 1901, the CTO draws on a centuries-long

legacy serving the Commonwealth region in fostering the use and application of telecommunications technologies. Access to long-standing local networks and a deep understanding of the local political and societal context are a crucial resource and success factor for project implementations (Interviews A3, A4, A5).

Lastly, recent years have seen a strong increase in the activities of especially one GPSF in delivering CCB projects. In the autumn of 2016, Deloitte acquired the small consultancy firm Intellium, which was specialized on cyber security strategy consulting for public and private clients (Deloitte, 2017). Prior to the acquisition, Intellium supported Italy in developing the 2016 National Framework for Cyber Security, worked with the International Telecommunication Union (ITU) on cyberdrills in the African, American, European, and Arab regions (ITU, 2014, 2015a, 2015b, 2016), and supported NATO in critical infrastructure protection exercises (NATO, 2015). Leveraging Intellium's issue-specific expertise and existing networks with Deloitte's organizational capacity followed thus a well-known model of niche firm acquisitions for expanded service offerings (Accountancy Daily, 2015).

Framing the Strategic Action Field

Access to greater organizational capacity allowed the new Deloitte/Intellium consortium to work with longer time horizons without a need for immediate profit. Consequently, the GPSF used the newly acquired technical expertise to move from being a specialized agent with limited capacity towards viewing cyber capacity building as a strategic investment for future profit opportunities.

> Cyber capacity building has over time become a priority for Deloitte and is part of a long-term strategy. Other companies need to focus more closely on the immediate profitability when approaching new markets. Deloitte – as a partner-led organization – is much better positioned to invest in these areas with a long-term strategy.
>
> Interview A5

Most significantly, this re-orientation was manifest in the development of a second strategic layer, leveraging the combination of top management consultancy and technical expertise to

engage in ‘thought-leadership’ and framing of the field (O’Mahoney & Sturdy, 2016; Sturdy, Wright, & Wylie, 2015a). These strategies are exemplary of the move towards CCB activity as an investment strategy.

With less focus on short-term performance, *pro-bono* work was a viable strategy to increase its presence in the emerging market. It has been documented elsewhere, how pro bono activities can be used to build reputation and demonstrate capabilities, and how unpaid work can create opportunities for future contracts (Linovski, 2017). Through the provision of in-kind contributions to cyberdrills, the company has become an official ‘key partner’ of the ITU (ITU, 2019). Further, Deloitte is similarly engaged in training national computer emergency response teams through the ITU, using this activity as a hub for network expansion. Beyond network expansion, pro bono work for governments through the ITU was used to stay ahead of the field and maintain thought leadership (Interview A5).

Testament to such thought leadership is the development of the 2018 “Guide to Developing a National Cyber Security Strategy” on a pro bono basis (ITU, World Bank, COMSEC, CTO, & NATO CCD COE, 2018). Published by a multi-stakeholder effort including the ITU, the World Bank, NATO, and the European Cybersecurity Agency (ENISA), Deloitte was able to assert its status as a leading source of expertise. Relatedly, Deloitte has published a “Digital Identity Road Map Guide” in cooperation with the ITU (ITU, 2018). Digital identity systems are closely linked to cybersecurity concerns and a key pillar of the World Bank’s digital development program (World Bank, 2018). Another example is the publication of the edited volume “Next Generation CERTs” through the “NATO Science for Peace and Security Programme” (Armando, Henauer, & Rigoni, 2019).This collaboration draws together the GPSF, NATO, and a prominent computer scientist, reaffirming the technical expertise of Deloitte and fostering ties to complementary sources of authority. These three examples underpin, how Intellium’s existing networks within the ITU and NATO could be leveraged to engage in strategic positioning within a long-term investment strategy.

The publication of best-practice guides are important tools to set standards of appropriate behavior and provide an opportunity to formalize social standing and strengthen relationships to relevant other stakeholders (c.f. Qu & Cooper, 2011). Entering into strategic cooperation with partner organizations, the cooperative approach allowed Deloitte to advance diagnostic and prognostic frames (Benford & Snow, 2000). Relying on a narrow representation of technical

expertise, Deloitte was able to exercise a high degree of control without the need to mobilize its full arsenal of organizational resources, reflecting Hurl's notion of global consultancies as 'modest witnesses' (Hurl, 2018).

Thought leadership and framing strategies went, however, beyond representations of technical expertise. The GFCE, as the central coordinating body of the nascent field, was identified as an arena of eminent importance to engage directly in conversations with donor and recipient state governments (Interviews 5,6,7). As one interviewee put it, "these conversations are important to understand the priorities of governments *and to help them understand their needs*" (Interview 5, emphasis added).

Deloitte's engagement at the GFCE relied much more heavily on brokering and framing strategies based on its organizational resources and access to global networks. Interventions during working group sessions in April 2019 revolved around a re-framing of local project ownerships, emphasizing the need to bring together local project partners and establishing multi-stakeholder initiatives that allow for demand-driven project design and sustainable project success.

This re-framing directly addresses a shared concern as lined out in the case description: the absence of the development community has cut CCB projects effectively out of local networks that development agencies maintain across the globe. The importance of project ownership for achieving sustainable development outcomes is well-established (Eade, 1997) and similarly a concern that is widely shared in the CCB community (Pawlak, 2014; Pijnenburg Muller, 2015; Schia, 2018). Yet, as local ownership requires the presence of implementing actors with the social capital to orchestrate local networks, alternative pathways are in high demand and consultancies with a global presence are in a unique position to act on such tasks.

Indeed, the ability of turning global presence into a strategic advantage in future CCB projects was highlighted decisively:

> Deloitte has extensive experience in dealing with private companies and can help to bring them in and make them an active part of the discussion. The latter is an area where most CCB projects are failing in design and execution. But

> national private players and large international companies are essential for successful projects, especially for national strategies.
>
> Interview A5

Deloitte only became a formal member of the GFCE in 2019. Yet, within a short period of time, it managed to take on central positions within the working groups on national strategies and cybersecurity cultures and skills[1]. Further, Deloitte senior partner Inge Bryan was appointed to the three-person board of the newly established GFCE foundation. At the presentation of the board during the 2020 working group meetings, the main task of the board was described as to provide strategic direction to the GFCE and move CCB closer to the digital development agenda (GFCE, 2020a). According to Deloitte's Inge Bryan, two key considerations for such development must be a "better involvement of the private sector and a new and more active role of the GFCE" (speech at GFCE Virtual Meeting, 2020). The latter should be contrasted with the expressly passive role of the GFCE in earlier years, limiting itself to a coordinative function (Interview A4). This was reiterated in a later interview:

> In the future, the GFCE should become more like a market place in which recipients, donors and other relevant organizations can interact and coordinate. Ideally, the GFCE should facilitate the organization, strategy development and orchestration of CCB projects.
>
> Interview A5

As CCB remains on the margins of the digital development field and both the market itself and market players are only just emerging, Deloitte ensured through its work at the GFCE that it is a player that cannot be ignored. Taking on key positions within the forum allows for the exercise of design power over the future organization of the field. Strategic re-framing of shared concerns over a lack of local project ownership opened new business opportunities to capitalize on the GPSF's global presence and ability to orchestrate public-private partnerships.

This framing soon appeared in the World Bank Report on the lessons learned from the Global Cybersecurity Capacity Program. Deloitte was the main implementing agency in this program,

[1] In toto, the GFCE is structured around four working groups.

advising on risk assessment and management processes, the development of national cyber strategies, and the identification of critical information infrastructure (World Bank, 2019, pp. 22–25, 46).

> Consultancy firms with presence on the local market have more comprehensive and deeper knowledge about the needs and current circumstances of the given country. Global expertise combined with local knowledge is key to providing professional high-quality services to governmental institutions. This outlined advantage can result in a more successful and efficient achievement of Program goals. Programs similar to the Global Cybersecurity Capacity Building Program might benefit from the identification of such consultancy firms by already implementing partners at early stages of the Program planning. Timely and regular involvement of consultancy firms from the very first steps of the Program activities can lead to a higher utilization of the local knowledge and expertise of the parties involved.
>
> (World Bank, 2019, p. 66).

The wording of "global expertise combined with local knowledge" is a clear reference to GPSFs who can leverage global networks and multi-faceted expertise. The involvement of GPSFs is argued to improve the chances of success and they should be involved "from the very first steps of the Program activities" to bring local knowledge to project planning, allowing for a demand-driven project design.

In sum, the case of Deloitte is a crucial illustration of how GPSFs possess unique resources to exert a lasting impact on the formation of nascent field within transnational policy issues. Access to global networks and organizational resources allows for the investment into nascent fields that do not yet represent a market large enough to provide short-term profits. Skillful positioning placed the GPSF in a structurally advantageous position to identify opportunity structures that can be exploited through targeted framing strategies. It has been documented how such framing was rewarded, enlisting central donor agencies into the prognostic frame. Such strategies are not very costly for a globally operating consultancy although the immediate pay-

off might be low. Taking a back-seat and intervening strategically allows them to “seed the cloud” and shape future market profiles.

Discussion

Global consultancy firms possess unique resources to play an important part in the administration of transnational policy issues and especially so during the formative stages of field emergence. As documented in the case study, Deloitte was able to strategically invest into the nascent field of CCB before significant market opportunities developed, shaping the organization of CCB activities and normalizing its own position as an obligatory passage point for the implementation of CCB projects.

While previous scholarship on consultancy in domestic public administrations has emphasized how GPSFs engage in thought leadership to establish new issues (Momani, 2017; Sturdy et al., 2015b), the presented case highlights how such activities are embedded within wider social processes in which the inscription of thought-leadership activities into best practice guides is as much a reflection of claims to epistemic authority as it is a positioning exercise to foster and cement organizational alliances with key actors (see also Hurl, 2018). Organizational financial resources are the foundation to engage in such longer-term strategies, while the organizational structure of the partnership model provides the necessary discretion for senior partners to take a longer outlook on investments and rely less on immediate returns than traditionally organized private actors.

Conceptualizing these processes as strategic action fields provides an integrated reading of what otherwise oftentimes is treated as individual aspects of consultancy resources. It also provides an important processual element in which social skill is developed and nurtured over time, underlining the significance of early-stage investments into nascent issue fields. Understood in this way, the successful re-framing of contentious issues around local ownership and demand-driven project designs, with an emphasis on public-value creation, was possible only because the underlying processes of alliance-building were enabled. Deloitte had the capacity to read the environment through continuous skillful engagement. The GPSF was able to place itself in the center of framing, including advantageously positioning itself close to the World Bank.

In many ways CCB represents a natural expansion of Deloitte's services. Government and public services account for the consultancy's third largest global revenue stream (Deloitte, 2020b) and its cybersecurity consulting remains the world's largest by market share (Deloitte, 2020a). Exercising design power over the development of CCB practices allows for the marriage of existing profit centers with the capitalization of global networks while avoiding clashes with incumbent competitors and professions coming into the market. As such, Deloitte has put in the work to make the most of increased service delivery and profits as the market matures.

This is significant for two reasons. First, it documents how international development is increasingly seen as a target of knowledge colonization for GPSFs (Seabrooke & Sending, 2020; Suddaby & Greenwood 2001). And second, it documents how global consultancies are an important part of the transnational agora with access to a unique set of resources and the ability to build up social skill over time and to 'seed the cloud' on emerging issues before market structures develop.

Conclusion

How do global consultancies contribute to the shaping of nascent transnational public policy fields? Departing from the observation that GPSFs are an understudied actor type in the global agora, this paper has advanced a case study on the early-stage investment of Deloitte into the nascent field of cyber capacity building.

Through a reading of the global agora as a strategic action field, this work contributes to our understanding of how the combination of organizational resources and social skill are equally important elements in GPSFs' strategies to develop alliances and shape the formation of settlements within nascent fields. The advantage of such an approach is that it allows us to interpret the strategic action of global consultancies from an integrated view. From this perspective the processes of knowledge colonialization and market-making cannot be separated from the institutional environment in which such action is embedded. Further, the concept of social skill highlights how strategic action is the outcome of mobilization and coalition-building which, in turn, is underpinned by the deployment of organizational resources and an ability to read the environment in order to develop effective framing strategies. Applying the strategic action field approach asks us to take a holistic view of the knowledge-producing, boundary-

spanning, and thought leadership activities of global consultancies. It is these activities that underpin the ability to engage in skillful social action. In this way, Deloitte's actions can be interpreted as an investment into the development and acquisition of social skill which is deployed in a forward-looking manner to 'seed the cloud' and normalize itself to act as a staging post as market opportunities increase. Paying closer attention to such early-stage engagement of global consultancies within nascent transnational issues should be an interesting avenue for further research.

Global consultancies are, unquestionably, not the only strategic actors investing into the development of nascent transnational issue arenas. Nor is their involvement necessarily a cause of concern but it is an issue worthy of further research interest. The global agora simultaneously exhibits a high degree of openness and power asymmetries (Stone, 2003). Consultancies working transnationally are well positioned to both contribute to and exploit this system. In this paper, it has been documented that GPSFs can successfully place themselves as central actors during early stages of field formation, providing them with design power over the form and practice of global public policy. Given the extensive research on GPSFs' propensity to reproduce global inequalities and post-colonial structures, future research would be well-advised to pay close attention to the effects of such 'seeding' activity.

References

't Hart, P, & Tindall, K. (2009). *Framing the global economic downturn: Crisis rhetoric and the politics of recessions*. Canberra, Australia: ANU Press.

't Hart, Paul. (2013). After Fukushima: Reflections on risk and institutional learning in an era of mega-crises. *Public Administration*, *91*(1), 101–113. https://doi.org/10.1111/padm.12021

Accountancy Daily. (2015). *Consulting: Big Four target niche firms to expand service offering*. *July*. Retrieved from https://www.accountancydaily.co/consulting-big-four-target-niche-firms-expand-service-offering

Andrews, L. (2018). Public administration, public leadership and the construction of public value in the age of the algorithm and 'big data.' *Public Administration*. https://doi.org/10.1111/padm.12534

Armando, A., Henauer, M., & Rigoni, A. (2019). An Introduction to CERT Types, Services and Organization Models. In *NATO Science for Peace and Security Programme*. Amsterdam: IOS Press.

Arnaboldi, M. (2013). Consultant-Researchers in Public Sector Transformation: An Evolving Role. *Financial Accountability & Management*, *29*(2), 140–160. https://doi.org/10.1111/faam.12008

Baekkeskov, E. (2011). Issue framing and sector character as critical parameters for government contracting-out in the UK. *Public Administration*, *89*(4), 1489–1508. https://doi.org/10.1111/j.1467-9299.2011.01948.x

Beaverstock, J. V., Faulconbridge, J. R., & Hall, S. J. E. (2010). Professionalization, legitimization and the creation of executive search markets in Europe. *Journal of Economic Geography*, *10*(6), 825–843. https://doi.org/10.1093/jeg/lbp058

Benford, R. D., & Snow, D. A. (2000). Framing Processes and Social Movements : An Overview and Assessment. *Annual Review of Sociology*, *26*, 611–639.

Berger, T., & Frey, B. (2015). Bridging the Skills Gap. In *Technology, globalisation and the future of work in Europe: Essays on employment in a digitised economy*. London: IPPR.

Boin, A., 't Hart, P., & McConnell, A. (2009). Crisis exploitation: Political and policy impacts

of framing contests. *Journal of European Public Policy*, *16*(1), 81–106. https://doi.org/10.1080/13501760802453221

Boussebaa, M., & Faulconbridge, J. (2018). Professional service firms as agents of economic globalization: a political perspective. *Journal of Professions and Organization*, *6*(1), 72–90.

Boussebaa, M., Morgan, G., & Sturdy, A. (2012). Constructing global firms? National, transnational and neocolonial effects in international management consultancies. *Organization Studies*, 33(4), 465-486.

Bouteligier, S. (2011). Exploring the agency of global environmental consultancy firms in earth system governance. *International Environmental Agreements: Politics, Law and Economics*, *11*, 43–61. https://doi.org/10.1007/s10784-011-9149-7

Brès, L., & Gond, J. P. (2014). The visible hand of consultants in the construction of the markets for virtue: Translating issues, negotiating boundaries and enacting responsive regulations. *Human Relations*, *67*(11), 1347–1382. https://doi.org/10.1177/0018726713519278

Broome, A., & Seabrooke, L. (2015). Shaping policy curves: Cognitive authority in transnational capacity building. *Public Administration*, 93(4), 956-972.

Brütsch, C., & Lehmkuhl, D. (2007). *Law and legalization in transnational relations*. London: Routledge.

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2015). Designing and Implementing Cross-Sector Collaborations: Needed and Challenging. *Public Administration Review*, *75*(5), 647–663. https://doi.org/10.1111/puar.12432

Canato, A., & Giangreco, A. (2011). Gurus or wizards? A review of the role of management consultants. *European Management Review*, 8(4), 231-244.

Canzler, W., Engels, F., Rogge, J. C., Simon, D., & Wentland, A. (2017). From "living lab" to strategic action field: Bringing together energy, mobility, and ICT in Germany. *Energy Research and Social Science*, *27*, 25–35. https://doi.org/10.1016/j.erss.2017.02.003

Collett, R. (2019). Project Mapping Tool. Retrieved December 6, 2019, from https://www.capacitylabs.org/projects

Cornelissen, J. P., & Werner, M. D. (2014). Putting Framing in Perspective: A Review of Framing and Frame Analysis across the Management and Organizational Literature. *Academy of Management Annals*, *8*(1), 181–235. https://doi.org/10.1080/19416520.2014.875669

Crosby, B. C., 't Hart, P., & Torfing, J. (2017). Public value creation through collaborative innovation. *Public Management Review*, *19*(5), 655–669. https://doi.org/10.1080/14719037.2016.1192165

David, R. J., Sine, W. D., & Haveman, H. A. (2013). Seizing opportunity in emerging fields: How institutional entrepreneurs legitimated the professional form of management consulting. *Organization Science*, *24*(2), 356–377. https://doi.org/10.1287/orsc.1120.0745

Davies, P. H. J. (2001). *Spies as Informants : Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services*. *21*(1), 73–80.

Deibert, R. J. (2013). *Black code: Surveillance, Privacy, and the Dark Side of the Internet*. Oxford: Signal.

Deloitte. (2017). Deloitte Risk Advisory acquisisce Quantum Leap | Deloitte Italy | Risk Advisory. Retrieved December 11, 2020, from https://www2.deloitte.com/it/it/pages/risk/articles/deloitte-risk-advisory-acquisisce-quantum-leap---deloitte-italy-.html

Deloitte. (2020a). Deloitte ranked No. 1 by revenue in Security Consulting Services globally according to Gartner | Deloitte Global. Retrieved December 14, 2020, from https://www2.deloitte.com/ru/en/pages/about-deloitte/press-releases/2020/deloitte-ranked-no--1-by-revenue-in-security-consulting-services.html

Deloitte. (2020b). Global Impact Report. Performance: By the numbers. Retrieved December 14, 2020, from https://www2.deloitte.com/global/en/pages/about-deloitte/articles/global-report-revenue.html

DfID. (2018). *Digital strategy 2018-2020: Doing development in a digital world*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701443/DFID-Digital-Strategy-23-01-18a.pdf

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity. *Journal of Information Policy*, *9*, 280–306. https://doi.org/https://doi.org/10.5325/jinfopoli.9.2019.0280

Eade, D. (1997). *Capacity-building: An approach to people-centred development*. Oxford: Oxfam.

Faulconbridge, J., & Muzio, D. (2017). Global professional service firms and institutionalization. In L. Seabrooke & L. F. Henriksen (Eds.), *Professional Networks in Transnational Governance* (pp. 219–232). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316855508.014

Fligstein, N. (1996). Markets as Politics : A Political-Cultural Approach to Market Institutions. *American Sociological Review*, *61*(4), 656–673.

Fligstein, N. (1997). Social Skill and Institutional Theory. *American Behavioral Scientist*, *40*(4), 397–405. https://doi.org/10.1177/07399863870092005

Fligstein, N. (2001). Social Skill and the Theory of Fields. *Sociological Theory*, *19*(2), 105–125.

Fligstein, N., & Dauter, L. (2007). The sociology of markets. *Annual Review of Sociology*, *33*, 105–128. https://doi.org/10.1177/001139287035001012

Fligstein, N., & McAdam, D. (2012). *A theory of fields*. Oxford: Oxford University Press.

Freeman, T., & Peck, E. (2007). Performing governance: A partnership board dramaturgy. *Public Administration*, *85*(4), 907–929. https://doi.org/10.1111/j.1467-9299.2007.00683.x

GCSCC. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Oxford.

Gerring, J. (2007). Is there a (viable) crucial-case method?. *Comparative political studies*, 40(3), 231-253.

GFCE. (2015). *Launch of the Global Forum on Cyber Expertise The Hague Declaration on the GFCE*.

GFCE. (2020a). GFCE V-Meeting: Meet & Greet with the GFCE Foundation Board – Global Forum on Cyber Expertise. Retrieved December 15, 2020, from https://thegfce.org/gfce-v-meeting-meet-greet-with-the-gfce-foundation-board/

GFCE, T. (2020b). GFCE and Microsoft announce an investment partnership in Cybersecurity

Capacity Building in Africa – Global Forum on Cyber Expertise. Retrieved December 11, 2020, from https://thegfce.org/gfce-and-microsoft-announce-an-investment-partnership-in-cybersecurity-capacity-building-in-africa/

Greenwood, R., Suddaby, R., & Hinings, C. R. (2002). Theorizing Change: The Role of Professional Associations in the Transformation of Institutionalized Fields. *The Academy of Management Journal*, *45*(1), 58–80. https://doi.org/10.2307/3069285

Gunter, H. M., Hall, D., & Mills, C. (2015). Consultants, consultancy and consultocracy in education policymaking in England. *Journal of Education Policy*, *30*(4), 518–539. https://doi.org/10.1080/02680939.2014.963163

Gusterson, H. (1997). Studying Up Revisited. *PoLAR 20, 114*.

Heeks, R. (2008). ICT4D 2.0: The Next Phase of Applying ICT for International Development. *Computer*, *41*(6), 26–33. https://doi.org/10.1109/MC.2008.192

Heimstädt, M., & Dobusch, L. (2018). Politics of Disclosure: Organizational Transparency as Multiactor Negotiation. *Public Administration Review*, *78*(5), 727–738. https://doi.org/10.1111/puar.12895

Hohmann, M., Pirang, A., & Benner, T. (2017). Advancing Cybersecurity Capacity Building Implementing a Principle-Based Approach. *Global Public Policy Institute (GPPi)*.

Hurl, C. (2018). Operationalizing austerity: the role of transnational professional service firms in local government restructuring. *Innovation: The European Journal of Social Science Research*, 31(1), 55-67.

Ingold, J. (2018). Employer engagement in active labour market programmes: The role of boundary spanners. *Public Administration*, *96*(4), 707–720. https://doi.org/10.1111/padm.12545

ISACA. (2019). *State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development*. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2019-part-1_res_eng_0319.pdf?regnum=500542

ITU. (2014). *Cyberdrill for Africa*. Livingstone, Zambia.

ITU. (2015a). *Regional Cyber Drill for the Arab Region*. Hurghada, Egypt.

ITU. (2015b). *Regional Forum on Cyber Security for the Americas Region*. Bogota, Colombia.

ITU. (2016). *Cyberdrill for Arab Region*. Yassmine Hammamet.

ITU. (2018). *Digital Identity Road Map Guide*.

ITU. (2019). Global Partnership. Retrieved February 11, 2020, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-partnership.aspx

ITU, World Bank, COMSEC, CTO, & NATO CCD COE. (2018). *Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity*. Retrieved from www.itu.int

Kaplan, S. (2008). Framing contests: Strategy making under uncertainty. *Organization Science*, *19*(5), 729–752. https://doi.org/10.1287/orsc.1070.0340

Kauppinen, I., Cantwell, B., & Slaughter, S. (2017). Social mechanisms and strategic action fields: The example of the emergence of the European Research Area. *International Sociology*, *32*(6), 796–813. https://doi.org/10.1177/0268580917726630

Kennedy, M. T., & Fiss, P. C. (2009). Institutionalization, framing, and diffusion: The logic of TQM adoption and implementation decisions among U.S. hospitals. *Academy of Management Journal*, *52*(5), 897–918.

Kipping, M., Bu, F., & David, T. (2019). Professionalization through symbolic and social capital : Evidence from the careers of elite consultants. *Journal of Professions and Organization*, *6*(3), 265–285.

Klimburg, A. (2017). *The Darkening Web: the war for cyberspace*. London: Penguin.

Klimburg, A., & Zylberberg, H. (2015). *Cyber Security Capacity Building: Developing Access*.

Leander, A. (2005). The market for force and public security: The destabilizing consequences of private military companies. *Journal of Peace Research*, *42*(5), 605–622. https://doi.org/10.1177/0022343305056237

Legrand, T. (2015). Transgovernmental policy networks in the Anglosphere. *Public Administration*, 93(4), 973-991.

Linovski, O. (2017). Pro Bono Practices and Government Agencies. *Journal of the American Planning Association*, *83*(2), 180–182. https://doi.org/10.1080/01944363.2016.1277779

Linovski, O. (2019). Shifting Agendas: Private Consultants and Public Planning Policy. *Urban Affairs Review*, *55*(6), 1666–1701. https://doi.org/10.1177/1078087417752475

Martin, J. F. (1998). *Reorienting a nation: consultants and Australian public policy*. Surrey, UK: Ashgate.

McCann, L. (2013). Reforming public services after the crash: the roles of framing and hoping. *Public Administration*, *91*(1), 5–16. https://doi.org/10.1111/padm.12016

Meier, H. E., & García, B. (2015). Protecting private transnational authority against public intervention: Fifa's power over national governments. *Public Administration*, *93*(4), 890–906. https://doi.org/10.1111/padm.12208

Mintrom, M., & Luetjens, J. (2016). Design Thinking in Policymaking Processes: Opportunities and Challenges. *Australian Journal of Public Administration*, *75*(3), 391–402. https://doi.org/10.1111/1467-8500.12211

Momani, B. (2017). Professional management consultants in transnational governance. In L. Seabrooke & L. F. Henriksen (Eds.), *Professional Networks in Transnational Governance* (pp. 245–265). Oxford: Oxford University Press. https://doi.org/10.1017/9781316855508.016

Morgus, R. (2018). *Securing Digital Dividens - Mainstreaming Cybersecurity in International Development*. Washington, DC: New America.

Moulton, S., & Sandfort, J. R. (2017). The Strategic Action Field Framework for Policy Implementation Research. *Policy Studies Journal*, *45*(1), 144–169. https://doi.org/10.1111/psj.12147

NATO. (2015, July 29). NATO - News: Enhanced cyber defence cooperation in the South Caucasus and Black Sea region, 29-Jul.-2015. Retrieved December 12, 2020, from https://www.nato.int/cps/en/natohq/news_121969.htm

Netherlands Ministry of Justice. (2018). *A cyber secure Netherlands - National Cyber Security Agenda*.

O'Mahoney, J., & Sturdy, A. (2016). Power and the diffusion of management ideas: The case of McKinsey & Co. *Management Learning*, *47*(3), 247–265. https://doi.org/10.1177/1350507615591756

OECD. (2012). Cybersecurity Policy Making at a Turning Point. In *OECD Digital Economy Papers* (Vol. 211). https://doi.org/http://dx.doi.org/10.1787/5k8zq92vdgtl-en

OECD. (2019). *Development aid drops in 2018, especially to neediest countries*. Retrieved from https://www.oecd.org/development/development-aid-drops-in-2018-especially-to-neediest-countries.htm

Pawlak, P. (2014). *Riding the digital wave: The impact of cyber capacity building on human development*. https://doi.org/10.2815/43313

Pawlak, P. (2016). Capacity Building in Cyberspace as an Instrument of Foreign Policy. *Global Policy*, *7*(1), 83–92. https://doi.org/10.1111/1758-5899.12298

Pawlak, P. (2018). *Operational Guidance for the EU's international cooperation on cyber capacity building*. https://doi.org/10.2815/38445

Pawlak, P., & Barmpaliou, P.-N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy*, *2*(1), 123–144. https://doi.org/10.1080/23738871.2017.1294610

Pijnenburg Muller, L. (2015). *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*.

Pollitt, C. (2010). Technological Change: A Central yet Neglected Feature of Public Administration. *NISPAcee Journal of Public Administration and Policy*, *3*(2), 31–53. https://doi.org/10.2478/v10110-010-0003-z

Poullaos, C., & Sian, S. (Eds.). (2010). Accountancy and empire: The British legacy of professional organization. London: Routledge.

Prince, R. (2012). Policy transfer, consultants and the geographies of governance. *Progress in Human Geography*, *36*(2), 188–203. https://doi.org/10.1177/0309132511417659

Principles for Digital Development. (2019). Principles. Retrieved January 21, 2020, from https://digitalprinciples.org/principles/

Qu, S. Q., & Cooper, D. J. (2011). The role of inscriptions in producing a balanced scorecard. *Accounting, Organizations and Society*, 36(6), 344-362.

Saint-Martin, D. (1998). The new managerialism and the policy influence of consultants in

government: An historical-institutionalist analysis of Britain, Canada and France. *Governance, 11*(3), 319–356. https://doi.org/10.1111/0952-1895.00074

Sandfort, J. R. (2018). Theoretical foundations and design principles to improve policy and program implementation. In E. Stazyk & H. Frederickson (Eds.), *Handbook of American Public Administration* (pp. 475–496). https://doi.org/10.4337/9781786432070.00039

Santos, F. M., & Eisenhardt, K. M. (2009). Constructing markets and shaping boundaries: Entrepreneurial power in nascent fields. *Academy of Management Journal, 52*(4), 643–671. https://doi.org/10.1109/ccst.1991.202189

Sargent, S. (2017). *World Bank Donor Perspective on Cyber Security*.

Schia, N. N. (2018). The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly*, *39*(5), 821–837. https://doi.org/10.1080/01436597.2017.1408403

Schia, N. N., & Willers, J. O. (2020). Digital Vulnerabilities and the Sustainable Development Goals in Developing Countries. *Industry, Innovation and Infrastructure*. Springer.

Seabrooke, L., & Sending, O. J. (2020). Contracting development: managerialism and consultants in intergovernmental organizations. *Review of International Political Economy*, 27(4), 802-827, https://doi.org/10.1080/09692290.2019.1616601

Shires, J. (2018). Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance*, *6*(2), 31–40. https://doi.org/10.17645/pag.v6i2.1329

Sian, S. (2011). Operationalising closure in a colonial context: The Association of Accountants in East Africa, 1949–1963. *Accounting, Organizations and Society*, 36(6), 363-381.

Sida. (2003). *Digital Empowerment – A Strategy for ICT for Development (ICT4D) for DESO*. Stockholm, Sweden: Swedish International Development Cooperation Agency

Sida. (2005). *Strategy and Action Plan for ICT in Development Cooperation*. Stockholm, Sweden: Swedish International Development Cooperation Agency

Stebbins, R. A. (2001). *Exploratory research in the social sciences*. Thousand Oaks, CA.: SAGE.

Stone, D. (2003). The "knowledge bank" and the global development network. Global Governance: *A Review of Multilateralism and International Organizations*, 9(1), 43-61.

Stone, D. (2008). Global Public Policy , Transnational Policy Communities , and Their Networks. *Policy Studies*, *36*(1), 19–38.

Stone, D. (2013). *Knowledge actors and transnational governance : The private-public policy nexus in the global agora*. London: Palgrave Macmillan.

Stone, D., & Ladi, S. (2015). Global public policy and transnational administration. *Public Administration*, *93*(4), 839–855. https://doi.org/10.1111/padm.12207

Stone, D., Porto de Oliveira, O., & Pal, L. A. (2020). Transnational policy transfer: the circulation of ideas, power and development models. *Policy and Society*, 39(1), 1-18.

Sturdy, A., Wright, C., & Wylie, N. (2015a). Management as consultancy – a case of neo-bureaucracy. In *Management as Consultancy* (pp. 1–13). https://doi.org/10.1017/cbo9781139108065.001

Sturdy, A., Wright, C., & Wylie, N. (2015b). Neo-bureaucratic management and consultancy. In *Management as Consultancy* (pp. 14–42). https://doi.org/10.1017/cbo9781139108065.002

Suddaby, R., & Greenwood, R. (2001). Colonizing knowledge: Commodification as a dynamic of jurisdictional expansion in professional service firms. *Human relations*, 54(7), 933-953.

Tansey, O. (2007). Process tracing and elite interviewing: A case for non-probability sampling. *PS - Political Science and Politics*, *40*(4), 765–772. https://doi.org/10.1017/S1049096507071211

Tarafdar, M., Gupta, A., & Turel, O. (2015). Introduction to the special issue on "dark side of information technology use." *Information Systems Journal*, *25*(4), 315–317. https://doi.org/10.1111/isj.12076

UK Cabinet Office. (2016). *The UK cyber security strategy: Annual Report*. (April), 1–43. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

United Nations. (2010). *A /65/201*. New York. United Nations.

United Nations. (2013). *A /68/98**. New York. United Nations.

United Nations. (2015). *A /70/174*. New York. United Nations.

Utenriksdepartementet. (2018). *Digital strategi for utviklingspolitikken*.

van den Berg, C., Howlett, M., Migone, A., Howard, M., Pemer, F., & Gunter, H. M. (2019). *Policy Consultancy in Comparative Perspective*. https://doi.org/10.1017/9781108634724

Vogel, R. (2012). Framing and counter-framing new public management: The case of germany. *Public Administration, 90*(2), 370–392. https://doi.org/10.1111/j.1467-9299.2011.01981.x

Vogelpohl, A., & Klemp, F. (2018). The creeping influence of consultants on cities: McKinsey's involvement in Berlin's urban economic and social policies. *Geoforum*, 91, 39-46.

Wilkinson, K., Lowe, P., & Donaldson, A. (2010). Beyond policy networks: policy framing and the politics of expertise in the 2001 foot and mouth disease crisis. *Public Administration, 88*(2), 331–345. https://doi.org/10.1111/j.1467-9299.2010.01831.x

World Bank (2008). Global economic prospects 2008: Technology diffusion in the developing world. The World Bank

World Bank. (2016). Digital Dividends. In *World Development Report*. Washington, DC: World Bank.

World Bank. (2018). *Identification for Development 2018 Annual Report*. Washington, DC: World Bank.

World Bank. (2019). *Global Cybersecurity Capacity Program - Lessons Learned and Recommendations towards strengthening the Program.*

Ylönen, M., & Kuusela, H. (2019). Consultocracy and its discontents : A critical typology and a call for a research agenda. *Governance, 32*, 241–258. https://doi.org/10.1111/gove.12369

ARTICLE 3: Linked ecologies for inscription-building in unstable markets: The emergence of cyber risk insurance

Linked ecologies for inscription-building in unstable markets: The emergence of cyber risk insurance

Co-authored article with Leonard Seabrooke. Currently under review with Accounting, Organizations, and Society.
Co-author statements can be located at the very end of this dissertation.

Abstract

Markets are stabilized through a combination of professional coordination and technological rationalization that permits product delivery and valuation. Here we examine the emergence of cybersecurity insurance, a new market that requires multi-professional cooperation among an array of uncoordinated product service providers. In this context some professionals are attempting to build relationships to give stability to the market, and to permit the inscription of quantitative risk assessment methods. We suggest such relations are part of a general process, where 'linked ecologies' are being created by professionals to permit the conditions for inscription at a distance to function. We synthesize the inscription and linked ecologies approaches to establish three phases in which professional coordination and technological rationalization can proceed. First, emergent technologies require professional coordination which, when established, permits a second phase of calibration around a strategic technology, including what can be quantified. Only if a consensus is reached can a third phase of inscription occur, which creates a purified technology that can operate at a distance and has ongoing distributive effects among professional groups. We provide evidence from a 'live' case on cybersecurity insurance that draws on interviews with practitioners, extensive participant observation, and document analysis from industry reports.

Keywords: cybersecurity; insurance; linked ecologies; inscription; technology; markets.

"It's kinda a crappy job to be a chief security officer...
It's like being a [chief financial officer] before accounting was invented"
- Alex Stamos, former chief security officer (CSO) at Facebook [1]

Introduction

It is a truism to suggest that markets of significant scale rely on a calculative rationality to combat instability. The development of calculation techniques and devices is a classic Weberian theme that underpins the development of accountancy and modern capitalism (Carruthers & Espeland, 1991; Miller & Napier, 1993). The regularization of calculation generally follows the establishment of professional coordination on who is tasked with authority over the diagnosis, inference, and treatment of a problem, and what jurisdictional protections they should be afforded (Abbott, 1988). When task allocation has been settled among the relevant professionals, technological rationalization can aide market stability, permitting predictable product delivery and valuation. Further regularization can be achieved through inscriptions – practices and technologies that are mobile, "immutable, presentable, readable, and combinable" (Latour, 1986, p. 7). The implementation of calculative devices to simplify and standardize valuation can then magnify the scale of both professional and market activity. We know that inscriptions can be associated with performativity effects that generate disruptions (MacKenzie, 2006), as well as hardening the homo economicus myth (Taffler, Spence, & Eshraghi, 2017). These processes, associated with technological rationalization, rest on prior professional coordination.

We examine this general proposition through a case on the rise of the market for cyber risk insurance. This market has developed over the past two decades, emerging in a piecemeal and fragmented fashion, with little alignment among the cybersecurity and insurance professionals on best practices, product development, and valuation. This market has been characterized by an extreme proliferation of products that do not align into profiles where their quality and predictability could be easily discerned by clients. This profiling capacity is fundamental for stable markets (White, 1981; Beckert, Rössel, & Schenk, 2017), and particularly important for market upscaling through the inclusion of small and medium enterprises (SMEs).

Despite a lack of coherence in the supply of products, demand for cyber risk insurance has increased. The heightened frequency of cyber-attacks demanding corporate ransom payments, as well as more mundane cyber threats, have accelerated this demand. In recent years this has spurred some cybersecurity and insurance professionals to create alliances, generating schemes to foster an understanding of what constitutes cybersecurity risks and insurance valuation, as well as developing quantified measures that can support insurance products at a scale that can anchor greater market stability.

The process of developing quantifiable measures is familiar to scholars working in the tradition of the sociology of translation (Callon, 1980), which draws attention to the processes through which sites, activities, and interactions are assembled into networks. In particular, research on the construction of inscriptions (Latour, 1987; Justesen & Mouritsen, 2011) specifies "how complex and distant relations come through, often multiple, translations to be inscribed and "represented" by singular objects" (Robson & Bottausci, 2018, p. 61). The process of inscribing is a subset of translation with material artefacts and has become a prominent feature within critical accounting literature (Busco & Quattrone, 2018; Jordan, Mitterhofer, & Jørgensen, 2018; Qu & Cooper, 2011; Robson, 1992). For most of this literature, the engagement with inscriptions - in the form of standards, best practices, calculations, or risk metrices – problematizes the performativity of management and accounting practices (Busco & Quattrone, 2015; Cooper, Ezzamel, & Qu, 2017).

An important aspect of research on inscriptions is the stability of the professional environment in which calculative devices can take hold. 'Inscription building' (Qu & Cooper, 2011) is a process of alliance building and network formation (Callon, 1986) that relies on professionals and technologies using social space to 'make an object known' (Robson, 1992, p. 689). While the performative power of inscriptions derives from the institutionalized nature of centers of calculations (Callon, 1998), inscription-building relies on intersubjective meaning exchanges between proximate and distant agents. In short, the presence of 'inscriptors' relies on successful prior professional coordination (Qu & Cooper, 2011, p. 345). In our case on cyber risk insurance, multi-professional cooperation has emerged transnationally in the absence of a dominant form of professionalization in one type of organization or a national jurisdiction where the state licenses the professions (Faulconbridge & Muzio, 2012; Blok et al., 2019; Harrington & Seabrooke, 2020). As a consequence, it is professionals that have driven attempts to bring

together cybersecurity and insurance to work on developing products that can potentially be inscribed to stabilize the market.

To locate the process through which multi-professional cooperation enables technological rationalization, we draw on the concept of 'linked ecologies' (Abbott, 2005), which examines how actors form alliances and compete with each other to have control over a 'location' (point of interest). Such control may include jurisdictional control over the allocation of professional tasks (Abbott, 1988). Linked ecologies do not only include formal professions but also other actors and organizations. Activity within linked ecologies is focused to develop relations that connect actors and locations in the struggle to define tasks (Abbott, 2005, p. 248–52). Actors can create strategies to influence each other, including forging common projects across groups ('hinges') and in propagating one's own perspective in other groups ('avatars'). This approach has been applied in a number of issue areas of interest to scholars of accounting and organization, including auditing (Mennicken, 2010), business school education (Fourcade & Khurana, 2013), life insurance (van der Heide, 2020), and financial surveillance (Seabrooke & Tsingou, 2021), among others.

While work on inscription and linked ecologies are seldom in conversation, we suggest that combining insights from them can aide the theorization of processes linking professional coordination to technological rationalization. In particular, we contribute to theorizing about the cooperative and competitive processes underpinning inscription-building, highlighting how it relies on links between professional groups (Robson & Bottausci, 2018). We also show that professional groups do not function independently of technological rationalizations. We suggest that market stability is the outcome of a process where professionals compete in establishing what is regular activity in the market and who has claims to what tasks. Inscription-building relies on this process to get a foothold in asserting what is best practice valuation.

We make three distinct contributions. First, by linking the inscription and linked ecologies frameworks, we articulate a process of professional interaction that assists with inscription-building and attempts to create technologies can aide market stability. Second, we highlight how the formation of 'hinges' allows translation over distance, providing evidence on how the selection of what can be quantified is calibrated within a social space populated by professionals and technologies. And third, we draw attention to the relationship between the process of inscription-building and change in hierarchies among professional groups.

Empirically, our case on cybersecurity insurance draws on 20 interviews with practitioners, extensive participant observation at online conferences, and document analysis from industry reports. We exploit this 'live' case to gain traction on how multi-professional cooperation and competition is acted out, and to trace the process through which inscription-building is staged. Geographically, our focus is on the North American and European markets, which account for the clear majority of written premiums in this new market. After a brief overview over the work on inscriptions and linked ecologies, we present our theoretical framework, highlighting the intricate relationship between professional competition over authority claims and inscription-building. This is followed by a methodology section prior to the case presentation and analysis section before we discuss the contributions.

Inscriptions

Inscriptions are a core concern for work in the Sociology of Translation (Robson & Bottausci, 2018). While translations refer to an actor's interpretation of their own and others interest (Latour, 1987, p. 108), inscriptions describe the mobile, stable, and combinable representations of translations that enable action at a distance (Latour, 1987, p. 236). Their significance stems from a mediating capacity, tying together networks around problematizations (Morgan & Morrison, 1999). Inscriptions can help to make things "calculable" and quantifiable (Miller, 1991; Power, 2003), providing for the dissemination of problematizations as "light travelers" across organizational and institutional settings (Kurunmäki, Lapsley, & Miller, 2011, p. 4). Since quantification remains the hallmark of knowledge representations (Robson, 1992, p. 687; Mennicken & Espeland, 2019), inscriptions serve as rationalization devices (Vollmer, Mennicken, & Preda, 2009).

Scholarship on accounting and organization typically engages with inscriptions post-fact and investigates the performative capacity of inscriptions as actants (Busco & Quattrone, 2015, 2018; Pollock & D'Adderio, 2012; Power, 2004; Quattrone, 2009). Inscriptions, in this work, take on performative qualities by producing the world that they represent (Callon, 1998; Themsen & Skærbæk, 2018, p. 20). In doing so, inscriptions identify and describe actions derived from a particular representation of calculability (Callon, 1998, pp. 4–5) and shape human cognition (Latour, 1986). What once was controversial becomes constructed as unchallenged facts through processes of purification, including the 'blackboxing' of input

variables in the calculative device (Latour, 1987, p. 246; Latour, 1999, p. 304). In this line of thinking accounting ideas, once widely accepted, become the 'obligatory passage points' that define problems and solutions (Cooper, Ezzamel, & Qu, 2017). 'Ranking devices' become a constitutive aspect of market settings (Pollock & D'Adderio, 2012, p. 584). Concurrently, the incompleteness of inscriptions facilitates continuous processes of re-interpretation that themselves are defined through the visual power of representations (Busco & Quattrone, 2015).

The performative capacity of rankings and other inscriptions has featured particularly prominently in work on risk management. Hilgartner classically argued that "definitions of risk get built into technology and shape its evolution" (Hilgartner, 1992), and Power has drawn attention to the various ways in which risk indices take on "a life of their own" and define policy options (Power, 2004, p. 771). Such formalized risk management templates narrow courses of action and can lead to a compliance rather than resilience focus (Hall & Fernando, 2016), with an emphasis on flexibility of application rather than their accuracy (Jordan, Mitterhofer, & Jørgensen, 2018). In sum, inscriptions focus rationalization processes, folding in what counts and can be counted, and normalizing this behavior through the use of technologies so that professionals do not question it.

The durability of an inscription derives from its mobility and flexibility, allowing actors to modify the tool in its application without, however, challenging the underlying representation; namely that what is represented indeed is risk. This is often a fragile process. Inscription-building relies on the ability of fact-builders to create "communities of interest" by enrolling actors into alliances and closing down areas of contestation (Latour, 1987, p. 112). In this sense, inscription-building "ignite[s] the process of knowledge fabrication" (Quattrone, 2009, p. 89) and reflects the construction of consensus-positions among relevant actors over what is important and what is not (Qu & Cooper, 2011, p. 347).

As discursive strategies involve understanding and strategic framing, the main actors in inscription-building are individuals and groups with an interest in how the object becomes constituted and defined. This, we propose, diminishes the role of non-human actants during periods of inscription-building to strategic devices employed by human actors in their pursuit to build alliances and align interests (Eyal, 2012, p. 181). In Callon's words (1980, p. 198):

> The protagonists are involved in a never ending struggle to impose their own definitions and to make sure that their view of how reality should be divided up prevails. Consensuses are reached, lasting for longer or shorter periods of time, concealing balances of power. […] During these preliminary skirmishes research problems and the groups which will take charge of them are simultaneously determined.

Inscription-building is foremost a process concerned with the forging of qualified consensuses around good and bad, pure and impure, input variables (Vollmer, Mennicken, & Preda, 2009, p. 623; Christensen & Skærbæk, 2010, p. 525). During this process, proto-inscriptions remain a property of the human agents, who strategically employ material representations of risk objects to enroll others into coalitions. Only in later phases, if successful, can this prior phase enable the agency of actants to facilitate networks at a distance (Latour, 1987, p. 232). Scholars working in this tradition have noted that it is important to "recognize explicitly the role of strategic agency in building networks and in influencing relational effects" (Cooper, Ezzamel, & Qu, 2017, p. 997). We suggest that the linked ecologies framework promises to provide important insights into these processes.

Inscription-Building in Linked Ecologies

The linked ecologies framework emerged from work on the systems of professions (Abbott, 1988) with recognition that professional coordination does not come from only inter- and intra-professional conflicts (Abbott, 2005). The linked ecologies approach is based on a critique of classic ecological conceptions of social space as bounded by individual competition among fixed entities, where there are strong assumptions of what binds an ecology together. Instead, Abbott (2005) perceives of social space as a shared arena, populated by actors and institutions that interact around a focal object. This ecological social space is not determined by pre-existing positions but actively created through the interaction of actors, the location (points of interest), and the economic, political, and social activities involved in interactions. The emphasis in the approach is on the "overlapping and interpenetrating of previously distinct worlds... [where] arenas and fields themselves come to be interlinked and reworked (Mennicken, 2010, p. 335, emphasis in original). Actors share an interest in this object, allowing one to trace how it

emerges as a focal point of contention. As any successful claim to the location must enlist actors across ecologies, the most important variable is alliance-building (Abbott, 2005, p. 247). Such alliance-building is concerned with the establishment of 'ligations', connecting actors, locations, and relations between them. These include 'hinge' strategies to link professional groups, as well as 'avatar' strategies to influence worldviews in other groups.

The linked ecologies framework has variously been applied to study aspects of control over tasks and issue areas. Technological rationalizations and forms of calculation are important for this professional interaction. For example, Mennicken (2010) details how former Soviet calculative practices and inspection technologies were reworked through professional interaction to transform auditing practices in Russia. Seabrooke and Tsingou (2016) show how professional conflicts between demographers, medical scientists, and economists over fertility have led to changes in the economic calculus of assisted reproduction technologies. Abbott's own work discusses how professional settlements include claims over technological advances, as, for example, in the attribution contest over who invented the whale harpoon gun (Abbott, 2001, pp. 209–239).

The linked ecologies framework can provide an important addition to the literature on inscriptions by highlighting how alliance-building on emergent issues is defined by multi-professional struggles over control. In return, a focus on inscription-building helps us understand how "points of contact" are not only limited to physical human interactions but can be widened through the inscription of rationalities across ecologies in situations of sparse personal contact (c.f. Abbott, 2005, p. 253).

Linked Ecologies for Inscription-Building

Connecting the work of linked ecologies with that of inscriptions allows us to understand inscription-building as a general process with recursive dynamics. During the initial phase, proto-inscriptions can be employed as tools to build alliances and align interests. Characteristic of this phase is that proto-inscriptions do not yet possess performative characteristics as they lack widespread acceptance. In Abbott's (2005) terms, they can function as 'hinges' to build alliances between professionals, who primarily act through groups. Competing inscriptions carry contrasting implications for the allocation of problems and tasks among professionals and, in doing so, can reorganize status hierarchies. Our contention is that inscription-building is an

inherently conflictual process that involves the mediation, shaping, and competition of competing interests and actor groups.

Figure 1 illustrates the phases of inscription-building and its relationship to professional groups in a process of technological rationalization within a market. We describe this recursive process as following three phases, acknowledging that this is not a global or universal process and that different professionals may be located in different phases in the same general period. In the first phase is an emergent technology, which has potential to concentrate activity within a market. The professional groups (A and B) both have an interest in the content of this emergent technology and in steering how it can be used to enhance their capacity for diagnosis, inference, and treatment. As the technology is emergent the chance to mold it may increase through active alliance building between professionals and organizations. Professionals have an incentive to create 'points of contact' and form a linked ecology that includes other organizations useful in enhancing their control of the 'location'. Market instability may accentuate distributional gains from such points of contact. Pressures in the external environment can affirm the need for the emergent technology to be treated as a strategic technology.

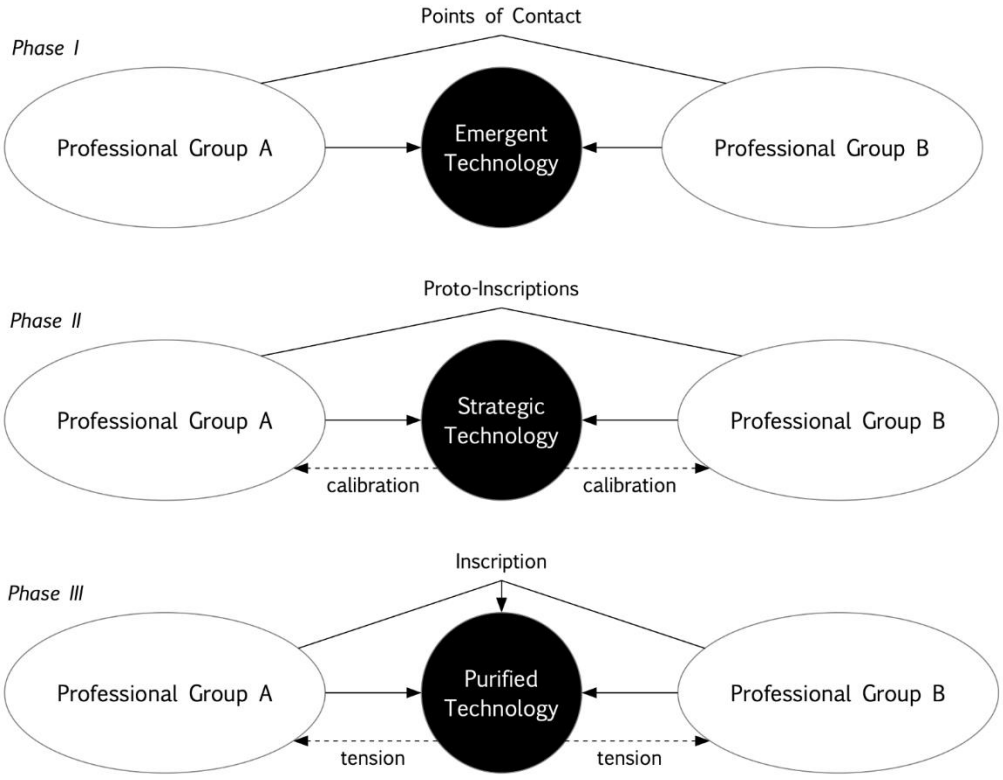


Figure 1: Linked Ecologies in Inscription-Building

In the second phase, the technology's potential to enhance particular behavior within the market makes it a strategic asset, which may be propelled by external pressures in the environment. Professionals have an interest in furthering alliance-building, and keeping out other competitors, by agreeing on forms of diagnosis, inference and treatment that will enhance the strategic technology in a manner that bolsters their jurisdictional control and aides market stability. Forming alliances with organizations that support this treatment is important in securing their control over the location in the linked ecology. Towards this aim a hinge can develop to tie the ecologies together in a manner directed towards the creation of proto-inscriptions. For example, in cases where forms of quantification are a key means of control both professional groups will propose what should be measured and counted. Linking proposals with other organizational actors can greatly assist this process. As these elements are introduced to the strategic technology this induces a calibration process, whereby the professional groups must select and deselect on what may eventually be inscribed.

In the third phase multi-professional coordination has led to an agreement around the technology, allowing for inscription to take place. This transforms the strategic technology – an object of contestation among professional groups – into a purified technology. In doing so, the technology becomes an actant that can operate at a distance, enfolding new professional groups and laypeople in the external environment into the activities the technology enables. This assists market stability and regularity, allowing the upscaling of activity and inclusion of many more organizations. We note that the distributional outcomes from the inscription may differ for the professional groups most concerned. This creates tensions that can lead to challenges to professional jurisdictional control (Kiviat, 2019), as well as forms of performativity in markets that have been well documented (e.g. Revellino & Mouritsen 2015). Extreme tensions may result in a reversion to the second phase, or in new efforts towards an emergent technology, as described in the first phase.

We suggest that the case of cybersecurity insurance follows the logic of these phases, with the current development between the second and third phase. As such this 'live' case provides insights into the relationship between professionals in linked ecologies and inscription-building.

Data and Methods

To analyze multi-professional organization and inscription-building, we draw upon a multi-method explanatory case study approach (Flyvbjerg, 2011), employing participant observation, semi-structured interviews, and a close reading of corporate and policy documents. We began the study with a broad search for relevant literature and policy documents. This provided an initial base for the mapping and identification of critical vantage points, actors and points of discussion. A Web of Science search for articles with the terms "cyber" and "insurance" in the title or keywords yielded a list of 150 academic articles published between 2010 and 2021. However, only 20 were anchored in the social and organizational sciences, while the vast majority were to be found within computer sciences and electronical engineering. We extended our search to include policy and practitioner documents, which proved a valuable strategy and identified a number of reports from international organizations (especially the Organisation for Economic Co-Operation and Development, hereafter OECD, and the European Union Agency for Cybersecurity, hereafter ENISA), industry associations (EIOPA, Geneva Association), major market actors (Lloyd's of London, Allianz, Zurich Re, Munich Re AXA, Chubb) and professional service firms (Deloitte, PwC, KPMG, EY).

Building upon this initial research phase, we advanced in the tradition of "netnography" to employ internet-based research techniques to locate sites, topics and people around a given issue (Kozinets, 2015). While such approaches typically focus on social media and other internet-based communities, our focus was to trace actors and practices in the cyber insurance arena. We followed online conference (live and recorded) and observed industry discussions in forums and webinars, accumulating 32 hours of direct participant observation. Many more hours were spent following cyber risk insurance online forums, which provided engagement with the professional community. In addition to these online discussions, we also undertook online training in cybersecurity insurance, led by a known practitioner in the field, and obtained a certificate in cyber risk management for insurance. This was primarily to ensure that we were informed about the key concepts, frames, and terms being used to bridge the cybersecurity and insurance professionals. Finally, we triangulated the data with the help of in-depth semi-structured interviews with industry insiders. Table 1 provides information on the interviewees, the interview format and participant observation venues. In total, we conducted 20 interviews, ranging between 30 minutes and two hours and 15 minutes, with a mean of just over one hour. Interviews were conducted between March 2020 and July 2021. All interviewees were granted

anonymity. During interviews, intensive hand-written notes were taken and subsequently transformed into detailed memos. In several cases, we exchanged several follow-up emails with those interviewed for clarifications and to approve the use of quotations.

Table 1: Empirical Materials

Interviews					
#	**Identifier**	**Sector**	**Date**	**Length**	**Position**
1	A1	Academia	09.03.2020	2 hours 15 minutes	Researcher
2	A2	Specialized Cyber Insurance Provider	13.01.2021	1 hour 30 minutes	CEO
3	A3	Insurance underwriting agency	14.01.2021	1 hour 12 minutes	Group Leader
4	A4	Insurance Broker	18.01.2021	1 hour 5 minutes	Senior Broker
5	A5	Insurance Company	22.01.2021	1 hour 15 minutes	Senior Underwriter
6	A6	Industry Association	22.01.2021	1 hour 10 minutes	Head of Section
7	A7	Insurtech Company	26.01.2021	35 minutes	CEO
8	A8	Insurtech Company	27.01.2021	55 minutes	Head of Insurance
9	A9	Insurance Broker	02.02.2021	1 hour 3 minutes	Head of Cyber Risk
10	A10	Insurance Agency	17.02.2021	Mail	Product Leader
11	A11	IT Security Consultancy	12.02.2021	1 hour	Senior Director
12	A12	Governmental Agency	22.02.2021	55 minutes	CISO
13	A13	Risk Modelling Company	09.03.2021	1 hour 5 minutes	Director
14	A14	Security Rating	10.03.2021	45 minutes	Senior Director
15	A15	Security Rating	11.03.2021	1 hour	President Sales
16	A16	Security Rating	15.03.2021	30 minutes	Director
17	A16	Security Rating	17.03.2021	45 minutes	Director
18	A17	Rating Agency	24.03.2021	1 hour	CEO
19	A18	Reinsurance Company	19.07.2021	56 minutes	Underwriter
20	A19	Reinsurance Company	20.07.2021	1 hour 7 minutes	Senior Underwriter

Conferences, Webinars, Training					
Name	**Type**	**Organizer**	**Date**	**Accessed**	**Duration**
The Role of Law and Government in Cyber Insurance Markets	Online Conference	University of Connecticut	12.03.2021	12.03.2021	5 hours
Cyber Risk Insights Conference	Online Conference	Advisen	24.-25.2.2021	24.-25.2.2021	3 hours
Cyber Insurance Summit	Online Conference	Blackhat 2019	07.08.2019	18.11.2020	2 hours 30 minutes
Plug and Play Winter Summit Insurtech	Online Webinar	Plug and Play Tech Center	19.11.2020	19.11.2020	3 hours 15 minutes
How insurers and startups are targeting the growing cyber insurance market	Online Conference Presentation	InsurTech Rising Europe	16.10.2018	21.12.2020	36 minutes
What does cyber insurance really bring to the table and…are you covered?	Online Conference Presentation	RSA Conference 2019	08.03.2019	17.11.2020	52 minutes
Virtual Cyber Risk Summit 2020	Online Conference	Net-diligence	30.06.-30.09.2020	23.02.2021	6 hours
Quantifying Cyber Risk	Webinar	ISACA	10.06.2021	14.07.2021	1 hour
Cyber Insurance and Risk Management Course	Online Course	cyRM	16.03.2020	16.03.2020	5 hours
Cyber Insurance Forum observation	CRIF – Cyber Risk & Insurance Forum	LinkedIn			5 hours

Case Context

Problems of risk definitions and valuation lie at the heart of cyber risk management (World Economic Forum, 2015). With the emergence of the cyber risk insurance industry, a distinct sector has developed to link the risk profiles of policyholders to premium categories and offer insured forms of protection against data breaches and cyberattacks (Lemnitzer, 2021). In its most basic form, cyber risk insurance allows organizations to transfer the financial risk of digital attacks to (re-)insurance carriers within a defined set of coverage areas (ENISA, 2016; OECD, 2017, 2020).

While the widespread marketization of cyber insurance products is a recent phenomenon, its history traces back at least twenty years with the first dedicated product brought to market in 1997 by AIG (Herr, 2021, p. 98). Institutionally, cyber insurance emerged out of errors and omissions ("E&O") policy coverage and targeted technology companies (Wrede, Stegen, & von der Schulenburg, 2020, p. 660). The initial uptake in the market was slow as digital risks were poorly understood and treated as exotic (Herr, 2021, p. 99). Since 2012 the market has experienced fast growth. With estimations of 25% compounded annual growth rates globally, it is among the fastest-growing insurance sectors (OECD, 2017, p. 60), accounting for an estimated US$ 4-5 billion in written premiums with over half of the market located in the United States (OECD, 2020). Beyond catering to individual demand, cyber risk insurance is increasingly recognized as a central pillar to improve societal resilience in the face of escalating threats to businesses and other organizational actors (ENISA, 2012, 2016; OECD, 2018; UK Cabinet Office, 2015). Despite growth in the market, cyber insurance providers have been pressed to accurately assess and price risks as traditional actuarial models cannot easily be transferred to new product lines (ENISA, 2016; Khalili, Liu, & Romanosky, 2019) and cyber risk insurance brokers lack the necessary expertise to identify risks and communicate insurance policies (Biener, Eling, & Wirfs, 2015; Kshetri, 2020, p. 5).

A particularly prominent problem for insurers has been the increased threat of ransomware. This is a digital extortion business model in which an attacker uses access to a victim's systems to encrypt data and only to release them for a defined amount of money to be transferred via cryptocurrencies. Over the past few years ransomware has evolved from being a minor risk factor to the most common cause of cyber related claims (Willis Towers Watson, 2020). Between 2015 and 2017, global ransomware-related damage is estimated to have increased from US$ 325 million to 5 billion and reached a staggering US$ 11.5 billion in 2019 (Taylor, 2020), causing significant deteriorations of insurers' loss ratios (Cordonnier, 2020). Against this backdrop of increasing professionalization in cybercrime (Insikt Group, 2021), security breaches increased by 27.4% in 2017 alone while the average cost for an organization falling victim to cybercrime increased by 72% between 2014 and 2018 (Ponemon Institute, 2017, 2019). Similarly, the number of cyber-related claims increased for some insurance providers close to ten-fold between 2016 and 2020 (Allianz, 2020), while demand for cyber risk insurance coverage boomed. The NotPetya and Wannacry cyberattacks showcased the contagion effects of

interconnectedness as infections spread within minutes around the world causing an estimated combined damage of US$ 15-18 billion (Hathaway, 2018; Wall, 2018).

Warren Buffett, the CEO of insurance behemoth Berkshire Hathaway, famously summarized the state of the industry at this time as follows: “I don’t think we or anybody else really knows what they’re doing when writing cyber” (Chiglinsky & Basak, 2018). Similarly, a recent review of the industry found cyber insurance to be “A booming phenomenon missing solid foundations”, highlighting the ‘inadequacy’ of pricing and risk assessment methodologies (Dambra, Bilge, & Balzarotti, 2020, p. 1367). With actuarial models unreliable, the most common underwriting approach is based on qualitative methods, typically in the form of questionnaires and client-meetings and sometimes supported by third-party risk assessments performed by specialized cybersecurity vendors (OECD, 2017, p. 14).

Consequently, cyber risk assessments are costly (Biener, Eling, & Wirfs, 2015, p. 145; Tøndel et al., 2016) and provide for only a limited snapshot picture as both questionnaires and interviews rely on the willingness and ability of policyholders to accurately represent or permit access to their IT-security and organizational procedures (Romanosky et al., 2019). In the absence of external guidance and regulation, risk assessment methodologies differ widely among insurance carriers, resulting in a fragmentation of product offerings and deviations in the diagnosis, inference, and treatment of cyber risks (ENISA, 2017). While this lack of harmonization has obvious ramifications for customers, insurers have equally recognized fragmentation of risk assessment methodologies as an obstacle to growth (ENISA, 2017, p. 44). A key aspect of such efforts is the establishment of knowledge-sharing mechanisms that ensure the productive translation of expert information on cyber risks across the social space.

Analysis: Proto-inscription-building in linked ecologies

Despite 20 years of market existence, a general lack of cyber-specific expertise remains a major barrier to growth of the cyber insurance industry, undermining the ability to price standalone policies and limiting insurance brokers in engaging with clients (Wrede, Stegen, & von der Schulenburg, 2020, p. 677; Kshetri, 2020, p. 5; Gerhards, 2018). To address fundamental questions of risk categorizations and valuation (Marotta et al., 2017), insurance professionals are increasingly building alliances with cybersecurity professionals to circumvent the lack of historical data and benchmark prices (EIOPA, 2018, p. 15). As the technical understanding takes

on a more central role in cyber insurance relative to traditional insurance lines (Grzadkowska, 2019; Kshetri, 2020, p. 5), the need for cross-industry and public-private collaboration is broadly acknowledged (EIOPA, 2018, p. 21; OECD, 2017, p. 8; Woods & Simpson, 2017). Historically, however, the creation of points of contacts between the professional ecologies remained scarce. The renowned 'Blackhat' cybersecurity conference, for example, premiered an insurance stream for the first time in 2019. Senior Vice-President at Chubb Insurance, Matt Prevost explains this lack of engagement on the basis of cultural barriers:

> [H]aving those conversations and cross-collaborations is what cyber insurance typically has not done. Our worlds have not collided, and there is a couple of reasons. We haven't interacted, we speak different languages, we dress differently, and it's easy to make fun of insurance.
>
> Matt Prevost, 2019[2]

The lack of a shared habitus has been an earlier impediment to multi-professional coordination for cyber risk insurance, and an important element for professionalization and market upscaling (e.g. Carter & Spence, 2014; Spence et al. 2017). Not surprisingly, then, to date no forum has developed that would successfully incorporate all of the relevant stakeholders and multi-professional cooperation occurs through direct attempts to produce common frames and procedures for cyber risk insurance (Woods & Simpson, 2017, p. 210).

Emergent Technology and Creating Points of Contact

In what can be understood as the first phase of inscription-building among the relevant professional groups, the insurance professionals recognized the need to link with cybersecurity professionals, and vice versa. Insurance professionals have been the most explicit in creating 'points of contact' to improve the underwriting of cyber risk. We identified three distinct strategies as part of this first phase: (1) In-sourcing specialized expertise, (2) build-up of internal knowhow through education and training, and (3) third-party contracting.

First, large insurers in-sourced cybersecurity expertise directly by headhunting expert-personnel directly from the security sector. Many interviewees noted to us that cybersecurity skills were in short supply and that insurers needed to create a bridge to link to cybersecurity professionals

through direct engagement and in-hiring (Interviews A2, A4, A13). This applied, in particular, to professionals with an ability to translate technical issues into business contexts (ISACA, 2019). Here a common understanding of risk assessment was an early 'hinge' in linking insurance and cybersecurity professionals, albeit a weak one. One broker highlighted that in-sourcing typically resulted in a small number of IT experts solely used for risk assessments without being further integrated into insurance operations (Interview A4). Within this setup, the insurance and cybersecurity professional groups worked on tasks independently, with the security-relevant information of applicants being passed on from the underwriter to IT experts, who either approved the information or rejected it. To the extent that insurers succeeded in attracting experienced cybersecurity practitioners, one insurance consultant pointed out that retainment is a major problem for insurance companies given heightened career mobility among cybersecurity professionals (Interview A2). Given this situation, professionals did not have to calibrate their interest and expertise around the underwriting technology. As one interviewee with extensive experience in the industry formulated:

> There is a poor understanding of how cyber insurance is different from other insurance products. The technical and process part needs to be integrated in cyber insurance. But these people do not exist. The main problem now is that the different teams – security, insurance, global risk - work for themselves. They do not work together. We cannot separate cybersecurity from insurance like that.
>
> Interview A12, CISO, Government Executive Office

Second, some insurers turned to internal strategies, supporting employees to develop cybersecurity skillsets through dedicated training programs. For example, the American insurance titan Chubb cooperated with Carnegie Mellon University to certify insurance practitioners in industry best practices to "give participants an opportunity to deepen their understanding of cyber risk and to be hand-on with cyber security" (Chubb, 2018). Similar efforts occurred in Europe, such as the Insurance Institute of Switzerland's advanced training on Cyber Risk (IIS, 2020) or the German insurance academy's course on cyber insurance (DVA, 2021). While the intensity of these trainings varies from three days to several weeks, the avatar

strategy has been used to produce baseline knowledge among in-house staff that subsequently can act as intermediaries between customers and third-party IT experts (Herr, 2021, p. 103; Talesh, 2018).

Bridging the gap between cyber and insurance has also been pursued through external strategies in the form of third-party contracting. It its simplest form, this is manifest in collaborative agreements with cyber security vendors for risk assessments of large clients and in the form of incident response (Franke, 2017; p, 137; Maccoll, Nurse, & Sullivan, 2021, p. 7). For example, cybersecurity giant FireEye has partnered with brokers and underwriters from Marsh, Allianz, AXA, and Beazley (FireEye, 2021). However, relying on third-party specialized expertise in making underwriting decisions has its own ramifications. For example, one interviewee from a risk-modelling firm complained that cybersecurity professionals are "so obsessed with detail" that their integration sometimes hinders rather than improves underwriting practices (Interview A13).

Developing direct points of contact between the insurance and cybersecurity professionals has been a sustained challenge for the development of standardized underwriting processes. Hinge strategies through the integration of cybersecurity professionals into insurance have been constrained by a general lack of available talent. Related strategies in the form of third-party contracting limit the extent of knowledge transfer between professional groups, while the development of avatars through cybersecurity training for insurance professionals does not compensate for the sustained creation of points of contact. The result is a proliferation of product offerings and risk assessment processes in need of harmonization (ENISA, 2017, p. 44). This creates professional difficulties:

> High levels of fragmentation in cyber insurance product deliveries result in part from the absence of clean and agreed upon quantification tools. In this fog, people see very different risks.
>
> Interview A18, Underwriter, Reinsurance Company

With increased cyberattacks directed at small and medium enterprises (SMEs), the need for greater coordination on underwriting technologies became apparent and insurers turned to

strategic technologies to cope with deteriorating loss ratios and uncertainty about pricing (Talesh & Cunningham, 2021):

> Insurance carriers in the US have been writing some form of cyber insurance for SMEs for decades. Now, for the first time they are forced to *underwrite* cyber insurance.
>
> Interview A8, Head of Insurance, Insurtech

Calibrating Strategic Technologies

The need for more accurate underwriting of cyber risk insurance, especially in light of deteriorating loss ratios, brings us to the second phase. Here the concern is with how quantitative approaches to underwriting became strategic technologies, resulting in greater product alignment. This is an evolving process with a great deal of calibration between the cybersecurity and insurance professionals. Technological tools are of particular importance as the cyber insurance market matures and achieves a scale that permits SMEs as regular clients. Big Data, automated security scans, and quantitative modelling are employed to assess the risks of customers and assign premium categories (Talesh & Cunningham, 2021). The calibration of such strategic technologies builds upon successful 'points of contact' described in the first phase.

Mature insurance lines routinely employ quantitative risk modelling. Due to underdeveloped historical incident data and the dynamic cyber risk landscape, these standard approaches cannot easily be transferred. The second phase in stabilizing the market is therefore primarily concerned with the design and calibration of alternative quantification methodologies. The central contention in this context is how the quantification process is shaped, what is included and what is sidelined (Jones, 2019). This raises concerns among the professionals about how their preferred forms of diagnosis, inference, and treatment are built into proto-inscriptions being created from quantification efforts.

While a number of vendors offer quantified statements about the quality of security practices of organizations, others provide cyber risk quantifications (CRQs) in terms of probabilities and magnitudes of potential cyber-related loss events. In both cases, the result is a numerical

abstraction of complex underlying processes. Our findings suggest that this calibration of quantitative risk assessments is a contested process and played out along a spectrum of measurement approaches, ranging from fully automated ones to those that derive quantifications from human input factors in the form of expert elicitation. A stylized illustration of this can be found in figure 2.

Figure 2: Spectrum of cyber risk quantifications

Of course, few would reject the potential value of technology and Big Data altogether. The closest observation to this ideal type is a class of integrated models that emphasize the importance of subject-matter expertise to understand the nuances that influence the risk profile of organizations (Jones, 2019, p. 21). The distinguishing factor of the integrated approach is therefore that the quantification process cannot be fully disconnected from the human element:

> Technologies and tools can of course be helpful, but they cannot substitute for the underwriter in the process. The underwriter should always be involved and understand the risk. Certifications are needed.
>
> Interview A2, CEO of specialized cyber insurance provider

The implication is that integrated models demand strong inter-professional cooperation to develop robust quantification models. In this way, the quantification process itself morphs into the arena to build strong inter-professional linkages. One interviewee highlighted this feature emphatically:

> The Cyber Risk Quantification process should be the activity that links client, brokers, consultants and carriers in order to underpin cyber insurance. This is the key thing and the glue that should put together the stakeholders.
>
> Interview A9, Head of Cyber Risk at Insurance Broker

In this context the quantification of cyber risk is an explicit hinge strategy to connect the cybersecurity and insurance professionals, a strategy upon which inscription-building can take place. That is, within an integrated model the quantification is contingent on the buildup of hybrid expert knowledge, which consequently takes a strategic priority (Wrede, Stegen, & von der Schulenburg, 2020, p. 677). Bringing stakeholders together through quantification processes faces, however, a multi-professional coordination problem. As the research director of Chartis, Sidhartha Dash, highlights: "getting risk, security, and technology teams all working together […] is more tricky than you'd expect" (quoted in Blaesing & Stauffenecker, 2020, p. 7). Insurers are instead pushing for more standardized models, linking events, coverage and claims (Interview A13). In such a standardized approach, cyber risks are priced through a combination of probabilistic modelling that allocate premium categories to policyholders based on industry type, size, and jurisdiction, while adjusting the pricing with security rating scores.

The consequence is that some insurers have been moving towards automated underwriting processes, in which "technology, predictive analytics, and security surveillance supplant the traditional insurance application and interview process" (Talesh & Cunningham, 2021, p. 8). The ensuing underwriting process is one in which human cybersecurity expertise increasingly is replaced with algorithms and big data, operated from afar and satisfying insurers' need for simplicity and generalizability. In this ideal case, located on the left-hand side of figure two, cyber risk quantification providers offer fully automated and purely data-driven methodologies, removing the need for expert elicitation for the user. This would move cyber risk insurance into the third phase where there is explicit inscription-building towards a purified technology. One example is the firm Black Kite which promises "detailed, accurate data on any company's security vulnerabilities in 60 seconds or less", delivering "a faster, more affordable way for cyber insurance providers […] to obtain a real-time, on-demand assessment of cybersecurity risks" (Black Kite, 2019), reducing the time needed to produce a risk assessment from days to one minute and reducing complexity to a single credit-rating-like score.

Underlying fully automated models are security rating methodologies that create a broad array of data points by scanning publicly facing internet connections and IP addresses to produce quantified statements about an organization's cybersecurity posture, very much similar to consumer credit rating agencies (Fourcade and Healy 2013; US Chamber of Commerce, 2017). Initially, this technology was marketed to financial institutions and third-party risk management (Interview A16) but expanded into the insurance sector with Liberty Mutual exploring the use cases of security ratings for underwriting as early as 2014 (Liberty Mutual, 2014). Today, the application of security scans is becoming standard practice and acts as a proxy to determine security postures of organizations (Talesh, 2018, p. 14). As an interviewee commented to us, proto-inscriptions through scans are encouraging product alignment at a fast pace:

> It is probably correct that hands-on approaches to risk assessments are going to decrease as more standards and modules are developed. Already today it seems that the insurance product itself is in need of only a few adjustments. In the future, standards and modules from the producer's side will therefore also improve the ability to build data and use standardized security on the basis of, for example, scans.
>
> Interview A11, Senior Director at IT Security Consultancy

Despite the widespread adaptation of security scans for risk assessments, they are associated with a number of limitations and represent a specific form of quantified underwriting that focuses on the external security posture of clients (Jones, 2019, pp. 9-12). On the one hand, this allows underwriters to make better informed judgements about the security posture of potential clients without having to invest in developing cybersecurity expertise. On the other hand, the scoring mechanism does not account for internal security practices of clients and thereby provides for a limited representation of the nuances that underlie risk work. This has direct implications for the question of professional control over the linked ecology of cyber risk insurance because technical cyber expertise is effectively kept at a distance from the practice of cyber insurance underwriting and confined to the role of post-incident service (see also Maccoll et al., 2021). How CRQs are designed has far-reaching implications for the understanding of what digital risks are, and how they should be addressed. Within this process, product offerings

are aligning and risk quantification modules are calibrated, gradually decreasing the need to direct involvement of specialized expertise in the risk assessment process. As this process develops further there is greater potential for inscriptions to become purified technologies that may introduce 'blackboxing' concerns. It is recognized that full automation comes at a heavy cost as expertise is lost in the process:

> At the end of the day, it is about the reliability of the results. To achieve this, experts are needed in the process who have a profound comprehension of what they are working with. It is vital that our underwriters and claims managers understand in detail how the results are produced... The competence of the staff alone is what defines the difference (in underwriting) between meaningful risk assessment and gambling, primarily for large risks.
>
> Interview A19, Senior Underwriter. Reinsurance Company

Discussion and Conclusion

We contend that technological rationalization within a market is generally built on professional coordination. Following this logic, inscription-building in unstable markets requires professionals to link to each other, develop hinges of mutual interest, and to calibrate their ambitions in determining who has jurisdictional control over what tasks. This calibration includes how profession-focused forms of diagnosis, inference and treatment are applied to the issue at hand, and how these forms produce conflicts or complementarities with other professional groups in a linked ecology. Inscription-building, in this phase, requires the development of a strategic technology that can be harnessed through a hinge. If this process is successful, then inscription-building can move into a further step. Here, inscriptions turn into a purified technology that objectify risk definitions and enable calculative devices to act at distance (Power, 2004). In a market context this also permits upscaling through the development of clear quality profiles and price signals (White, 1981), encouraging actors who are uncertain about their own capacity to judge quality and to join the market (Podolny, 2001).

Inscription-building is a process that can be properly initiated when built on professional coordination (Qu & Cooper, 2011). Here we have documented the phases through which linked ecologies enable inscription-building. Particularly important in the case of cyber risk insurance is professional calibration over forms of calculative infrastructures that can be considered a proto-inscription. That quantification is invoked as a device for technological rationalization is of no surprise given how common quantification is to knowledge representation (most recently Mennicken & Espeland, 2019). More surprising is how poorly coordinated the market for cyber risk insurance has been in the past two decades. Spurred by a surge in external demand and explicit attempts to make 'points of contacts' from cybersecurity and insurance professionals, attempts at market stabilization through hinge strategies and inscription-building began in earnest within the past five years. Organizations including governments, universities, and global professional service firms have also linked to professionals to encourage market stabilization based on their own perceived risks. Our case is therefore 'live', allowing us to trace how linked ecologies are tied to inscription-building.

Figure 3 provides a summary of our analysis, building on the theoretical specification of phases in Figure 1. We can see that in the first phase there was a proliferation of cyber risk insurance products, leading to market instability and confusion over how to underwrite cyber risks. Cybersecurity and insurance professionals established hinges through interpersonal contacts, namely through in-sourcing of expertise, developing training programs, and through third-party contracting. Characteristic of this phase was that demand far exceeded the supply of cybersecurity professionals, who in turn exhibited high career mobility. They scoffed at insurance professionals as unknowledgeable and unfashionable, suggesting that positions in the professional status hierarchy favored those with a technological edge - the 'coding elite' (Burrell and Fourcade, 2021). On the other hand, specialized cybersecurity expertise was described as "too focused on detail", indicating a valuation of business development skills over detailed technical expertise (Spence et al. 2017, pp. 85, 91). Consequently, insurance professionals struggled to properly integrate cyber risk expertise into insurance product development. But both professional groups watched market demand grow, making these initial points of contacts useful for the treatment of underwriting as a strategic technology. Measuring cyber risks remained largely confined to cybersecurity and insurance professionals, with early engagement from public institutions starting to explore and encourage attempts to quantify risk (UK Cabinet Office, 2015).

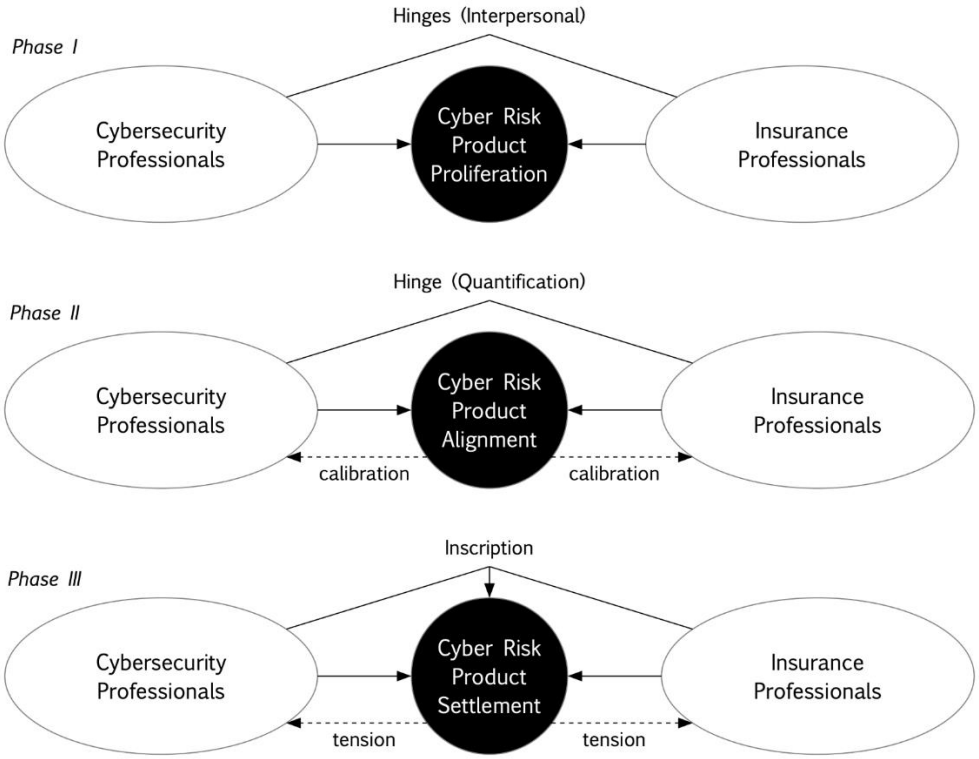


Figure 3: The development of cyber-risk insurance products

This led to the second phase. In this phase the explicit hinge created between cybersecurity and insurance professionals centers on forms of quantification. Owing to the development of multiple yet similar quantified risk assessment methodologies, this phase encourages gradual cyber risk insurance product alignment. Although insurance companies have spearheaded efforts to quantify cyber risks, the second stage equally sees new actors emerging. Global professional service firms (GPSFs), such as Deloitte (2020), PwC (Blaesing & Stauffenecker, 2020) and Boston Consulting Group (BCG, 2019), began to produce their own methodologies, and public institutions actively encouraged alignments of risk assessment methodologies with the participation of experts from insurance, cybersecurity, and academia (ENISA, 2016; OECD, 2017). Similar cooperative initiatives were launched through the Global Cyber Risk Quantification Network (GCRQN), bringing together representatives from government, academia, and industry (GCRQN, 2018).

To meet demand market stability is required, which needs better risk metrics. These forms of quantification are being fostered as predictive analytics, automated surveillance scans, and the development of certification systems to align professional conduct. These forms of

quantification are proto-inscriptions. The cybersecurity and insurance professionals have an interest in developing cyber risk underwriting in a manner that favors their forms of diagnosis, inference, and treatment. But they must also calibrate their preferences in relation to the other professional groups to allow market stabilization. We have identified this calibration exercise to be centered around the various degrees of automation that CRQs exhibit, either reinforcing or minimizing the need for specialized cybersecurity expertise on the customer side. This phase in the process of professional coordination and technological rationalization is akin to what Power has described as how accounting begins, with "a combination of disappointment and the promise of improvement in terms of a conceptual or abstract 'performance object' as the solution" (Power, 2015, p. 48).

Professional coordination is emerging within this second phase, especially around the notion of risk quantification as a metric, the use of automated scans, and increasingly a financial logic that provides an automated shortcut for underwriters and potential clients. In particular, the incorporation of value-at-risk models has gained popularity among insurance and cybersecurity professionals alike. One especially prominent example here is the propagation of Return on Investment (ROI) models that maintain a tight focus on the "financial prioritization of CVEs" (common vulnerabilities and exposures).[3] From this logic a ROI can be computed from the "mitigation spend" involved in protecting different elements of the company. The potential harm to a company's data warehouse can be differentiated from its payment processing systems or treasury. With metrics on financial risk reduction, implementation costs, and the probability of a cyberattack, the ROI can be automated for the client.

The use of short-termist financial logics to legitimate the growth of a market has been identified as a common pathway to market upscaling (Botzem & Dobusch, 2017; Grisard, Annisette, & Graham, 2020). In the case of cyber risk insurance, the rise of a financial logic in quantification has been led by the insurance professionals. Simultaneously, however, new competitors have identified the opportunity to shape the development of proto-inscriptions, such as GPSFs, who now are in direct competition with insurance professionals to develop risk quantification metrics. It is no surprise that managers in the Big Four global accounting firms have been attracted to new market opportunities to manage fat tail risks (Kornberger, Justesen, & Mouritsen 2011, p. 516). Given the capacity of the Big Four to upscale market activity, the entry of GPSFs into the linked ecology is significant (cf. Mennicken, 2010, p. 355).

With greater movement towards product alignment, we can expect a move towards fully articulated inscription-building, as predicted in the third phase. The inscription of a purified technology would then aide cyber risk product settlement and permit translations enacted at a distance. The maintenance of hinge strategies through interpersonal points of contacts is no longer the most prominent means of multi-professional coordination, nor is calibration between professional groups over what should be quantified, and how, through hinges of proto-inscription. Relations between actors can become translations at a distance by actants, represented by a purified and singular calculative device (Latour 1987; Robson & Bottausci, 2018).

For the cyber risk insurance market this would permit easier entry for SME clients, a persistent concern raised by our interviewees. We would also expect that stable calculative devices blending cybersecurity and insurance would lead to other innovations in the market, as demonstrated in other cases (Revellino & Mouritsen, 2015). This may include extensions of input variables to be used in the inscribed technology. Insurance companies' harvesting of Facebook posts to determine car insurance premia is one example of such extensions (Kornberger, Pflueger, & Mouritsen, 2017, p. 89, fn. 9). Such problems with automated assignment of insurance premiums have led to conflicts among professional groups as moral and expert claims are disentangled (Kiviat, 2019).

In this context, an important element of the third phase is that we would expect to see ongoing tensions, given that inscriptions do not eradicate conflicts among professional groups (Power, 2003). In the current environment the insurance professional group is dominant in determining what can be quantified in underwriting cyber risk insurance products, while leaning on cybersecurity professionals to provide subject matter and technical expertise. Following this logic, cyber risk insurers are producing lists of trusted cybersecurity vendors, enfolding them into the linked ecology and fostering a status hierarchy (cf. Mennicken, 2010, p. 353; Marsh, 2019).

The professional status hierarchy may be stabilized by market upscaling, but cyber risks are also volatile, which can then empower cybersecurity professionals with access to knowledge that is not accessible to the inscribed technology. Not unlike the production of the balanced scorecard as a management accounting technique, processes of inscription-building for cyber risk insurance close down the ambiguous nature of measurement variables, providing them with an

objective quality (Qu & Cooper, 2011, p. 360) and defining causal links between actions and outcomes (Cooper, Ezzamel, & Qu, 2017, p. 1010). Similarly, cyber risk quantifications define what is good and bad security practices. As this performance metric is passed on, risk quantifications engage security and technology officers in client organization, helping them to order investments and measure performance (c.f. Busco & Quattrone, 2015, p. 1244). It has already been documented how insurance companies act as compliance managers for customers, defining the nature of compliance and rational risk governance processes (Talesh, 2018, p. 431).

In doing so, definitions of cyber risk are inscribed into quantified frameworks creating a form of accounting system, the absence of which Alex Stamos so emphatically lamented in the opening quote of this article. Putting numbers on risks and defining corresponding ROIs, cyber risk inscriptions promise to objectify the performance of chief information security officers and elevate their status to a more strategic leadership role within organizations (c.f. Deloitte, 2017, p. 19). This process closes down underlying questions of how the quantification process is shaped and what input variables are used (Jones, 2019). Acting on the resulting quantified output to decide on underwriting decisions and steer cybersecurity investments within organizations, the inscription begins to take on performative qualities, defining what should be counted as risky and what security practices count. In this way, definitions of risk "get built into technology" (Hilgartner, 1992) with a corresponding danger that performativity effects of purified technologies represent risks incompletely and contribute to the development of 'black swan' events (MacKenzie, 2006).

In conclusion, we suggest that professional coordination is important for technological rationalization. There is a threshold for consensus among professional groups within a linked ecology prior to the rise of 'inscriptors' who can then implement calculative devices that allow actants to translate at a distance and enfold new actors (Qu & Cooper, 2011; Power, 2015). This is important for understanding change in new markets, like cyber risk insurance, given that market instability comes at great economic and social costs. Theoretically, we have proposed phases whereby points of contact are developed among professionals while products are proliferating around an emergent technology. Successful points of contact can then foster hinges and a common project to create proto-inscriptions that align products in the markets. As this phase involves the development of a strategic technology, a great deal of professional calibration over input factors is required – a process with stark implications for the stabilization of professional hierarchies. Consequently, this final process also creates tensions. However, if

all of this works, then professional and product settlement allows for inscription and the creation of a purified technology.

In this context, the inscription-building and linked ecologies approaches can be integrated to mutual benefit. Work on inscriptions helps us identify how control over points of interest can be managed through calculative devices and technologies that operate at a distance, blinkering professionals into particular ways of diagnosis, inference, and treatment. The linked ecologies approach points to how actors from previously disconnected social spaces begin to overlap and interpenetrate. Here, relations are fostered through mutual projects that transform how a location, a point of interest, is controlled by professionals and the organizations concerned (Mennicken, 2010, p. 335). Hence, the linked ecologies approach helps us to locate the boundaries around 'strategic agency' in inscription-building (Cooper, Ezzamel, & Qu, 2017, p. 993). Integrating these approaches allows us to see how interpersonal relations are important for the enabling of multi-professional coordination, and how hinges forged across professionals ferment the process of inscription-building. It also allows insights into how the process of inscription-building is affected by, and affects, professional status hierarchies, including aspects of task allocation and control, and who can organize to stabilize a market. In sum, this conceptual integration helps us to trace processes of professional coordination and technological rationalization in the emergence of cyber risk insurance.

Finally, mapping the relationship between inscription-building and linked ecologies within cyber risk insurance has clear political economy implications. The management of cyber risk is a key parameter for sustained societal trust in digital developments. As such, mitigations of digital insecurities are fundamental for the ability of organizations and societies to reap the benefits of digital transformation. How cyber risks are managed and to what extent societal actors are able to act on digital risks depends to a large degree on the process of risk assessment. These diagnostic processes rely, in turn, on the configuration of linked ecologies and multi-professional coordination that define the parameters of inscription-building. The developments documented in this article suggest that the quality of risk assessments, including corresponding risk management and mitigation strategies, is heavily skewed towards large and resource-heavy customers of cyber insurance products and services. However, in a climate of escalating cyberattacks against, especially, SMEs the private enforcement of cybersecurity practices by insurance providers threatens to reinforce digital divides and unequal access to effective risk mitigation strategies.

Endnotes

[1]: Former Facebook security chief Alex Stamos: Being a CSO can be a 'crappy job'. TechCrunch, September 6, 2018, available at https://tinyurl.com/2z5p2zzm

[2]: Presentation at "Blackhat 2019", available at https://www.blackhat.com/us-19/speakers/Matt-Prevost.html (Minute 04:11).

[3]: As presented in a ThreatConnect webinar on "Understanding Cyber Insurance & Quantifying Risk", 13 July 2021.

References

Abbott, A. (1988). *The System of Professions: An Essay on the Division of Expert Labor*. The University of Chicago Press.

Abbott, A. (2001). *Time Matters: On Theory and Method*. University of Chicago Press.

Abbott, A. (2005). Linked ecologies: States and universities as environments for professions. *Sociological Theory*, Vol. 23, pp. 245–274. https://doi.org/10.1111/j.0735-2751.2005.00253.x

Allianz (2020). Managing the Impact of Increasing Interconnectivity: Trends in Cyber Risk. *Allianz Global Corporate and Specialty*

BCG (2019). A Smarter Way to Quantify Cybersecurity Risk. https://www.bcg.com/capabilities/digital-technology-data/smarter-way-to-quantify-cybersecurity-risk

Beckert, J., Rössel, J., & Schenk, P. (2017). Wine as a cultural product: Symbolic capital and price formation in the wine field. Sociological Perspectives, 60(1), 206-222. https://doi.org/10.1177/0731121416629994

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158. https://doi.org/10.1057/gpp.2014.19

Black Kite (2019). Black Kite Launches Industry-First Rapid Cyber Risk Scorecard. https://blackkite.com/black-kite-launches-industry-first-rapid-cyber-risk-scorecard/

Blaesing, N., & Stauffenecker, J. (2020). The Necessity of Cyber Risk Quantification. *Harvard Business Review Analytical Services*.

Blok, A., Lindstrøm, M. D., Meilvang, M. L., & Pedersen, I. K. (2019). Ecologies of boundaries: Modes of boundary work in professional proto-jurisdictions. *Symbolic Interaction*, 42(4), 588-617. https://doi.org/10.1002/symb.428

Botzem, S., & Dobusch, L. (2017). Financialization as strategy: Accounting for inter-organizational value creation in the European real estate industry. *Accounting, Organizations and Society,* 59, 31-43. https://doi.org/10.1016/j.aos.2017.05.001

Burrell, J., & Fourcade, M. (2021). The society of algorithms. *Annual Review of Sociology,* 47, forthcoming. https://doi.org/10.1146/annurev-soc-090820-020800

Busco, C., & Quattrone, P. (2015). Exploring How the Balanced Scorecard Engages and Unfolds: Articulating the Visual Power of Accounting Inscriptions. *Contemporary Accounting Research, 32*(3), 1236–1262. https://doi.org/10.1111/1911-3846.12105

Busco, C., & Quattrone, P. (2018). Performing business and social innovation through accounting inscriptions: An introduction. *Accounting, Organizations and Society*, *67*(March), 15–19. https://doi.org/10.1016/j.aos.2018.03.002

Callon, M. (1980). Struggles and Negotiations to Define What is Problematic and What is Not: The Sociologic Translation. In W. A. Schwartz, K. D. Knorr, R. Krohn, & R. Whitley (Eds.), *The Social Process of Scientific Investigation* (pp. 197–220). https://doi.org/10.2307/2068551

Callon, M. (1986). The sociology of an actor-network: The case of the electric vehicle. In Mapping the dynamics of science and technology (pp. 19-34). Palgrave Macmillan, London.

Callon, M. (1998). Introduction: The Embeddedness of Economic Markets in Economics. *The Sociological Review*, *46*(1_suppl), 1–57. https://doi.org/10.1111/j.1467-954x.1998.tb03468.x

Carruthers, B. G., & Espeland, W. N. (1991). Accounting for rationality: Double-entry bookkeeping and the rhetoric of economic rationality. *American Journal of Sociology,* 97(1), 31-69. https://doi.org/10.1086/229739

Carter, C., & Spence, C. (2014). Being a successful professional: An exploration of who makes partner in the Big 4. *Contemporary Accounting Research,* 31(4), 949-981. https://doi.org/10.1111/1911-3846.12059

Chiglinsky, K & Basak, S. (2018). Buffett Cautious on Cyber Insurance Because No One Knows Risks. *Bloomberg.* https://www.bloomberg.com/news/articles/2018-05-05/buffett-cautious-on-cyber-insurance-because-no-one-knows-risks

Christensen, M., & Skærbæk, P. (2010). Consultancy outputs and the purification of accounting technologies. *Accounting, Organizations and Society*, *35*(5), 524–545. https://doi.org/10.1016/j.aos.2009.12.001

Chubb (2018). Chubb Collaborates with Carnegie Mellon University's Heinz College of Information Systems and Public Policy. https://news.chubb.com/2018-07-10-Chubb-Collaborates-with-Carnegie-Mellon-Universitys-Heinz-College-of-Information-Systems-and-Public-Policy

Cordonnier, A. (2020). Cyber reinsurance in the "new normal". https://www.swissre.com/reinsurance/property-and-casualty/reinsurance/casualty-reinsurance-underwriting/cyber-reinsurance-in-the-new-normal.html

Cooper, D. J., Ezzamel, M., & Qu, S. Q. (2017). Popularizing a Management Accounting Idea: The Case of the Balanced Scorecard. *Contemporary Accounting Research*, *34*(2), 991–1025. https://doi.org/10.1111/1911-3846.12299

Dambra, S., Bilge, L., & Balzarotti, D. (2020). SoK: Cyber insurance–technical challenges and a system security roadmap. In *2020 IEEE Symposium on Security and Privacy (SP)*. 1367-1383. doi: 10.1109/SP40000.2020.00019.

Deloitte (2017). New perspectives on how cyber risk can power performance. *Deloitte University Press.https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-cyberrisk.pdf*

Deloitte (2020). Beneath the surface of a cyberattack: Collision avoidance. https://www2.deloitte.com/us/en/pages/risk/articles/quantifying-cyber-risk-to-chart-a-more-secure-future.html

DVA (2021). Cyberrisiken bewerten und versichern. *Deutsche Versicherungsakademie.* https://www.versicherungsakademie.de/cyberrisiken-bewerten-und-versichern-v341/

EIOPA (2018). Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies. https://doi.org/10.2854/33407

ENISA (2012). Incentives and barriers of the cyber insurance market in Europe. https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe

ENISA (2016). Cyber Insurance: Recent Advances, Good Practices and Challenges. https://doi.org/10.2824/065381

ENISA (2017): Commonality of risk assessment language in cyber insurance - Recommendations on Cyber Insurance. https ://doi.org/10.2824/691163

Eyal, G. (2012). Spaces Between Fields. In P. S. Gorski (Ed.), *Bourdieu and Historical Analysis* (pp. 158–182). Duke University Press.

Faulconbridge, J. R., & Muzio, D. (2012). Professions in a globalizing world: Towards a transnational sociology of the professions. *International Sociology*, 27(1), 136-152. https://doi.org/10.1177/0268580911423059

FireEye (2021). Cyber Risk Insurance Partners. https://www.fireeye.com/partners/strategic-technology-partners/cyber-risk-insurance/cyber-risk-insurance-partners.html

Flyvbjerg, B. (2011). Case Study in Norman K. Denzin and Yvonna S. Lincoln, eds., *The Sage Handbook of Qualitative Research*, 4th Edition, Chapter 17, pp. 301-316. SAGE.

Fourcade, M., & Healy, K. (2013). Classification situations: Life-chances in the neoliberal era. *Accounting, Organizations and Society*, 38(8), 559-572. http://dx.doi.org/10.1016/j.aos.2013.11.002

Fourcade, M., & Khurana, R. (2013). From social control to financial economics: the linked ecologies of economics and business in twentieth century America. *Theory and Society*, *42*(2), 121–159. https://doi.org/10.1007/sl

Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security*, 68, 130-144. https://doi.org/10.1016/j.cose.2017.04.010

GCRQN (2018). Quantifying Systemic Cyber Risk Report on the "Connectedness in Cyber Risk" Workshop. http://web.stanford.edu/~csimoiu/doc/Global_CRQ_Network_Report.pdf

Gerhards, E. V. (2018). Cybersecurity insurance: popular but poorly understood. *InsurTech Center*. https://www.propertycasualty360.com/2018/07/10/cybersecurity-insurance-popular-but-poorly-understood/

Grisard, C., Annisette, M., & Graham, C. (2020). Performative agency and incremental change in a CSR context. *Accounting, Organizations and Society*, *82*, 101092. https://doi.org/10.1016/j.aos.2019.101092

Grzadkowska, A (2019). With evolution in cybercrime, brokers' roles are more complex and critical. https://www.insurancebusinessmag.com/us/news/cyber/with-evolution-in-cybercrime-brokers-roles-are-more-complex-and-critical-163659.aspx

Hall, M., & Fernando, R. (2016). Beyond the Headlines: Day-to-day Practices of Risk Measurement and Management in a Non- Governmental Organization. In *Riskwork: Essays on the Organizational Life of Risk Management* (pp. 72–90). https://doi.org/10.1093/acprof

Harrington, B., & Seabrooke, L. (2020). Transnational Professionals. *Annual Review of Sociology*, 46, 399-417. https://doi.org/10.1146/annurev-soc-112019-053842

Hathaway, M. (2018). Managing National Cyber Risk. Organization of American States. White Paper Series, (2).

Herr, T. (2021). Cyber insurance and private governance: The enforcement power of markets. *Regulation & Governance,* 15(1), 98-114. https://doi.org/10.1111/rego.12266

Hilgartner, S. (1992). The Social Construction of Risk Objects: Or, How to Pry Open Networks of Risk. In J. F. Short & L. Clarke (Eds.), *Organizations, uncertainties, and risk* (pp. 39–53). Boulder: Westview Press.

IIS (2020). Answers to Cyber Risk. *Insurance Institute of Switzerland*. https://www.insurance-institute.ch/de/weiterbildung/risk-management/managing-cyber-risk-standardkurs

Insikt Group (2021). The Business of Fraud - An Overview of How Cybercrime Gets Monetized. https://www.recordedfuture.com/how-cybercrime-gets-monetized/

ISACA. (2019). State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2019-part-1_res_eng_0319.pdf?regnum=500542

Jones, J. (2019). Understanding Cyber Risk Quantification A Buyer's Guide. *FAIR Institute*.

Jordan, S., Mitterhofer, H., & Jørgensen, L. (2018). The interdiscursive appeal of risk matrices: Collective symbols, flexibility normalism and the interplay of 'risk' and 'uncertainty.' *Accounting, Organizations and Society*, *67*, 34–55. https://doi.org/10.1016/j.aos.2016.04.003

Justesen, L. N., & Mouritsen, J. (2011). Effects of Actor-Network Theory in Accounting Research. *Accounting, Auditing and Accountability Journal,* 24(2), 161-193. https://doi.org/10.1108/09513571111100672

Khalili, M. M., Liu, M., & Romanosky, S. (2019). Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Journal of Cybersecurity*, 5(1), 1-16. https://doi.org/10.1093/cybsec/tyz010

Kiviat, B. (2019). The moral limits of predictive practices: The case of credit-based insurance scores. *American Sociological Review*, 84(6), 1134-1158. https://doi.org/10.1177/0003122419884917

Kozinets, R. V. (2015). *Netnography: redefined*. Sage.

Kurunmäki, L., Lapsley, I., & Miller, P. (2011). Accounting within and beyond the state. *Management Accounting Research*, *22*(1), 1–5. https://doi.org/10.1016/j.mar.2010.11.003

Kornberger, M., Justesen, L., & Mouritsen, J. (2011). "When you make manager, we put a big mountain in front of you": An ethnography of managers in a Big 4 accounting firm.

Accounting, Organizations and Society, 36(8), 514-533. https://doi.org/10.1016/j.aos.2011.07.007

Kornberger, M., Pflueger, D., & Mouritsen, J. (2017). Evaluative infrastructures: Accounting for platform organization. *Accounting, Organizations and Society*, 60, 79-95. https://doi.org/10.1016/j.aos.2017.05.002

Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. Telecommunications Policy, 44(8), 1-14. https://doi.org/10.1016/j.telpol.2020.102007

Latour, B. (1986). Visualisation and Cognition: Thinking with Eyes and Hands. *Knowledge and Society: Studies in the Sociology of Culture Past and Present*, Vol. 6, pp. 1–40.

Latour, B. (1987). *Science in Action* (11th ed.). Cambridge, MA: Harvard University Press.

Latour, B. (1999). *Pandora's hope.* Cambridge, MA: Harvard University Press.

Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. Journal of Cyber Policy, 1-19. https://doi.org/10.1080/23738871.2021.1880609

Liberty Mutual (2014). Liberty International Underwriters to Provide Network Activity Monitoring through BitSight Technologies for all LIU Data Insure Policyholders https://www.libertymutualgroup.com/about-lm/news/articles/liberty-international-underwriters-provide-network-activity-monitoring-through-bitsight-technologies-all-liu-data-insure-policyholders

Maccoll, J., Nurse, J. R. C., & Sullivan, J. (2021). Cyber Insurance and the Cyber Security Challenge. London: Royal United Services Institute for Defence and Security Studies.

MacKenzie, D. A. (2006) *An Engine, Not a Camera: How Financial Models Shape Markets.* Cambridge, MA: MIT Press.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. Computer Science Review, 24, 35-61. https://doi.org/10.1016/j.cosrev.2017.01.001

Marsh (2019). Marsh Reveals Inaugural Class of Cyber Catalyst Designated Solutions. https://www.marsh.com/us/media/inaugural-class-cyber-catalyst-designated-solutions.html

Mennicken, A. (2010). From inspection to auditing: Audit and markets as linked ecologies. *Accounting, Organizations and Society*, *35*(3), 334–359. https://doi.org/10.1016/j.aos.2009.07.007

Mennicken, A., & Espeland, W. N. (2019). What's new with numbers? Sociological approaches to the study of quantification. *Annual Review of Sociology,* 45, 223-245. https://doi.org/10.1146/annurev-soc-073117-041343

Miller, P. (1991). Accounting innovation beyond the enterprise: Problematizing investment decisions and programming economic growth in the UK in the 1960s. *Accounting, Organizations and Society*, 16(8), 733–762. https://doi.org/10.1016/0361-3682(91)90022-7

Miller, P., & Napier, C. (1993). Genealogies of calculation. *Accounting, Organizations and Society*, 18(7-8), 631-647. https://doi.org/10.1016/0361-3682(93)90047-A

Morgan, M. S., & Morrison, M. (1999). Models as mediators (p. 347). Cambridge: Cambridge University Press.

OECD (2017). Enhancing the Role of Insurance in Cyber Risk Management, *OECD Publishing*, Paris, https://doi.org/10.1787/9789264282148-en

OECD (2018). Unleashing the Potential of the Cyber Insurance Market: Conference Outcomes. http://www.oecd.org/daf/fin/insurance/Unleashing-Potential-Cyber-Insurance-Market-Summary.pdf

OECD (2020), Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation, www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

Podolny, J. M. (2001). Networks as the pipes and prisms of the market. *American Journal of Sociology*, 107(1), 33-60. https://www.jstor.org/stable/2781237

Pollock, N., & D'Adderio, L. (2012). Give me a two-by-two matrix and I will create the market: Rankings, graphic visualisations and sociomateriality. *Accounting, Organizations and Society*, *37*(8), 565–586. https://doi.org/10.1016/j.aos.2012.06.004

Ponemon Institute (2017). Cost of Cybercrime Study: Insights on the security investments that make a difference.

Ponemon Institute (2019). The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study

Power, M. K. (2003). Auditing and the production of legitimacy. *Accounting, Organizations and Society*, 28(4), 379-394. https://doi.org/10.1016/S0361-3682(01)00047-2

Power, M. (2004). Counting, control and calculation: Reflections on measuring and management. *Human Relations*, *57*(6), 765–783. https://doi.org/10.1177/0018726704044955

Power, M. (2015). How accounting begins: Object formation and the accretion of infrastructure. *Accounting, Organizations and Society,* 47, 43-55. https://doi.org/10.1016/j.aos.2015.10.005

Qu, S. Q., & Cooper, D. J. (2011). The role of inscriptions in producing a balanced scorecard. *Accounting, Organizations and Society*, *36*(6), 344–362. https://doi.org/10.1016/j.aos.2011.06.002

Quattrone, P. (2009). Books to be practiced: Memory, the power of the visual, and the success of accounting. *Accounting, Organizations and Society*, *34*(1), 85–118. https://doi.org/10.1016/j.aos.2008.03.001

Revellino, S., & Mouritsen, J. (2015). Accounting as an engine: The performativity of calculative practices and the dynamics of innovation. *Management Accounting Research,* 28, 31-49.

Robson, K. (1992). Accounting numbers as "inscription": Action at a distance and the development of accounting. *Accounting, Organizations and Society*, *17*(7), 685–708. https://doi.org/10.1016/0361-3682(92)90019-O

Robson, K., & Bottausci, C. (2018). The sociology of translation and accounting inscriptions: Reflections on Latour and Accounting Research. *Critical Perspectives on Accounting, 54*(June 2017), 60–75. https://doi.org/10.1016/j.cpa.2017.11.003

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk?. *Journal of Cybersecurity,* 5(1),1-19. https://doi.org/10.1093/cybsec/tyz002

Seabrooke, L., & Tsingou, E. (2016). Bodies of knowledge in reproduction: Epistemic boundaries in the political economy of fertility. *New Political Economy,* 21(1), 69-89. https://doi.org/10.1080/13563467.2015.1041482

Seabrooke, L., & Tsingou, E. (2021). Revolving doors in international financial governance. *Global Networks*, 21(2), 294–319. https://doi.org/10.1111/glob.12286

Spence, C., Zhu, J., Endo, T., & Matsubara, S. (2017). Money, honour and duty: Global professional service firms in comparative perspective. *Accounting, Organizations and Society,* 62, 82-97. https://doi.org/10.1016/j.aos.2017.09.001

Taffler, R. J., Spence, C., & Eshraghi, A. (2017). Emotional economic man: Calculation and anxiety in fund management. *Accounting, Organizations and Society*, 61, 53-67. https://doi.org/10.1016/j.aos.2017.07.003

Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. Law and Social Inquiry, 43(2), 417–440. https://doi.org/10.1111/lsi.12303

Talesh, S. A., & Cunningham, B. (2021). The Technologization of Insurance : An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy.

Taylor, H. (2020). 20 Ransomware Statistics You're Powerless to Resist Reading. https://journalofcyberpolicy.com/2020/03/01/20-ransomware-statistics-youre-powerless-resist-reading-security-boulevard/

Themsen, T. N., & Skærbæk, P. (2018). The performativity of risk management frameworks and technologies: The translation of uncertainties into pure and impure risks. *Accounting, Organizations and Society*, 67, 20–33. https://doi.org/10.1016/j.aos.2018.01.001

Tøndel, I. A., Seehusen, F., Gjære, E. A., & Moe, M. E. G. (2016). Differentiating cyber risk of insurance customers: The insurance company perspective. In *International Conference on Availability, Reliability, and Security* (pp. 175-190). Springer, Cham.

UK Cabinet Office (2015). UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk. https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance

US Chamber of Commerce (2017). Principles for Fair and Accurate Security Ratings https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

van der Heide, A. (2020). Making financial uncertainty count: Unit-linked insurance, investment and the individualisation of financial risk in British life insurance. *The British Journal of Sociology*, 71(5), 985-999. https://doi.org/10.1111/1468-4446.12783

Vollmer, H., Mennicken, A., & Preda, A. (2009). Tracking the numbers: Across accounting and finance, organizations and markets. *Accounting, Organizations and Society*, *34*(5), 619–637. https://doi.org/10.1016/j.aos.2008.06.007

Wall, M. (2018). Firms buy insurance 'in mad panic' as cyber-attacks soar. *BBC*. https://www.bbc.com/news/business-42687937

White, H. C. (1981). Where do markets come from? *American Journal of Sociology*, 87(3), 517-547. https://doi.org/10.1086/227495

Willis Towers Watson (2020). Cyber claims analysis report - Turning data into insight. https://www.willistowerswatson.com/en-GB/Insights/2020/07/cyber-claims-analysis-report

Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: A framework. *Journal of Cyber Policy*, 2(2), 209-226. https://doi.org/10.1080/23738871.2017.1360927

World Economic Forum (2015). Partnering for Cyber Resilience Towards the Quantification of Cyber Threats

Wrede, D., Stegen, T., & von der Schulenburg, J. M. G. (2020). Affirmative and silent cyber coverage in traditional insurance policies: qualitative content analysis of selected insurance products from the German insurance market. The Geneva Papers on Risk and Insurance-Issues and Practice, 45(4), 657-689.

ARTICLE 4: The Globalization of the Surveillance Industry

The Globalization of the Surveillance Industry

Co-authored article with Lars Gjesvik. Previously submitted to International Security and rejected after first round of reviews. Currently under revision for submission at International Studies Quarterly.

Abstract

The privatization of military and security functions is a key characteristic of international security architectures in the 21st century. Conventionally, scholars have voiced concern that unregulated private security markets can act as a destabilizing force in the international system. While these approaches emphasize the need to exercise public control over private enterprise, the recent growth of private intrusion and surveillance contractors (PISC) raises questions as to the viability of traditional control mechanisms. In this article we document how PISC markets have evolved since the beginning of the century and suggest that the structural characteristics of these markets place new barriers on the exercise of public control. We draw on evidence from extensive historical conference data including 5973 product demonstrations and training seminars, and in-depth interviews with industry insiders. Our findings indicate that the combined effect of transnationally operating and competitive markets, distributed agencies, largely intangible product types, and vested interests of public regulators spur proliferation dynamics that are difficult to control. By providing detailed historical evidence for the evolution of PISC markets the article adds an important empirical element to substantiate discussions about the market-based proliferation of offensive cyber capabilities. Theoretically, we contribute to current debates about the security implications of global markets through a structural account of control in which we identify PISC markets as a distinct phenomenon from PMSCs.

Keywords: Privatized Security; Offensive Cyber Capabilities; Control; Market Structures; Private Intrusion and Surveillance Contractors

Introduction

Today's "surveillance industry" is an arms industry in everything but name. On offer are "cyber warfare trainings" and other capabilities to conduct offensive operations in the digital domain. Historically, this market emerged out of a nexus of law enforcement and intelligence agencies and is feeding on the exploitation of vulnerabilities to facilitate the interception of digital data transmissions and intrusions into digital systems. Law enforcement agencies rely on the market for the acquisition of digital tools for the prevention, investigation, and mitigation of criminal activities. Intelligence agencies leverage digital surveillance for signals intelligence and espionage in the international arena. Not dissimilar from concerns about the internationalization of arms industries after the end of the cold war, fears are growing that the surveillance industry is beginning to undermine Western security interests (Bitzinger, 1994; Buchanan, 2020, pp. 316–317; Clapper, 2013; Smith, 2020).

The surveillance market therefore reflects the increasing relevance of markets for the shaping of international security architectures (Farrell & Newman, 2019; Lind & Press, 2018; Mousseau, 2019). Most prominently, this tendency has been addressed in the context of the globalization of the conventional arms industry and the use of private military and security contractors (PMSCs) (Avant, 2005b). Yet, while the literature on PMSCs is vast, little is known about its digital equivalent. How are these private intrusion and surveillance contractors (PISCs) organized? How has the market evolved? And not least, what are the implications for international security?

With the renewed growth of privatized force in the neoliberal era, a considerable body of literature has attempted to assess the consequences of such privatization tendencies (Abrahamsen & Williams, 2011; Avant, 2005a, 2005b; Avant & Sigelman, 2010; Bitzinger, 1994; Kinsey, 2007; Leander, 2005; Singer, 2008). The effects of private military and security markets, this scholarship suggests, depend on the extent to which states can exercise control over market actors (Avant, 2005b; Bitzinger, 1994; Leander, 2005).

While privatized and competitive defense markets are associated with improved efficiency and technological innovation, they also supplant a dominant logic of security and control with an imperative of organizational survival and profit maximization. At the heart of concerns about the negative externalities of privatized markets for arms and force is therefore the difficulty to align profit-oriented private enterprise with the special demands of security politics for control

(Avant, 2005b, p. 5). A failure to align the two might undermine rather than improve the security posture of states (Bitzinger, 1994; Leander, 2005).

Reflecting such theoretical considerations, the globalization of the surveillance industry has raised two major concerns with respect to international security: Potential chilling effects on human rights, and an increasing accessibility of offensive cyber capabilities that might undermine the international security architecture by allowing late comers to the cyber arms race to project power abroad (Buchanan, 2020; Clapper, 2013; Marczak, Scott-Railton, McKune, Abdul Razzak, & Deibert, 2018; Perlroth, 2021).

First, the degree to which digital surveillance and intrusion technologies undermine human rights depends on the legal regime into which they are embedded. While ideally constrained by a closely sanctioned legal process, the unchecked use of lawful interception technologies can be used on a far broader scope. This turns the technology into a convenient tool to stifle protest movements (Privacy International, 2016b; Sonne & Coker, 2011) or undermine political opposition (Privacy International, 2015). The extent of alleged PISC-enabled human rights violations is reflected in a recent call by the United Nation's Special Rapporteur David Kaye for an immediate memorandum on the operations of the market (Kaye, 2019). Crucially, human rights abuse oftentimes transgresses state boundaries when individuals outside of the country become the target of government-sponsored campaigns, as was the case with Washington Post journalist Jamal Khashoggi (Kirkpatrick, 2018).

The second dimension of concern focuses on the potential effect of the market in allowing second- and third-tier states to use offensive cyber capabilities against foreign – including Western – targets.[1] In a 2013 Senate Hearing, director of US National Intelligence James Clapper stated that "Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products. Foreign governments already use some of these tools to target US systems" (Clapper, 2013). In 2020 Brad Smith - President of Microsoft - mirrored the sentiment, warning that the market was starting to take the form of "21st-century mercenaries" and cautioning that the development risked adding "even more capability to the leading nation-state attackers, and

[1] Offensive cyber capabilities refer in this context to the National Security Agency's use of the term 'Computer Network Exploitation', meaning the ability to exploit vulnerabilities of an adversary's networks with the purpose to gain intelligence or to engage in computer network attacks and prepare the battlefield. See Kaplan (2016, p. 137)

[…] generates cyberattack proliferation to other governments that have the money but not the people to create their own weapons. In short, it adds another significant element to the cybersecurity threat landscape" (Smith, 2020).

Many of these considerations are based on guesstimates. Little is known of the broader dimensions of the market for surveillance equipment and services (for an exception see Burkart & McCourt, 2017). Apart from occasional debate following from journalistic or NGO engagement, the market has largely eclipsed public attention.[2] As a result, current knowledge is formed on the basis of extreme cases – the picture of ruthless cyber mercenaries of the 21st century (Mazzetti, Goldman, Bergman, & Perlroth, 2019). Such work has been of instrumental importance in raising awareness about market-based proliferation mechanisms but it remains limited in that it does not address the contours of the wider market into which such operations are embedded. This article widens the debate by providing a historically grounded analysis of the market. In doing so, we make two contributions. First, by mapping market structures since the early 2000s, we provide an empirical contribution that we believe to be necessary for the substantiating of political discussions about the nature and consequences of the market. Second, we argue that market structures are a key variable in explaining the ability of states to control market outcomes. In doing so, we build on recent scholarship within the field of privatized force (Mahoney, 2017, pp. 30-59; McFate, 2017). We adapt a broad definition of market structure, characterized by the concentration of vendors and buyers, the scope of market offerings, barriers to entry, geographic reach, and the ease with which market actors and products can be transferred to new locations (Swedberg, 2008, pp. 113–119). While such a definition allows us to incorporate insights from classical economic theory about the micro-positioning of market actors, it also provides for an analysis of the market in its own right with a focus on how transactions of surveillance technologies are facilitated (Coase, 1988, pp. 1–31).

Drawing on historical conference data and supported by in-depth interviews with industry insiders, we show how the wave of telecommunication privatizations of the 1990s in combination with a transformation towards digital communications provided a fertile soil for the first specialized surveillance companies in their current form to emerge. As ever new

[2] The Citizen Lab of the Munk School at the University of Toronto is a critical exception. However, despite their longstanding engagement with the market, no coherent efforts have been undertaken to place the market at the center of analysis. The work of Citizen Lab has instead focused on individual market players and products.

possibilities for the interception of communication were developed, the market moved away from an initial compliance focus towards a competitive and highly innovative posture. With the rise of encryption and improved security practices of technology manufacturers in the 2010s, surveillance and intrusion became a more demanding undertaking. PISCs responded by developing increasingly sophisticated products and knowledge transfer became a bigger part of the services on offer. The result is a transnationally operating and highly competitive market. While the globalization of the market begun on the demand side in the mid-2000s, suppliers have followed suit and are operating increasingly from outside the original US-European-Israeli triad. In this context of distributed agencies and collective action problems, public control over market actors is severely challenged. Given the expanding range of products available – partly catering overtly to military agencies – these developments make the PISC market a growing security concern.

The remainder of this article is structured as follows: The next section provides for a review of relevant literature on the causes and consequences of the privatization of force. Subsequently, methods and data are presented. Third, the early phase of market development up until the early 2000s is analyzed. The following three sections are based on our historical analysis of conference data through which we follow the evolution of PISC markets from a regional enterprise into a closely integrated global network. The three sections cover respectively the period leading up to internationalization beyond Europe and the U.S.; the early period of the global market (2008-13), and the most recent period starting roughly in 2014. For each period, we focus on the substance of product offerings, the geographies of supply and demand, and the contextual features influencing directions of change. In the seventh section, we tie the findings together. We identify similarities and divergences between private military and security markets and the here studied digital equivalent. Further, we discuss how dynamic market structures are beginning to undermine prospects of public control, and we provide a perspective on emerging private control regimes. Finally, we conclude and identify avenues for further research.

The privatization of force and corporate security

Owing to enduring waves of privatization throughout the neoliberal era, markets have taken on an ever more central role in questions of international security (Avant, 2005b; Bitzinger, 1994; Farrell & Newman, 2019; McFate, 2017; Singer, 2001). Most rigorously, this phenomenon has been studied in the context of the privatization of force (Avant, 2005b; McFate, 2017; Singer, 2008). Private military and security companies (PMSCs) have evolved into a global

phenomenon and debates have ensued as to the scope, implications, and desirability of such developments (Singer, 2008, p. 18). In many aspects, PISCs are a natural extension of private military and security markets (Chesterman, 2008). Because private intrusion and surveillance markets have largely escaped academic attention[3], existing scholarship on private force can serve as a guiding stick for the identification of patterns, historical contingencies and debates relevant to this new area of concern (Bean, 2016; Hansen, 2014).

Separating the modern PMSC from traditional mercenaries, Singer suggests that the distinctiveness of the current trend towards market-based military and security provisions in the international arena is based on the corporate organizational structure of private military firms. PMSCs are organized as legal entities, engage in profit-seeking behavior, and are embedded into wider market structures including financial and recruitment channels (Singer, 2008, p. 47).

PMSCs offer services relevant to internal security functions of the state as well to external functions related to military and intelligence operations (Abrahamsen & Williams, 2011, p. 7; Avant, 2005b). Private actors run prisons (Lundahl, Kunz, Brownell, Harris, & van Vleet, 2009), guard critical infrastructure (Parfomak, 2004), support law enforcement (Button, 2019), and provide military functions (McFate, 2017; McFate, 2016, pp. 118–129).

From a perspective of international security, concerns have been voiced as to the role of unconstrained private enterprise in facilitating the proliferation of military capabilities previously available only to the most advanced states (Avant, 2005a, p. 224; Singer, 2008, p. 170). Profit-seeking enterprise, so the argument, causes tensions regarding political accountability and creates trade-offs between private-sector enabled efficiency gains and public control over societal security (Singer, 2008, p. 235). Against such complex balancing of control and efficiency, a large body of work has argued that the privatization of force is contributing to destabilizing dynamics in the international system (Baumann & Stengel, 2014), undermining democratic processes (Avant & Sigelman, 2010; Krahmann, 2008; Verkuil, 2009), and creating unpredictable long-term consequences as key state functions are outsourced to private corporations (Heinecken, 2014; Machairas, 2014).

With market-based deliveries of core public functions, privatization causes new forms of governance and control to emerge (Avant, 2005b). While control over PMSCs remains

[3] For notable contributions see Burkart & McCourt, 2017; Harkin, Molnar, & Vowles, 2020; Ruohonen & Kimppa, 2019.

paramount, its exercise has become more complicated and is increasingly performed through the market by a more varied set of actors (Avant, 2004). Identifying and understanding such governance mechanisms is an important task for security studies in general but particularly so in the context of cybersecurity-related topics due to the overwhelming private ownership over infrastructures, resources, and expertise (Bureš & Carrapiço, 2018).

Market mechanisms of control, Avant argues, can be effective when social and material mechanisms reinforce each other, resulting in situations in which privatized force both adds to critical security functions of the state and is viewed as legitimate in the eyes of the collective (Avant, 2005b, pp. 253–256). From a perspective of political control, however, the privatization of force always implies a power shift and a potential for agency slippage in which decisions about the deployment of force no longer remain within the exclusive realm of public authority (Avant, 2005b, p. 253).

The creation of such mutually reinforcing mechanisms of control requires high levels of state capacity and is always a balancing act. However, exercising political, functional, and social control at the transnational level adds another layer of complexity (Avant, 2005b, pp. 66–69; Krahmann, 2009, pp. 23–26; see also Leander, 2005, pp. 611–618; Singer, 2008, pp. 180–182). Here, the existence of multiple principals limits the sanctioning power of any individual market actor on either the supply or demand side (Avant, 2005b, p. 66). To the extent that states attempt to regulate transnational security markets, their ability to do so is constrained by questions of extraterritoriality (McFate, 2017, pp. 160–162) and a lack of effective international regulation (Dunigan & Petersohn, 2015, pp. 10–11). Further, PMSCs tend to be less constrained by large capital investments than traditional arms manufacturers, placing additional burdens on public efforts to exercise oversight as suppliers can relocate across jurisdictions with ease and engage in regulatory arbitrage (Avant, 2005b, p. 66; McFate, 2017, p. 24).

Confronting these problems of internationally operating and highly mobile PMSCs, recent scholarship has synthesized the question of control in private security markets through the lenses of market structures (Dunigan & Petersohn, 2015; Mahoney, 2017; McFate, 2017). From this perspective, the ability to control PMSC activity is rooted in principal-agent dynamics, which in turn are shaped by the varying structures of security markets (Mahoney, 2017). For example, competitive markets that are characterized by a large number of sellers and buyers are likely to foster client segmentation and product differentiation (Avant, 2005b, pp. 219–224). As profit

margins in more respectable market segments dry up in response to high levels of competition, firms might begin to cater to demand from other regions and exploit their ability to move across regions with ease (Singer, 2008, p. 175). On the other hand, in markets characterized by a large number of suppliers and only a few buyers – an oligopsony – the principal will enjoy high levels of control through the buying power that such a market structure affords the monopsonist (McFate, 2016). Common to these approaches is an appreciation of the altered authority structures provided through the operations of the markets. In these situations, state control is linked to purchasing power (Avant, 2005b, p. 67) and exercised through for example standard-setting (McFate, 2017, pp. 162–163).

States are thus faced with a dilemma: Private companies might be better placed to develop innovate and efficient solutions, but to maintain control states need to preserve a strong bargaining position vis-à-vis their suppliers. The dynamic nature of security markets will, however, challenge such market constraints as the buying power of a single state is limited even in the case of a global superpower and market dynamics attract increasing numbers of competitors (Leander, 2005, pp. 612–613). Reacting to increased levels of competition, market actors diversify and seek to find market niches in which competition is less tense. This can result in product and service innovation, but it can equally result in strategies to diversify the client base, which in turn decreases the relative buying power of the monopsonist (McFate, 2017, pp. 162–168).

Control over private security markets needs therefore to be asserted during the early stages, when the monopsonist effectively can leverage control over market actors and define the rules of the game (McFate, 2017, p. 163). As markets internationalize, no single actor can control and define the operations of the marketplace (Garud & Karnøe, 2003; Quack, 2007).

Similar dynamics between the market and states exist for surveillance and intelligence activities, but the topic remains poorly understood (Bean, 2016; Hansen, 2014). This trend features most prominently in the United States, where evidence from the late 2000s suggests that the US intelligence community dramatically increased its reliance on contractors in the wake of the 9/11 terrorist attacks (Bean, 2016). According to some estimates, 70% of the US intelligence budget was spent on private contractors in 2007 (Chesterman, 2008), making “intelligence contracting […] a large, profitable and rapidly expanding business” (Cohen, 2010, p. 232; see also Priest & Arkin, 2010).

It has been suggested that the electronic surveillance requirements of the US post-9/11 have been a major driver of this uptick in demand, with procurements of ICT hardware and software including electronic intelligence collection and analysis capabilities being major cost factors (Chesterman, 2008). This is further underlined by the fact that in 2015 US Cyber Command awarded contracts worth $475 million to private companies to get the agency up to speed (Maurer, 2018, p. 71).

While we have a rudimentary understanding of the larger intelligence market in the U.S. (Mahoney, 2017), Maurer points to the existence of a largely unnoticed market catering to intelligence and military demands in the context of cybersecurity and offensive cyber capabilities. This market is made up by transnationally operating 'boutique firms' that offer their services to law enforcement and intelligence agencies around the world (Maurer, 2018, pp. 73–75). Burkart and McCourt characterize these market vendors as "ostensibly stateless", selling off-the-shelf spyware and offensive services around the world (Burkart & McCourt, 2017, p. 40). The existence of this market has been noted repeatedly, yet our knowledge of it remains underdeveloped (Buchanan, 2020, p. 317; Maurer, 2018, pp. 73–75; Singer, 2008, p. 175). The remainder of this article is an attempt to address this shortcoming.

Methods & Data

Trade fairs are an underexploited source of data in the otherwise notoriously secretive industry of privatized security. At these events vendors and customers interact, new products are presented, and market opportunities explored (Bathelt & Schuldt, 2008; Ramírez-Pasillas, 2010; Seringhaus & Rosson, 1994; Shires, 2018). In this article, we make use of the rich information contained in conference brochures and related documents to trace the evolution of PISC markets across the globe.

Digital surveillance technologies are nowadays a normalized part of most military trade fairs. The French Milipol conference for example hosts dedicated sections on cybersecurity and facial recognition. Other conferences are solely focused on the digital surveillance market. The "ISS World" conference series is the most well-known and important of these. With a history reaching back to 2003 and venues around the world, ISS World has earned itself the somewhat dubious title of the "Wiretappers' Ball". This title is testament to its central position in the global marketplace, bringing together "service providers, law enforcement agencies, the Federal

Government and international standards body representatives and product/service vendors" (Telestrategies, 2003).

As such, ISS World is not merely a reflection of the market but takes on a performative role, playing a key part in bringing together the European and US markets in the early 2000s, and later expanding into new regions such as the African continent. Recognizing the central place of ISS World, we have gathered conference brochures and related material through the Internet Archive and other publicly available sources. Conference brochures remained remarkably similar in form over the almost 20 years of investigation and provided extensive information on topics, sponsors, speakers, exhibitors, and training seminars. This information was coded into a comprehensive dataset, covering 5974 presentations, panels, product demonstrations, and training seminars for the period 2003-2020 across 64 conferences. This was supplemented by detailed demographic data on central companies (including home country, revenue, subsidiaries, ownership structure).

Based on this information, we conducted a historical analysis to establish trends in product evolutions and company characteristics. Information from the brochures make up the core of our analysis and arguments. To validate the thus identified trends and observations and to identify gaps in the quantitative research, 19 in-depth interviews with industry insiders, public officials, and civil society observers were conducted. A comprehensive overview of the data gathered can be found in Appendix 1. The result of this extensive data collection is a story about the growth of an industry that is neither fully autonomous nor controlled. It is a market at the nexus between law enforcement, intelligence, and cyber warfare. And it is a shadowy reflection of the unwanted side-effects of digitalization.

Despite the extensive data gathered, there are some clear limitations to our analysis. The first limitation stems from the types of data. While historical conference data can provide accurate information on general trends, qualitative data in the form of participant observations would have been a welcome supplement to gather more detailed data on the content of presentations and forms of interactions of professionals. Unfortunately, the ISS World conference is closed for the public and researchers are not welcome. Interview and attendance requests were categorically rejected by the organizers. A second limitation concerns a potential Western bias in the data. While it is well-known that Chinese and Russian vendors have become active participants on the market, we see relatively little activity of these actors in our data. A final

note of caution should be expressed regarding the top-segment of product offerings. Vendors in this segment can at times rely on direct contacts to the largest customers such as the NSA and associated Five Eyes intelligence agencies (Cox & Franceschi-Bicchierai, 2018). They do not need to market their products through conferences and trade fairs. Accordingly, a limited number of companies identified in journalistic accounts is not present in our data.

Analysis: Mapping the Wiretapper's Ball

Market Emergence: The 1990s, de-regulation and the rise of digital communications

Intercepting communications has been a staple of both law enforcement and intelligence practices for as long as communication systems existed. Famous examples like the Zimmermann Telegram, impacting the US intervention into the First World War or the legacy of Bletchley Park, are but two examples of how interception of communications has shaped history.

In the period after the world wars, telecommunications systems were largely constructed, owned, and operated by public entities, or companies with close historical and institutional ties to the state (c.f. Wu, 2011). Intercepting communications on these systems was primarily delegated to a limited set of telecommunications companies operating within a given country, either on their own or with assistance from one or two specialized firms. While some of the companies operating today trace their origins to this era, such as the Dutch vendor 'Group 2000' that was founded in 1978, these are a minority. Prior to the 1990s, both lawful interception and the market catering to it, were limited and highly controlled.

The events of the 1990s should revolutionize the field. First, the advance of networking technology and digital communications saw the emergence of a new form of communication network that was global in scope. Secondly, the explosive growth in telecommunication providers following sustained rounds of privatizations and de-monopolizations, created a much more complex environment. In both Europe and North America, new legislation was introduced that would require all telecommunication providers to comply with interception requests.[4] At

[4] Most significantly, the US 1994 CALEA act (amended in 2005 to cover digital communications and voice over IP services), and the 1995 European Union requirements on lawful interception capabilities of Member States, subsequently broadened by the 2002 Data Privacy Directive.

the end of the 1990s, the changes in technology and market structures for telecommunication services had laid the groundwork for a new age of wiretapping.

Compounding the developments within the market, the events of 9/11 provided a watershed moment that elevated interception capabilities to a level of strategic importance for security services in the US and European countries (Graham & Wood, 2003; Perlroth, 2021, p. 47). Intercepting communications was an essential component of such pre-emptive security logics (Amoore, 2006; Ball & Webster, 2003; de Goede, 2008; van Brakel & Hert, 2011) and a dominant belief in the efficiency and cost-effectiveness of private enterprise bolstered the growth of private security in the early 2000s (Abrahamsen & Williams, 2011; Bures & Carrapico, 2017). It is at this stage that the market for lawful interception and intrusion systems formally constitutes itself in the United States and Europe, capitalizing on the exploitation of digital communications and vulnerabilities where public actors lacked capacity and expertise (Abrahamsen & Williams, 2011, p. 71).

Market integration, compliance and expanding reach

The new requirements for lawful interception led to a demand for compliance-enhancing networking between the public sector, telecommunication operators, and surveillance companies. Acting on this demand, a small family-owned company named Telestrategies, which previously had organized conferences for the telecommunications industry and published an industry magazine named 'Billing World', started a new conference series in 2003 under the name of 'Intelligence Support Systems (ISS) World', conveniently located in McLean, Virginia. The invitational letter spells out the compliance demand in detail:

> Service Providers are facing increased information and technical assistance requests to support law enforcement CALEA request, subpoenas, court orders, search warrants and more. On the other hand, law enforcement agencies face subpoena backlogs, expensive telecommunications interface options to collect data and at times guarded cooperation from service providers. At ISS World 2003, the industry's premier event addressing Lawful Interception and Internet Surveillance, conference presenters and exhibitors have the answers both carriers and LEAs need now.
>
> (Telestrategies, 2003)

The early compliance focus was evident with one in five speakers at the conference from public agencies such as the FBI, DHS, or the Federal Communications Commission, and 28 internet service providers present. Over time compliance faded into the background and the role of public actors decreased. By 2006 they accounted for only one in eight of the listed speakers.

While ISS World started off as an American exercise with as little as two non-US vendors presenting in 2003[5], this situation changed quickly as the parallel European and American markets started to integrate. In 2006, almost one third of the presenting LI vendors were European (22) with an additional 8% (6) being located outside the transatlantic market.[6] With Detica, Atis Uher, and Siemens, three of the seven lead sponsors were German. Mirroring the increasing integration with European suppliers, the number of countries represented equally increased from 15 in 2003 to 33 in 2006.

Thematically, product offerings remained limited to basic lawful interception and telecommunications infrastructure, slowly expanding into mobile and wireless interceptions in 2006. With global demand increasing and a seemingly unstoppable growth of online communications and digital data, the industry entered a phase of rapid expansion over the years 2007-12. With little or no public scrutiny, and digital security remaining low on the public agenda, the period of the early global market was marked by an increasing product differentiation as telecommunications companies started to leave the market and a growing number of specialized small companies competed for new customers.

Early global market

In 2007, ISS World expanded into Europe and the Middle East, with South-East Asia following in 2008. In 2011, a fifth annual conference was added in Latin America. This expansion reflects the globalization of demand which is characteristic for this era. By 2013, 110 states would attend the conferences annually, a staggering increase of 233% since 2006. At the same time, the supply remained almost exclusively western, clustered around the US-Europe-Israeli triad. Notable exceptions, like Indian firm ClearTrail or Chinese ZTE Corporation were present but remained on the margins of the market. It was therefore a lopsided globalization: Global in demand and Western in supply. While largely confined to western suppliers, the increased demand led to a corresponding increase in vendors entering the market. According to

[5] Accuris (Ireland) and Aqsacom (France). Additionally, Verint should be mentioned, being US-Israeli.
[6] Primarily Israeli

Telestrategies' own statistics, the number of ISS vendors attending the US conference increased from 87 in 2006 to 133 (2008) and 351 in 2011. In this regard it is notable that the US conference series quickly was overtaken by the Middle Eastern and European branch as the largest and most profitable conferences. The 2012 Dubai and Prague conferences attracted 1129 and 973 participants respectively, with Kuala Lumpur in fourth place with 873 attendees in 2011.

Thematically, mobile intrusion and location, big data analysis, and deep packet inspections became prominent topics during these years. With the beginning adaption of the smartphone, mobile intrusion became a focal point for accessing relevant data for LI and intelligence purposes. The now infamous Italian vendor Hacking Team presents its mobile intrusion kit for the first time at the 2010 Prague conference, and Israeli spyware firm ELTA Systems introduced mobile location and interception tools in 2009. At the same 2010 Prague conference, German-UK company Gamma Group gives a closed session titled "Tactical Mobile Phone Infection and Interception Beyond Borders", providing the first unambiguous evidence of lawful interception tools now being supplied for operations with an international scope. One year later, in 2011, NSO Group would present their notorious Pegasus intrusion suit at the Latin American conference in Brazil. As the Stuxnet operation against Iranian nuclear facilities in Natanz provided states around the world with the proof for how powerful the exploitation of digital vulnerabilities could be in military operations, intrusion techniques were in growing demand. Rumors will have it that one company provided a closed session on its role in the Stuxnet operation. Similarly, mobile location made a first appearance in the 2007 spring US conference. Later that year, a Verint presentation suggested that "Geo-location is quickly becoming a widespread commodity, with new systems and applications appearing constantly." From 2009 onwards, mobile location has been an established part of the market with a designated conference track.

A second topic on the rise in this period is big data analysis, which grows into a key solution to the problem of ever-growing amounts of digital data. Danish ETI Connect captured this challenge nicely in their 2011 presentation "From Gigabits to Terabits: Why You Want to Work Smarter and Not Harder". Similar data handling tools are presented by German Trovicor and French Qosmos. With the advent of social media platforms, open source intelligence (OSINT) can be leveraged to connect the dots, providing information on the "Where, who and what" of

intelligence targets, as seen in the product offerings of for example US company Polaris Wireless.

Third, deep packet inspections (DPI) gained traction from 2008 onwards as an approach to cope with massive bandwidths of data. DPI is used for inspecting detailed information of packets sent over the internet, allowing for the inspection of data streams according to defined filtering criteria. DPI has a range of applications that are useful for law enforcement and operators (for example, by filtering relevant information from a bulk of data) but can equally be applied for internet censorship and eavesdropping (Bendrath & Mueller, 2011).

With the advent of the Arab Spring, the quiet days of the surveillance industry would start to be numbered as it was revealed that European firms had supplied regimes in Egypt and Syria, which in turn used the newly acquired capabilities to enable oppression and torture of dissidents (Privacy International, 2016b). The revelations led to widespread criticism and condemnation of the companies involved, even resulting in a lawsuit against French company Qosmos (Defraia, 2012). These were no single instances either, both German-English Gamma Group (McVeigh, 2011) and Italian Hacking Team were involved in similar activity regarding Egypt and Ethiopia respectively (Gibbs, 2015). Some of the systems that had been sold also had uses beyond domestic security. In the Ethiopian case, Hacking Team tools were for example found to target US residents (Marczak, Scott-Railton, & McKune, 2015). The Wikileaks release of the 'Spy Files' starting in 2011 provided detailed insights into the operations of the market, which were published in cooperation with media outlets around the world including the Washington Post, La Repubblica and Süddeutsche Zeitung among others (WikiLeaks, 2011). On top of this, the Snowden documents and various investigations of civil-society actors such as Privacy International and Amnesty International pulled the industry into the spotlight for good (Amnesty International, 2014; Privacy International, 2016a; Reporters Without Borders, 2014).

In response, the market would become increasingly secretive in the years to come. Operationally, however, the industry was far from slowing down. New challenges emerging from the increased use of encryption and improving cybersecurity practices should drive the vendors to ever more sophisticated product offerings and regulatory efforts to limit the scope of operations had little effect to the extent that they were enacted at all (Maurer, 2018, p. 149).

Consolidation of global market

In the years to follow the Snowden revelations, the geographic expansion phase of the global surveillance industry came seemingly to a halt. A final push to move into the South African region in 2014 was short-lived and eventually dropped after 2016. In this consolidating phase, market dynamics were shaped increasingly by the incorporation of new technologies such as facial recognition and responses to improved security awareness among the major technology corporations and users (Perlroth, 2021, pp. 37–38). Among the latter, basic security measures such as regular vulnerability patching and the use of encrypted communication applications had a profound impact on the viability of interception and surveillance technologies (Bellovin, Blaze, Clark, & Landau, 2014).

Vendors catering to basic lawful interception applications in the form of passive surveillance remained relatively untouched by the increasingly complex environment, even though encryption made accessing data en route less valuable (Swire & Ahmad, 2012). With growing use of encryption, access to the device itself is needed to exfiltrate the desired communication before it is encrypted (Young Sic Jeong & Shin Gak Kang, 2013). However, the improving security practices meant that the middle segment that used to supply tools on the more offensive end had to reconsider their business model. The growing costs involved in developing intrusion tools capable of infiltrating security-conscious targets meant that only those with deep pockets were able to buy them. While a 0-day[7] would trade for under $100 in early 2000, the price for similar unknown exploits increased to six-figure numbers quickly (Egelman, Herley, & van Oorschot, 2013; Perlroth, 2021, pp. 219–220). Consequently, law enforcement agencies lost their central place and the market shifted to catering to the needs of intelligence agencies. In the words of one interviewee with intimate knowledge of the industry, such tools have gone from "bullets to missiles".[8]

As law enforcement became increasingly marginalized, a new type of actor quickly took its place. With NATO's recognition of cyberspace as a fifth domain of warfare at the 2016 Warsaw summit (Minárik, 2016), military agencies started to enter the market to a greater extent.[9] The shift in customers from law enforcement to national security is evidenced by the appearance of presentations such as "CyberRange: virtual environment for cyberwarfare training" held by

[7] 0-days refer to previously unknown vulnerabilities in software code.
[8] Interview with industry insider 10/23/2020
[9] Interview with industry insider 10/23/2020

Global Security Networks (GSN), a French-owned company based in the UAE in 2019; or "Cyber Weapons, Warfare, Decryption and Evasion Platforms" and "Cyber Weapons and Remote Delivery Mechanisms. A Live Presentation for Asymmetric Warfare and Decryption of Closed Online Services" by Indian company Aglaya who subsequently were revealed to sell "Cyber Warfare Services" targeting power grids and other critical infrastructures (Franceschi-Bicchierai, 2016).

Structurally, the result was a segmentation of the market with some products and companies catering to a broad list of non-sophisticated customers and others catering to highly advanced and technically savvy customers in intelligence agencies and the military. Relying on direct contacts to intelligence and military actors, some of the top-segment suppliers such as L3-TRL (now L3Harris), Raytheon, and BAE Systems start to leave the conference series or return only occasionally.

On the supply side, these developments accelerated a re-ordering of the market. Consolidation of the market had been occurring for years, and the rising production costs put smaller companies under growing pressure as the race to develop or purchase previously unknown security vulnerabilities intensified. Resultingly, smaller companies struggling to compete had to adapt their strategies or be scooped up by larger players. Three aspects of consolidation are identified: First, a series of mergers and acquisitions by leading firms to strengthen their position and cater to the full spectrum of clients. Mergers and acquisitions have been a part of the market since its inception and is a continuous consolidating force throughout. German provider of data retention solutions Utimaco was acquired by Sophos in 2008 for $314 million (McMillan, 2008) and Israeli Verint Systems acquired German niche firm Syborg in 2011 (Verint, 2011). Classic arms manufacturers like Rohde & Schwarz bought their way into the market by acquiring Ipoque in 2011(Rohde & Schwarz, 2011) and BAE Systems aquired Detica (2008) and ETI Connect (2011) (BAE Systems, 2021). The pace of M&As has remained high over the latter years with examples such as Nuance Communications buying Spanish Agnitio in 2016 (Lee, 2016) and the abovementioned L3-TRL acquiring niche suppliers Linchpin and Azimuth in 2018 (Shoorbajee, 2018) before merging with Harris shortly thereafter (L3Harris, 2019). In 2018, a merger between the two Israeli firms Verint and NSO Group would have created an unrivalled market champion, but the $1 billion deal fell apart ultimately (Reuters, 2018).

NSO Group remains instead a good example of a second type of market consolidation, exercising a great degree of control over a limited market segment. With the company's Pegasus suite, it is a market leader in the mobile interception segment, a market that amounts according to the company's own estimate to $12 bn annually outside of the United States (Moody's, 2019). Charging $650,000 plus a $500,000 setup fee according to reporting by the New York Times (Perlroth, 2016), mobile interceptions remain one of the most profitable market segments, and NSO Group's control over it has sparked a third type of market consolidation: the formation of strategic alliance between smaller competitors to counter the market dominance of the likes of Verint or NSO Group.

In 2019, Intellexa was formed as an alliance comprising French Nexa, Israeli-Cypriot WiSpear, Israeli Senpai and Cytrox (Intellexa, 2019). Integrating the specialized expertise of their members, the alliance is now developing a shared analysis platform to cover the entire spectrum of mobile interception. Intellexa made their first appearance at ISS World Europe 2020, presenting how "Intellexa combines native 3G/4G interception and long-range WiFi interception to make field cyber operations more successful than ever". While the lasting impact of such new forms of consolidation in the market remain to be seen, the effects of public exposure following the revelations of the early 2010s has had an unambiguous effect of decreasing transparency.

Civil-society actors explained in interviews how attending the conference had become more difficult than ever.[10] Closed sessions, anonymized speakers and the use of pseudonyms have become common to the extent that it is arguably the norm. Our data shows that closed sessions accounted for approximately half of the ISS sessions since 2014. Efforts to regain the comfort of operating out of the shadows without public scrutiny are equally mirrored by industry dynamics. One trend sees companies moving their headquarters away from states with stricter export regulation and enforcement, such as German market-leader Trovicor moving to the United Arab Emirates (PitchBook, 2021)[11], or offensive intrusion specialist Gamma Group relocating to Italy from the United Kingdom.[12] Another frequently deployed tactic is the opening of subsidiaries or regional offices in third countries, with Italian company Area opening a subsidiary in Oman, or

[10] Interviews A1, A5, A7

[11] Leaked materials from 2012 displayed Trovicor's headquarters to be in Munich, while currently their headquarter is listed as Dubai, see (Trovicor, 2012).

[12] Gamma Group's homepage claims their headquarters are based in the United Kingdom, but has not updated this information since 2019 and subsequently the company has operated out of Italy (see Crunchbase, 2021 and Gamma Group, 2019)

Qosmos (owned by Swedish ENEA), recently opening offices in Singapore. Finally, a third trend is companies being acquired by investors based in countries with less oversight, such as Cobham being acquired by Impetus of India.[13]

Avoiding public scrutiny is, however, only a partial explanation for the re-location to the Middle East and Asia. While the superiority of Western spy firms has been taken for granted until recently, new competitors have emerged in areas outside of the European-Israeli-US triad. United Arab Emirates' DarkMatter became famous as the facilitator of the country's international spying and hacking efforts (Bing & Schectman, 2019). Chinese vendor Semptian entered the market initially in 2010, providing deep packet inspection services. Later, the company expanded its product offerings, being a central provider of social network monitoring tools and open source intelligence in the Asian and Middle Eastern regions. Another Chinese manufacturer, Sinovatio, entered the market in 2014 and expanded aggressively into social, network monitoring, big data analytics, and most recently 5G interception.

A final development, partly spurred by the increasing sophistication of the products on offer, has been the growth in workshops, trainings, and seminars for knowledge transfers. At the ISS World the number and scope of pre-conference workshops has increased, as has the range of topics covered. At the 2021 Dubai conference for instance, attendees could attend trainings on topics such as OSINT investigations, 5G Networking and cryptocurrency alongside more aggressive approaches such as defeating encryption and interception and Man-In-The-Middle attacks. Interviewees have confirmed similar patterns in the industry more broadly, as the growing sophistication of the industry make sufficient training a necessary component of any sale.

This latest wave of developments within the global surveillance market has produced highly sophisticated products targeted increasingly at intelligence and military actors – sometimes directly marketing "Cyber Warfare as a Service" (Cox, 2018) and requiring extensive knowledge transfers in the form of trainings and workshops. Whereas previous periods witnessed a globalization of demand, the most recent years have followed through with a beginning globalization of supply. Established industry giants like NSO Group are beginning to be challenged by smaller competitors that enter alliances and pool resources. Finally, in the

[13] Information on headquarters and mergers acquired from the Orbis database, see https://www.bvdinfo.com/en-gb/our-products/data/international/orbis

wake of public scrutiny, the industry has adopted a number of strategies to keep operating in the shadows.

Discussion

As documented in the analysis, the market for surveillance and intrusion products has evolved dramatically since the beginning of the 21st century. Mirroring these changes in market structure, state control over market actors is becoming ever more challenging. Against these structural limitations to effective control, new actors have entered the scene, attempting to fill the regulative void and confronting market actors directly. These three elements – dynamic market structures, challenges to effective control, and the emergence of private-private control mechanisms – are important to discuss.

The evolving market structure for digital arms and surveillance

Variations in market structures have a significant bearing on the ability of states to exercise control over private security markets and limit the severity of market-related externalities. Mirroring developments in the markets for private military contractors, we have documented how the initial emergence of PISCs was driven by a combination of ideological and practical considerations (Singer, 2001). As demand for surveillance products and services increased in the wake of the 9/11 attacks, it was the private sector that controlled the necessary expertise to access the digitized communications of intelligence and law enforcement targets (Abrahamsen & Williams, 2011, p. 71). Underpinned by a dominant belief in private sector efficiency and innovation, the result was a reliance of even todays most advanced Western cyber powers on private contractors to deliver the technologies for lawful interception and intelligence purposes (c.f. Maurer, 2018, pp. 37–38).

Since its inception the structure of the market for lawful interception and intrusion technologies has been dramatically altered on three dimensions. The first is a geographic expansion, resulting in a globalized marketplace. This development started out on the demand-side of the market as more and more states sought to bolster their surveillance capabilities through the marketplace and found a market centered in western states willing to provide such capabilities. This altered the demand side structure from resembling an oligopsony with a limited number of buyers to a broader and more heterogenous customer base. Whereas the initial market was structured around European and North American customers, as early as in 2006 representatives from public

agencies in 33 countries would attend the ISS conference series. A few years later, in 2013, this number had risen to 110.

Similarly, the supply-side of the market has undergone dramatic, albeit lagged, changes on two levels. First, the number of vendors catering to the market mirrors the increase in demand. In 2006, 87 vendors attended the US branch of the conference. In 2011, the number increased to 351. However, the geography of supply remained centered around the US-Europe-Israeli triad that had dominated the market since the early 2000s. Only recently has a significant number of vendors entered the market from outside these regions, while Western firms are increasingly opening subsidiaries in especially the Middle East and South-East Asia.

A second general trend has been the broadening of product offerings in the market. In the early 2000s, the market was largely compliance-oriented, driven by legal requirements in the US and Europe. The 9/11 terrorist attacks drove the number of intercepts to new heights with the number of CALEA orders growing by 62% from 2004 to 2007 (Singel, 2007). Suppliers delivered the technology required for data retention and point-and-click interceptions systems that tapped communication while travelling through the networks of internet and telecommunication service providers.

Over time, three additional categories of surveillance tools have become more important, rivalling or overtaking the central position of passive interception tools. Open-Source Intelligence Techniques leverage the growing amounts of publicly available personal data available through search engines and social media to gather information about targets. In addition, the ubiquity of mobile phones has provided ample opportunity for mobile location tracking services. If neither passive surveillance, mobile location, nor OSINT delivers the needed information, offensive intrusion tools can access the endpoint communication device to access information directly from the target's computer or smartphone. This is at times needed to circumvent encryption or to access data stored on a device. While the increasing scope of product offerings has greatly increased the capabilities of law enforcement and intelligence agencies, the growing sophistication of products puts high demands on their customers and include a high degree of knowledge transfer and customer support.

Finally, and relatedly, as the market gradually moved away from a compliance focus and broadened its supply, we observe indications of a segmentation of customers. Law enforcement agencies seem to become increasingly marginalized as police budgets do not allow for the

procurement of expensive targeted cyber intrusions packages offered at the upper scale of the market. In its place, intelligence agencies and military representatives are becoming the most important customers. The combined impact of new agencies entering the market and rising demand from outside the original marketplace has lent renewed urgency to the question of market-based control.

Re-asserting control over global surveillance markets

While the question of control is a consequence of vanishing state monopolies over security and intelligence functions, it makes little sense to compare the current market for surveillance and intrusion techniques to idealized notions of pure state agency and advocate for a return to an era in which public agencies would produce and operate surveillance tools themselves. Absent a paradigm shift in the structural relationship between states and digital markets, digital surveillance will have to involve some role for private companies. Additionally, rapid cycles of innovation have placed high barriers to the development of sufficient in-house capabilities within public agencies (Lachow, 2016; Pattison, 2020). As long as public security actors deem it necessary to incorporate offensive cyber capabilities, the private sector will have a role to play.

Without such self-sufficiency, control exercises operate through principal-agent dynamics. To minimize agency slippage, principals rely on the ability to monitor and sanction undesirable behavior. However, such capacities hinge on the market position of the buyer. While monopsonies and oligopsonies facilitate market-based control, competitive markets will not afford any individual buyer the market-power to steer developments unilaterally.

Mahoney suggested that intelligence contracting operates in a monopsony (Mahoney, 2017). While this remains relatively true for the top segment of vendors contracting with US agencies[14], we have documented that the global market has a markedly different structure. The problem of exercising control through buying power in the global marketplace is exacerbated by the fact that the market has increasingly gravitated towards the Middle East and Southeast Asian regions. As the relative buying power of US and European countries declines, the enforcement power over PISCs becomes distributed across regions and agents. Here, no single actor can control and define the operations of the marketplace (Garud & Karnøe, 2003; Quack, 2007).

[14] There are notable exceptions to this rule. For example, French Vupen has contracted with the NSA while simultaneously working with the German agency BSI.

As documented above, some vendors choose to pursue exclusive contracts with a single or limited number of states as a business strategy. This is both feasible at the most sophisticated level of the market and for vendors at the more mundane level of data retention where contracts tend to be long, and relationships characterized by trust. While the former is viable only for the most advanced vendors, the latter strategy provides for limited business opportunities and has a similar natural upper limit to saturate supply. Exclusivity is thus a luxury that only a small minority of vendors can afford in their product offerings.

Market dynamics incentivize most PISCs to broaden their client base. To control how such client diversification is performed, states cannot rely on their buying power alone. Effective control in the context of distributed agency and transnational markets requires collective action. But as the limited success of multinational efforts such as the Wassenaar Agreement indicate, collective control efforts are extremely difficult to deliver.[15] Our findings point to at least three constraining dimensions of collective control.

First, the nature of goods and services traded on the market departs significantly from that of private military and security contractors. While parts of the surveillance market provide physical equipment, many of the products are intangible software products that are ill-fitting within existing control mechanisms. Crucially, intrusion products can be largely standardized: once vulnerabilities for a certain device are weaponized, the intrusion platform can be used at scale, limited only by the fact that too broad an application might attract the interest of security researchers and render the underlying exploits useless.[16] The production costs of offensive capabilities are thus defined by high initial costs and near-zero marginal cost. This is markedly different from the deployment of private military and security services and incentivizes vendors to sell to multiple clients.

Further, private sector companies providing offensive cyber capabilities do so along a spectrum that spans from vulnerability research, through development and technical infrastructures up to intangibles such as trainings (DeSombre et al., 2021). These services have multiple use-cases. Since a vital part of the market is the dissemination of knowledge and tacit know-how (Bellovin, Landau, & Lin, 2017), it is almost impossible to limit the application of capabilities to a single end-user. An example is the so-called “Project Raven” in which the US company CyberPoint

[15] For an elaborate discussion on the inclusion of surveillance and intrusion software into the Wassennaar Agreement, see Ruohonen & Kimppa, 2019
[16] For an in-depth discussion about this, see Smeets (2016)

was hired by the United Arab Emirates in 2014 to support its anti-terrorism efforts through the application of market-leading surveillance techniques. As Emirati security officials learned about the effectiveness of these tools, they silently broadened the spectrum of targets from suspected terrorists to regime critics and later foreign intelligence targets including Turkish, Irani and Qatari officials (Bing & Schectman, 2019). Once UAE intelligence actors had internalized the offensive cyber capabilities provided by CyberPoint, the contract was terminated, and the program continued under the auspices of the newly formed Emirati company DarkMatter, with contractors either let go or transferred along.

Second, and relatedly, while the product characteristics limit the utility of end-user licenses in surveillance markets, the existence of legitimate use cases for offensive capabilities can hardly be disputed. Contrary to PMSCs, there is no viable alternative to private sector security provision. For example, enhancing the security of organizations around the world is deemed indispensable from a cybersecurity point of view. A critical aspect of such efforts is the ability to test security practices through so-called red teaming, where outside hackers try to penetrate an organization's networks and identify vulnerabilities. Disassociating such penetration-testing from more problematic transfers of offensive cyber capabilities to state actors is an enduring regulative challenge.

To complicate things further, even the transfer of designated surveillance capabilities to authoritarian regimes can be viewed as legitimate if it serves narrow security interests of exporting states. While a desire to protect human rights and prevent proliferation of technologies pulls towards limiting the transfer of technologies, other security considerations pull in the opposite direction. The European Union, for example, regularly funds capacity building initiatives for law enforcements in third countries and oftentimes these include the transfer of advanced digital surveillance technology (Privacy international, 2019). The EU Trust for Africa is a case in point. A key component of the Trust is to enhance the capacity of African states to regulate and manage migration towards the European Union (EU Emergency Trust Fund for Africa, 2021). To support this mission, the EU funded the acquisition of an IMSI catcher[17] for the border police of Niger for a total of Euro 11.5 million (Privacy International, 2019). On a more general level, Article 19 through 21 of the Convention on Cybercrime ("the Budapest

[17] An IMSI-catcher is an eavesdropping device that allows for the interception of mobile traffic and location data. It has been marketized on ISS conferences since 2012 by the Swiss firm Neosoft AG and British IP Access among others and is regularly updated to follow the rollout of new communication standards (2G, 3G, 4G etc.).

Convention") requires signatories to establish legal frameworks and processes for the lawful interception, retention and real-time monitoring of digital communications (Convention on Cybercrime, 2001).

The combination of a transnational competitive market, distributed agencies, largely intangible product types and vested interests therefore significantly hampers collective control efforts to reign in the market for surveillance and intrusion solutions. For states, the possibilities of controlling the market unilaterally based on their strong market position or collectively through international agreements are both severely challenged.

Absent such political mechanisms of control, Avant's work suggests that informal mechanisms can substitute formal control with social sanctioning. Given the close linkages between many vendors and domestic intelligence services, an intermediate strategy of internationalization caters to broader segments of customers with the tacit approval of domestic intelligence in order not to counteract national security interests.[18] This creates linkages between companies' home country and new customers that often follow historical and colonial lines.

An example is the French firm Amesys, which has been involved in controversial sale of surveillance equipment to Libya (Sonne & Coker, 2011), yet who still supplies authoritarian regimes as the one in Egypt with the tacit approval of French Intelligence (Tesquet, 2017). Similarly, Israeli market leaders Verint sell their products broadly across the globe while also maintaining a close and well-documented relationship with the country's intelligence agency Unit 8200 (Bamford, 2012). By fostering such connections, domestic security agencies can remain close taps on the foreign operations of vendors without regulating the industry or ensuring other formal means of control.

This informal form of control through market mechanisms has in turn been bolstered by personal connections between PISCs and their domestic intelligence services. Individuals at PISCs often have histories of working for intelligence agencies, as was the case in the above-mentioned 'Project Raven' for which the US vendor CyberPoint recruited more than a dozen former US intelligence operatives from among others the NSA (Bing & Schectman, 2019). Fostering these forms of personal connections is mutually beneficial as it provides control for the state and business opportunities for the companies. Moreover, it ensures a shared ethos

[18] Interview with industry insider 10/28/2020

between the intelligence agency and its suppliers, creating a sense of responsibility and purpose on both sides of the exchange.[19]

The extent of such control is, however, dependent on both the ability and willingness of domestic intelligence agencies to set boundaries. Some states appear to keep a close eye on their PISCs, while others have adopted a more laissez-fair approach.[20] As mentioned above, NSO group attended the Latin American ISS conference in 2011, presenting the at the time recently developed spyware product Pegasus. In the years following their conference attendance the company largely moved in the shadows, avoiding tradeshows until it was revealed in 2015 that they had provided the government of Panama with their spyware (Rodriguez, 2015). In 2018, amidst growing controversies, additional revelations showed that the company had supplied some 45 countries with the Pegasus spyware (Marczak et al., 2018). A similar pattern can be observed with surveillance vendor Circles, who attended conferences in 2014 and 2015 before disappearing, and who were subject to a 2020 Citizen Lab investigation, revealing that the company sold products to 25 states across four continents (Marczak, Scott-Railton, Rao, Anstis, & Deibert, 2020). While both companies have close ties to Israeli intelligence, their business history suggest they operate with a longer leash than similar companies based elsewhere (Shezaf & Jacobson, 2018). The existence of informal control over individual market actors is evident. However, there is reason to question the extent to which social control can align market outcomes with public interest.

Beyond the informal control exercised through social networks, Deborah Avant suggested that value alignment might equally put informal boundaries on business practices as "the social control of force can be said to vary by the degree to which the tools that perform security tasks reflect these prevailing societal values" (Avant, 2005b, p. 42). Contrary to the provision of security functions, for surveillance markets this alignment has never been fully warranted. To the contrary, the very act of surveillance is oftentimes recognized as an illiberal practice putting the industry at odds with many of the leading values of international society (Glasius & Michaelsen, 2018).

In sum, then, the prospects for individual and collective control over the globalized market for surveillance are impeded by the distinct market structure of the surveillance market. Adding to

[19] Interview with Industry Insider 09/23/2020
[20] For an in-depth investigation into diverging licensing practices in the European Union, see Goslinga & Tokmetzis, 2017

the complexities associated with the market for force, the digital equivalent is characterized by high mobility, widespread use-cases, and production functions that incentivize sales to multiple customers. While the early market resembled an oligopsony, once regulative efforts were discussed in the context of the Wassenaar Agreement in 2013 and the revision of dual-use export regulations in the European Union starting in 2014, market dynamics had already changed the underlying structure and placed Western countries in a more peculiar position to regulate market activities beyond their own jurisdictions. Mirroring Shawn McFate's assessment of the private military industry, it seems that the previous 'megaconsumers' in the US and Europe have missed their chance to shape professional norms, standards and best practices (McFate, 2017, p. 163).

The emergence of private control regimes

Absent state-led control over private surveillance markets, global technology companies have entered the scene and begin to fill the regulative void. In doing so, social media and technology platforms have started to take-on the job of states in defining red lines for the surveillance industry. This is both an emphatic articulation of the failure of Western states to set bare minimum standards against the most unhinged segment of the market as it is testament to novel ways through which market-based control can be exerted above and beyond the state.

In October 2019, the private messaging service WhatsApp and Facebook sued Israeli spyware vendor NSO Group for using its application to send malware to approximately 1,400 mobile phones and devices for surveillance purposes.[21] Arguing that these actions were in violation of the Computer Fraud and Abuse Act and a violation of its terms of use among others, the case has received the support of a coalition of technology giants including Microsoft, Alphabet, Cisco and Dell (Satter, 2020a), and human rights groups including Amnesty International, Privacy International and Reporters Without Borders (Satter, 2020b). In October 2020, the district court allowed the case to proceed, providing for a precedent to allocate responsibilities in the spyware market.

Similar recourse to legal matters was taken by Amnesty International, who filed a case against NSO Group at the District Court of Tel Aviv in May 2019 with the aim to force the Israeli Ministry of Defense to revoke the company's export license. This bid was, however, rejected as

[21] US District Court Northern District of California. Case No. 19-cv-07123-PJH. 2020. gov.uscourts.cand.350613.111.0.pdf

the district judge found that Amnesty did not provide sufficient evidence to document that the company's spyware was used knowingly against activists (Holmes, 2020). While it is certainly too early to judge the effectiveness of emerging private control regimes, their arrival is significant and testament to an important structural condition that differentiates private surveillance markets from traditional markets for force.[22]

While PMSCs produce direct and unmediated effects through the projection of force and manpower, effects in surveillance markets are mediated through digital platforms and technologies, drawing large multinational companies into the complex web of how this market produces security-relevant outcomes. Potentially, this enrollment of technology companies might act as a counterweight to power-asymmetries arising from the unmediated market in which latecomers to the cyber arms race can use their buying-power to develop offensive cyber capabilities to crack down on human rights and project power abroad.

Conclusions

Building on a historical analysis of almost 6000 presentations, trainings, panels, and seminars over the period 2003-20, this paper has added new detail to the discussion about the opportunities and perils of the surveillance industry. We demonstrate how the market for surveillance technology developed from initially separate but similar European and US endeavors to an integrated and highly dynamic Western supply base organized around the US-Europe-Israeli triad. Demand grew quickly and by 2008 the market had effectively globalized. While the existence of a global market has been in effect much longer than commonly assumed (Perlroth, 2021), supply would only expand in any significant volume beyond Western states in the later stages of the 2010s. However, at this stage the market itself had transformed, moving from a compliance focus to an increasingly offensive posture with the supply of intrusion products starting in 2010.

Based on these empirical findings, we have argued that the consequences of market-based surveillance solutions depend on the ability of states to control market developments. Not all markets are detached from public control, especially not security markets. In determining the possibilities of control, market structures play a significant role. If suppliers are tightly embedded into domestic security architectures – either through informal means of control or

[22] Another interesting case of private control regimes is the case against Amesys and Nexa Technologies currently in the Paris Judicial Court, see Fussell, 2021.

through captive business relationships – the existence of private markets does not necessarily pose a risk to security objectives. However, in market situations where few vendors can sustain their existence based on individual customers, control becomes a more pressing issue. With the Middle Eastern and South-East Asian regions surpassing Western states as profit centers for the industry, the market-led proliferation of offensive cyber capabilities is becoming increasingly difficult to control.

We find that the market for surveillance products is largely made up of small boutique vendors. However, as the market has grown, large defense companies have similarly entered the market and the level of mergers and acquisitions has accelerated. Further, like PMSCs, PISCs are highly mobile owing to the largely immaterial nature of product offerings and relocate quickly. Nonetheless, proximity to markets seems to be important as witnessed in the trend towards opening subsidiaries close to profit-centers.

From a meso-perspective, the market has undergone a similar development to that of other security markets. With strong roots in the European and US regions, the market emerged and evolved around the demands of a small group of states. This oligopsonistic structure provided for a favorable environment to set standards and draw red lines for acceptable behavior. However, no such efforts materialized. As the market attracted ever increasing demand from new customers inside and outside Western states, the power to shape market structures became more distributed. Consequently, efforts to reign in the market are structurally much more complex than they were in the early period of market formation and require collective efforts.

Yet, despite these similarities, a number of idiosyncrasies have been identified that undermine collective control efforts. Most importantly, products and services traded on the market are inherently dual-use. This implies that defensive capacities can be re-designed for offensive purpose with little effort and that offensive capabilities aimed for narrow use-cases in legitimate areas such as law enforcement can travel to proximate use-cases in the intelligence and military sectors. Given that capabilities require little physical hardware, this lateral proliferation is a cause of concern.

Relatedly, the dual-use nature of products spurs conflicting security interests within the administrations of exporting states. As documented, institutional frameworks incentivize the transfer of interception and surveillance capabilities for limited use cases in cybercrime prevention and border security. However, control over the use of exported capabilities post

transfer is extremely difficult, potentially adding unwittingly to the proliferation of offensive cyber capabilities around the globe. Simultaneously, the existence of an integrated market in which several vendors cater both to law enforcement and intelligence does open the question whether such an arrangement amplifies the use of advanced surveillance and intrusion products for law enforcement.

Finally, the production function of PISCs is markedly different from that of PMSCs. Whereas the latter faces significant marginal costs when expanding operations, the opposite is true for cyber capabilities that are marked by near-zero marginal cost. To what extent this structural condition drives market-led proliferation of offensive cyber capabilities is an important question for further research.

Our findings raise a number of additional questions for future inquiries. First, the question of social control could not be addressed fully in our research. To what extent relationships between vendors and intelligence agencies serve as limiting factors deserves more attention. Relatedly, anecdotal evidence points to significant variation in the willingness of public agencies to exercise social and formal control over vendors. Documenting this variation and identifying causal mechanisms promises important insights into the potential for control more generally.

Second, our findings indicate that product offerings seem to cater more closely to military customers in the latest years. Documenting the extent of this trend and the drivers thereof (including NATO's declaration of cyber as the fifth domain) will be important to gain a better understanding of market segmentation, including the question whether we are witnessing the emergence of separate markets for lawful interception and offensive capabilities respectively. Finally, surveillance vendors are embedded into multi-layered value chains. Identifying patterns of value-chain management could provide useful insights into potential avenues for control.

Appendix 1: Empirical Material

Conference Data				
Region	**Period**	**Conferences covered**	**Missing Data**	**Presentations & trainings**
America	2003-2019	17[23]	2005; 2009; 2018	1762
Europe	2008-2020	13	None	1802
Middle East	2008-2020	12	2018	967
Asia	2008-20019	12	None	885
Latin America	2011-2019	7	2014; 2017	369
Africa	2014-2016	3	None	188
Total		**64**		**5973**
Interviews				
Interview #	**Interviewee Identifier**	Date	**Sector**	Duration (minutes)
1	A1	07/09 2020	NGO	67
2	A2	09/01 2020	Research Institute	64
3	A3	09/07 2020	Politician	35
4	A4	09/08 2020	NGO	75
5	A5	09/09 2020	NGO	58
6	A6 (joint with A5)	09/09 2020	Political Advisor	58
7	A7	09/10 2020	Political Advisor	67
8	A8	09/23 2020	Private Sector	64
9	A9	10/22 2020	Public Sector	56
10	A10	10/23 2020	Private Sector	75
11		11/05 2020	Private Sector	60
12	A11	10/28 2020	Private Sector	37
13	A12	11/17 2020	Public Sector	30
14	A13	11/17 2020	Private Sector	62

[23] For the period 2004-07, the US conference was held bi-annually.

15	A14	09/21 2020	Journalist	40
16	A15	09/23 2020	NGO	67
17	A16 (joint with A15)	09/23 2020	NGO	67
18	A17	12/10 2020	Private Sector	67
19		12/14 2020	Private Sector	80

References

Abrahamsen, R., & Williams, M. C. (2011). *Security beyond the state: Private security in international politics.* Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511974441

Amnesty International (2014, November 20). *Detekt: New tool against government surveillance: Questions and Answers.* Retrieved from https://www.amnesty.org/en/latest/news/2014/11/detekt-new-tool-against-government-surveillance-questions-and-answers/

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. *Political Geography*, 25(3), 336–351. https://doi.org/10.1016/j.polgeo.2006.02.001

Avant, D. (2004). The Privatization of Security and Change in the Control of Force. *International Studies Perspectives*, 5(2), 153–157. https://doi.org/10.1111/j.1528-3577.2004.00165.x

Avant, D. (2005a). Private security companies. *New Political Economy*, 10(1), 121–131. https://doi.org/10.1080/13563460500031297

Avant, D. (2005b). *The Market for Force: The consequences of privatizing security*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511490866

Avant, D., & Sigelman, L. (2010). Private Security and Democracy: Lessons from the US in Iraq. *Security Studies*, 19(2), 230–265. https://doi.org/10.1080/09636412.2010.480906

BAE Systems (2021). *Our History.* Retrieved from https://www.baesystems.com/en/cybersecurity/about-us/our-history

Ball, K., & Webster, F. (2003). *The intensification of surveillance: Crime, terrorism and warfare in the information age*. London: Pluto Press.

Bamford, J. (2012, April 3). *Shady Companies With Ties to Israel Wiretap the U.S. for the NSA.* Wired. Retrieved from https://www.wired.com/2012/04/shady-companies-nsa/

Bathelt, H., & Schuldt, N. (2008). Between Luminaires and Meat Grinders: International Trade Fairs as Temporary Clusters. *Regional Studies*, 42(6), 853–868. https://doi.org/10.1080/00343400701543298

Baumann, R., & Stengel, F. A. (2014). Foreign policy analysis, globalisation and non-state actors: state-centric after all? *Journal of International Relations and Development*, 17(4), 489–521. https://doi.org/10.1057/jird.2013.12

Bean, H. (2016). *Privatizing Intelligence.* In Routledge Handbook of Private Security Studies. Abrahamsen, R., & Leander, A. (Eds.). London, New York: Routledge.

Bellovin, S. M., Blaze, M., Clark, S., & Landau, S. (2014). Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. *Nw. J. Tech. & Intell*, 12(1).

Bellovin, S. M., Landau, S., & Lin, H. S. (2017). Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications. *Journal of Cybersecurity*, 3(1), 59–68.

Bendrath, R., & Mueller, M. (2011). The end of the net as we know it? Deep packet inspection and internet governance. *New Media & Society*, 13(7), 1142–1160. https://doi.org/10.1177/1461444811398031

Bing, C., & Schectman, J. (2019, January 30). *Exclusive: Ex-NSA cyberspies reveal how they helped hack foes of UAE*. Retrieved from https://www.reuters.com/investigates/special-report/usa-spying-raven/

Bitzinger, R. A. (1994). The Globalization of the Arms Industry: The Next Proliferation Challenge. *International Security*, 19(2), 170–198.

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Cambridge, Massachusetts: Harvard University Press.

Bures, O., & Carrapico, H. (2017). Private security beyond private military and security companies: exploring diversity within private-public collaborations and its consequences for security governance. Crime, *Law and Social Change*, 67(3), 229–243. https://doi.org/10.1007/s10611-016-9651-5

Bureš, O., & Carrapiço, H. (Eds.) (2018). *Security privatization: How non-security-related private businesses shape security governance*. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-63010-6

Burkart, P., & McCourt, T. (2017). The international political economy of the hack: A closer look at markets for cybersecurity software. *Popular Communication*, 15(1), 37–54. https://doi.org/10.1080/15405702.2016.1269910

Button, M. *Private Policing* (2nd ed.). Abingdon: Oxon; Routledge.

Chesterman, S. (2008). We Can't Spy … If We Can't Buy! The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'. *European Journal of International Law*, 19(5), 1055–1074. https://doi.org/10.1093/ejil/chn055

Clapper, J. R. (2013, March 12). *Worldwide Threat Assessment of the US Intelligence Community: Senate Select Committee on Intelligence.* Retrieved from https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf

Coase, R. H. (1988). *The firm, the market, and the law.* Chicago, London: The University of Chicago Press.

Cohen, R. S. (2010). Putting a Human and Historical Face on Intelligence Contracting. *Orbis*, 54(2), 232–251. https://doi.org/10.1016/j.orbis.2010.01.005

Convention on Cybercrime (2001). Retrieved from https://rm.coe.int/1680081561

Cox, J. (2018, January 22). *A Spyware Company Audaciously Offers* 'Cyber Nukes'. Vice. Retrieved from https://www.vice.com/en/article/59weqb/a-spyware-company-audaciously-offers-cyber-nukes

Cox, J., & Franceschi-Bicchierai, L. (2018, January 7). *How a Tiny Startup Became the Most Important Hacking Shop You've Never Heard Of. Vice*. Retrieved from https://www.vice.com/en/article/8xdayg/iphone-zero-days-inside-azimuth-security

Crunchbase (2021). *Gamma Group*. Retrieved from https://www.crunchbase.com/organization/gamma-group

Defraia, D. (2012, July 26). *Qosmos tech company accused of aiding Syrian regime*. Global Post. Retrieved from https://www.pri.org/stories/2012-07-26/qosmos-tech-company-accused-aiding-syrian-regime

de Goede, M. (2008). The Politics of Preemption and the War on Terror in Europe. European Journal of International Relations, 14(1), 161–185. https://doi.org/10.1177/1354066107087764

DeSombre, W., Campobasso, M., Allodi, L., Shires, J., Work, J. D., Morgus, R., . . . Herr, T. (2021, January 3). *A primer on the proliferation of offensive cyber capabilities*. Retrieved from Atlantic Council website: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/#offensivecybercapabilities

Dunigan, M., & Petersohn, U. (Eds.) (2015). *The Markets for Force: Privatization of security across world regions* (1st ed.). Philadelphia, Pennsylvania: University of Pennsylvania Press.

Egelman, S., Herley, C., & van Oorschot, P. C. (2013). *Markets for zero-day exploits*. In M. E. Zurko (Ed.), ACM Digital Library, Proceedings of the 2013 workshop on New security paradigms workshop (pp. 41–46). New York, NY: ACM. https://doi.org/10.1145/2535813.2535818

EU Emergency Trust Fund for Africa (2021). *Our Mission*. Retrieved from https://ec.europa.eu/trustfundforafrica/index_en

Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351

Franceschi-Bicchierai, L. (2016, February 9). *This Leaked Catalog Offers 'Weaponized Information' That Can Flood the Web.* Vice. Retrieved from https://www.vice.com/en/article/d7ywvx/leaked-catalog-weaponized-information-twitter-aglaya

Fussell, S. (2021, June 23). *French Spyware Executives Are Indicted for Aiding Torture*. Wired. Retrieved from https://www.wired.com/story/french-spyware-executives-indicted-aiding-torture/?fbclid=IwAR0fN84qgdCXp7YrVPlNcTUbsEI_LrRkjn_1ZnW9jWysdKvO022vW2luMYo

Gamma Group (2019). *About Us*. Retrieved from https://www.gammagroup.com/

Garud, R., & Karnøe, P. (2003). Bricolage versus breakthrough: distributed and embedded agency in technology entrepreneurship. *Research Policy*, 32(2), 277–300. https://doi.org/10.1016/S0048-7333(02)00100-2

Gibbs, S. (2015, July 13). *Hacking Team boss: we sold to Ethiopia but 'we're the good guys'*. The Guardian. Retrieved from https://www.theguardian.com/technology/2015/jul/13/hacking-team-ethiopia-attack-data

Glasius, M., & Michaelsen, M. (2018). Authoritarian Practices in the Digital Age| Illiberal and Authoritarian Practices in the Digital Sphere — Prologue. *International Journal of Communication*; Vol 12 (2018), 3795–3813.

Goslinga, M., & Tokmetzis, D. (2017, February 23). The surveillance industry still sells to repressive regimes. Here's what Europe can do about it. The Correspondent. Retrieved from https://thecorrespondent.com/6249/the-surveillance-industry-still-sells-to-repressive-regimes-heres-?fbclid=IwAR28tIfhNF5QlzsDXVfNAoDsdsCjVjt8OKBHqZRHSAp4KGfkqvto45DNe7c

Graham, S., & Wood, D. (2003). Digitizing Surveillance: Categorization, Space, Inequality. *Critical Social Policy*, 23(2), 227–248. https://doi.org/10.1177/0261018303023002006

Hansen, M. (2014). Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community. *Intelligence and National Security*, 29(1), 58–81. https://doi.org/10.1080/02684527.2012.703044

Harkin, D., Molnar, A., & Vowles, E. (2020). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. *Crime, Media, Culture: An International Journal*, 16(1), 33–60. https://doi.org/10.1177/1741659018820562

Heinecken, L. (2014). Outsourcing Public Security. *Armed Forces & Society*, 40(4), 625–646. https://doi.org/10.1177/0095327X13489974

Holmes, O. (2020, July 13). *Israeli court dismisses Amnesty bid to block spyware firm NSO. The Guardian*. Retrieved from https://www.theguardian.com/world/2020/jul/13/israeli-court-dismisses-amnesty-bid-to-block-spyware-firm-nso

Intellexa (2019). *The Intelligence Alliance: About*. Retrieved from https://web.archive.org/web/20190807051349/https://intellexa.com/

Kaplan, F. M. (2016). *Dark territory: The secret history of cyber war*. New York: Simon & Schuster.

Kaye, D. (2019, June 25). *Moratorium call on surveillance technology to end 'free-for-all' abuses: UN expert* [Press release]. Retrieved from https://news.un.org/en/story/2019/06/1041231

Kinsey, C. (2007). *Corporate soldiers and international security: The rise of private military companies*. London, New York, NY: Routledge.

Kirkpatrick, D. D. (2018, December 2*). Israeli Software Helped Saudis Spy on Khashoggi, Lawusit Says.* The New York Times. Retrieved from https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html

Krahmann, E. (2008). Security: Collective Good or Commodity? *European Journal of International Relations*, 14(3), 379–404. https://doi.org/10.1177/1354066108092304

Krahmann, E. (2009). Private Security Companies and the State Monopoly on Violence: A case of norm change? *PRIF reports*: Vol. 88. Frankfurt: Peace Research Inst. Frankfurt.

L3Harris (2019, July 1*). L3harris Technologies Merger Successfully Completed; Board Of Directors, Leadership And Organization Structure Announced* [Press release]. Retrieved from https://www.l3harris.com/newsroom/press-release/2019/07/l3harris-technologies-merger-successfully-completed-board-directors

Lachow, I. (2016). The Private Sector Role in Offensive Cyber Operations: Benefits, Issues and Challenges. *SSRN Electronic Journal*. Advance online publication. https://doi.org/10.2139/ssrn.2836201

Leander, A. (2005). The Market for Force and Public Security: The Destabilizing Consequences of Private Military Companies. *Journal of Peace Research*, 42(5), 605–622. https://doi.org/10.1177/0022343305056237

Lee, J. (2016, November 9). *Nuance Communications acquires voice recognition firm Agnitio.* Biometric Update. Retrieved from https://www.biometricupdate.com/201611/nuance-communications-acquires-voice-recognition-firm-agnitio

Lind, J., & Press, D. G. (2018). Markets or Mercantilism? How China Secures Its Energy Supplies. *International Security*, 42(04), 170–204. https://doi.org/10.1162/isec_a_00310

Lundahl, B. W., Kunz, C., Brownell, C., Harris, N., & van Vleet, R. (2009). Prison Privatization. *Research on Social Work Practice*, 19(4), 383–394. https://doi.org/10.1177/1049731509331946

Machairas, D. (2014). The Ethical Implications of the Use of Private Military Force: Regulatable or Irreconcilable? *Journal of Military Ethics*, 13(1), 49–69. https://doi.org/10.1080/15027570.2014.908645

Mahoney, C. W. (2017). Buyer Beware: How Market Structure Affects Contracting and Company Performance in the Private Military Industry. *Security Studies*, 26(1), 30–59. https://doi.org/10.1080/09636412.2017.1243912

Marczak, B., Scott-Railton, J., & McKune, S. (2015). *Hacking Team Reloaded*. Retrieved from https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. J. (2018). *Hide and Seek: Tracking NSO Group's Pegasus Spyware in 45 Countries* (Research Report). University of Toronto.

Retrieved from Citizen Lab website: https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf

Marczak, B., Scott-Railton, J., Rao, S. P., Anstis, S., & Deibert, R. J. (2020). *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*. Retrieved from https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

Maurer, T. (2018). *Cyber Mercenaries*. Cambridge: Cambridge University Press.

Mazzetti, M., Goldman, A., Bergman, R., & Perlroth, N. (2019, March 21). *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments*. New York Times. Retrieved from https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html

McFate, S. (2016). PMSCs in international security sector reform. In *Routledge handbook of private security studies*. Abrahamsen, R., & Leander, A. (Eds.), 118-127. London: Routledge.

McFate, S. (2017). *The Modern Mercenary: Private armies and what they mean for world order*. Oxford: Oxford University Press.

McMillan, R. (2008, September 30). *Sophos concludes $314 million Utimaco buy*. Networkworld. Retrieved from https://www.networkworld.com/article/2277096/sophos-concludes--314-million-utimaco-buy.html

McVeigh, K. (2011, April 28). *British firm offered spying software to Egyptian regime – documents*. The Guardian. Retrieved from https://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finfisher

Minárik, T. (2016). *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*. Retrieved from https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Moody's (2019, March 12). *Moody's assigns B2 CFR to NSO Group; outlook stable*. Retrieved from https://www.moodys.com/research/Moodys-assigns-B2-CFR-to-NSO-Group-outlook-stable--PR_396559

Mousseau, M. (2019). The End of War: How a Robust Marketplace and Liberal Hegemony Are Leading to Perpetual World Peace. *International Security*, 44(1), 160–196. https://doi.org/10.1162/ISEC_a_00352

Parfomak, P. W. (2004, November). *Guarding America: Security guards and US critical infrastructure protection*. Library of Congress Washington DC. Congressional Research Service. CRS Report for Congress. Retrieved from: https://apps.dtic.mil/sti/pdfs/ADA454027.pdf

Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. European Journal of *International Security, 5(*2), 233–254. https://doi.org/10.1017/eis.2020.6

Perlroth, N. (2016, March 9). *How Spy Tech Firms Let Governments See Everything on a Smartphon*e. The New York Times. Retrieved from https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html

Perlroth, N. (2021). *This Is How They Tell Me the World Ends : The Cyber Weapons Arms Race*. Bloomsbury Publishing Plc.

PitchBook (2021). *trovicor General Information*. Retrieved from https://pitchbook.com/profiles/company/57962-98#overview

Priest, D., & Arkin, W. M. (2010, July 19). *Top Secret America: A hidden world, growing beyond contro*l. Washington Post. Retrieved from https://www.washingtonpost.com/investigations/top-secret-america/2010/07/19/hidden-world-growing-beyond-control-2/

Privacy international (2015, September 1). *Demand/Supply:: Exposing the Surveillance Industry in Colombia*. Retrieved from Privacy international website: https://privacyinternational.org/sites/default/files/2017-12/DemandSupply_English.pdf

Privacy international (2016a). *The Global Surveillance Industry*.

Privacy international (2016b). *Open Season: Building Syria's Surveillance State*. Retrieved from https://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state

Privacy international (2019, September 18). *The EU Funds Surveillance Around the World: Here's What Must be Done About it*. Retrieved from https://privacyinternational.org/long-read/3221/eu-funds-surveillance-around-world-heres-what-must-be-done-about-it

Quack, S. (2007). Legal Professionals and Transnational Law-Making: A Case of Distributed Agency. *Organization*, 14(5), 643–666. https://doi.org/10.1177/1350508407080313

Ramírez-Pasillas, M. (2010). International trade fairs as amplifiers of permanent and temporary proximities in clusters. *Entrepreneurship & Regional Development*, 22(2), 155–187. https://doi.org/10.1080/08985620902815106

Reporters Without Borders (2014). *Enemies of the Internet*. Retrieved from https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf

Reuters (2018, July 23). *Verint merger talks with Israel's NSO Group terminated: source*. Reuters: Reuters. Retrieved from https://www.reuters.com/article/us-verint-systems-m-a-nso-idUSKBN1KD15G

Rodriguez, R. (2015, August 7). *Abren sumario en caso Hacking Team. La Prensa*. Retrieved from https://www.prensa.com/locales/Espiar-obsesion-Martinelli_0_4271572998.html

Rohde & Schwarz (2011, May 23). *Rohde & Schwarz Acquires ipoque GmbH*. PRNewswire: PRNewswire. Retrieved from https://www.prnewswire.com/news-releases/rohde--schwarz-acquires-ipoque-gmbh-122454548.html

Ruohonen, J., & Kimppa, K. K. (2019). Updating the Wassenaar debate once again: Surveillance, intrusion software, and ambiguity. *Journal of Information Technology & Politics*, 16(2), 169–186. https://doi.org/10.1080/19331681.2019.1616646

Satter, R. (2020a, December 21). *Microsoft, Google, Cisco, Dell join legal battle against hacking company NSO*. Reuters. Retrieved from https://www.reuters.com/article/us-facebook-nso-cyber-idUSKBN28V2WX

Satter, R. (2020b, December 23). *Coalition of human rights groups joins suit against Israeli firm NSO*. Reuters. Retrieved from https://www.reuters.com/article/us-nso-cyber-idUSKBN28X2QS

Seringhaus, F., & Rosson, P. J. (1994). International trade fairs and foreign market involvement: Review and research directions. *International Business Review*, 3(3), 311–329. https://doi.org/10.1016/0969-5931(94)90008-6

Shezaf, H., & Jacobson, J. (2018, October 20). *Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays*. Haaretz. Retrieved from https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027

Shires, J. (2018). Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance*, 6(2), 31. https://doi.org/10.17645/pag.v6i2.1329

Shoorbajee, Z. (2018, July 11). *L3 Technologies acquires two hacking companies*. Cyberscoop. Retrieved from https://www.cyberscoop.com/l3-acquires-azimuth-and-linchpin/

Singel, R. (2007, August 29). *Point, Click … Eavesdrop: How the FBI Wiretap Net Operates*. Wired. Retrieved from https://www.wired.com/2007/08/wiretap/

Singer, P. W. (2001). Corporate Warriors: The Rise of the Privatized Military Industry and Its Ramifications for International Security. *International Security*, 26(3), 186–220.

Singer, P. W. (2008). *Corporate Warriors: The rise of the privatized military industry*. Ithaca (N.Y.), London: Cornell University Press.

Smeets, M. (2016). A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies*, 41(1-2), 6–32. https://doi.org/10.1080/01402390.2017.1288107

Smith, B. (2020). *A moment of reckoning: the need for a strong and global cybersecurity response*. Retrieved from https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

Sonne, P., & Coker, M. (2011, August 30). *Firms Aided Libyan Spies: First Look Inside Security Unit Shows How Citizens Were Tracked*. Wall Street Journal. Retrieved from https://web.archive.org/save/https://www.wsj.com/articles/SB10001424053111904199404576538721260166388

Swedberg, R. (2008). *Principles of economic sociology*. Princeton: Princeton University Press.

Swire, P., & Ahmad, K. (2012). Encryption and Globalization. *Colum. Sci. & tech. L. Rev*., 13(Spring), 416-481. Retrieved from

Telestrategies (2003). *Lawful Interception Mandates Requires an Intelligence Support Systems (ISS) Strategy*. Retrieved from https://web.archive.org/web/20030810082238fw_/http://telestrategies.com/issworld/index.htm

Tesquet, O. (2017, May 7). *Amesys: Egyptian trials and tribulations of a French digital arms dealer*. Telerama. Retrieved from https://www.telerama.fr/monde/amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php?fbclid=IwAR0fsbwVmT7FFDTCLsiamCPkZQ1jErk2xcIYReRHdryjLOZP-MIrR7yLwKQ

Trovicor (2012). *Paris Expo*, WikiLeaks.

Van Brakel, R., & Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Journal of Police Studies*, 20, 163–192.

Verint (2011, January 31). *Verint, Subsidiaries of Verint* (as of January 31, 2011) (2011); Exhibit provided to the U.S. Securities and Exchanges Commission, https://www.sec.gov/Archives/edgar/data/1166388/000095012311033115/c14986exv21w1.htm.

Verkuil, P. R. (2009). *Outsourcing sovereignty: Why privatization of government functions threatens democracy and what we can do about it*. New York: Cambridge University Press.

WikiLeaks (2011, December 1). The Spy Files.

Wu, T. (2011). *The master switch: The rise and fall of information empires*. New York: Vintage Books.

Young Sic Jeong, & Shin Gak Kang (2013). E-mail encryption methods and lawful interception methods of it. In 2013 *15th International Conference on Advanced Communications Technology* (ICACT), 29-32.

Final Remarks

I started this dissertation with an ambition to showcase the role of experts and private actors in shaping how cyber risks come to be understood and acted upon. Based on a recognition of how these processes operate through institutional settings that are characterized by epistemic uncertainty and interdependence, I have advanced an analytical framework of embedded social action within open systems of organization. The central argument put forward is that cyber risk work derives its political significance from the recursive processes through which the diagnostics of cyber risk come to be amplified across sectoral and jurisdictional boundaries to shape the contours and terms of interdependence. In that way, even the mundane activities of risk assessments in organizational contexts gain a new political significance and can shape shared understandings of what risks are and what should be done about them. As cybersecurity has become both a strategic priority and a coveted competency with demand far outstripping supply, experts and private actors take on roles that can far exceed the implementation of publicly determined rules. Instead, they can act in concert with, and at times challenge, the authority of states and other public organizations to shape the parameters of administrative and governance efforts.

Across the four case studies, variations of this argument have been explored. I have documented how the authority to speak about the unknown no longer is confined to purely technical experts, and how such expert status derives increasingly from an ability to mediate between epistemes. Acting on such opportunity structures, the case of cybersecurity capacity building has highlighted how this mediating capacity can be operationalized at the transnational level by combining global claims to best practice and access to local networks to forge and cement decisive actor coalitions. Further, the analysis of the cyber insurance industry indicated how claims to authoritative knowledge not necessarily are correlated with detailed and elaborate representations of risk. Instead, the contestation over risk quantifications showcased how the translation of risk representations into actionable advice can trump the mastery of technical complexities. Finally, through a historical analysis of the market for surveillance and interception products I showcased how such authority structures, once firmly established, can be difficult to challenge.

Throughout, it has been documented how definitional power has shaped the organization of risk through processes of diagnosis and inscription. Experts translate technical knowledge into

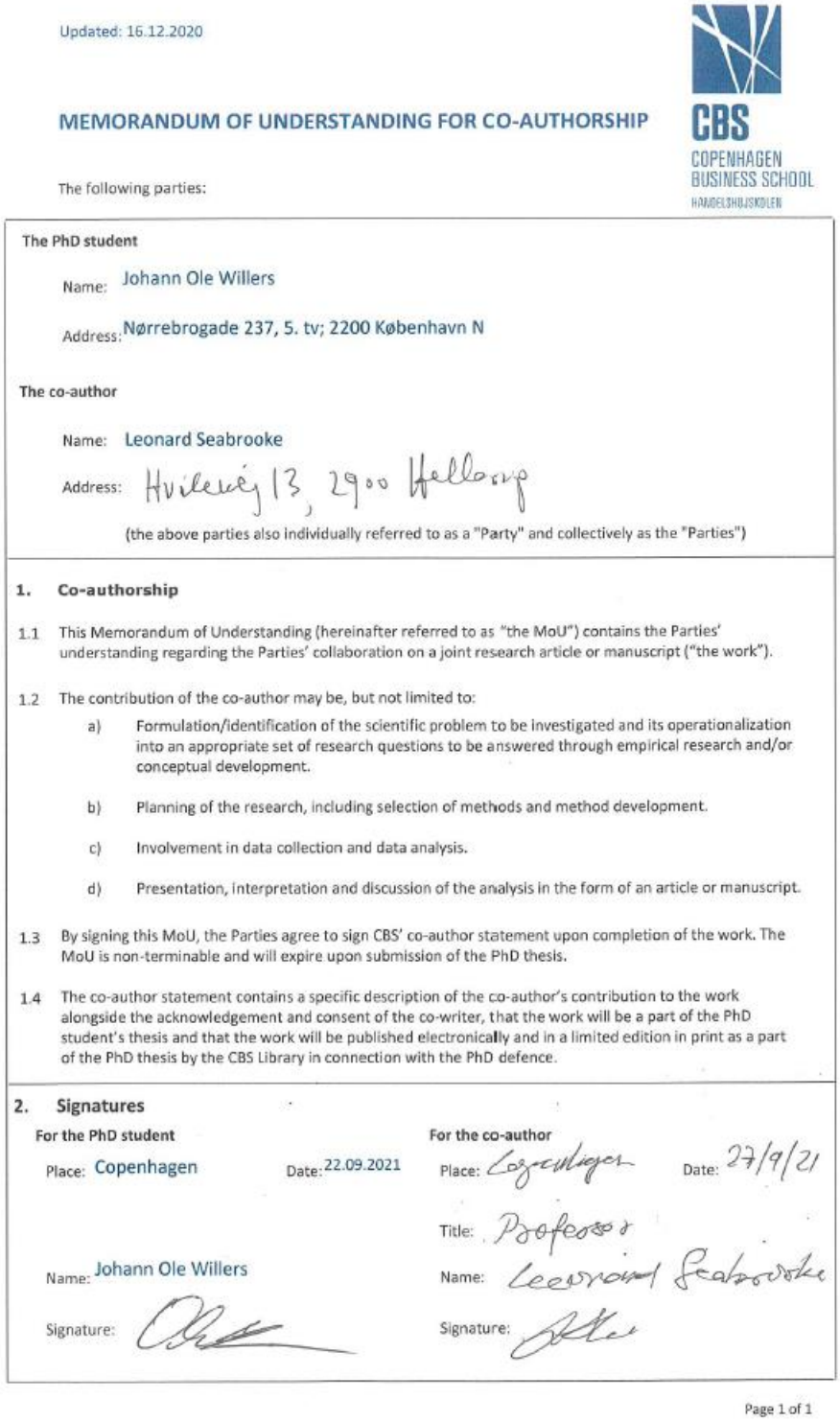
operational advice and strategies, turning interpretations of risk into mediating policies. Sometimes, such translations are advanced not solely on altruistic grounds. The strategic framing of problematizations can open new opportunities to monetize on risk and manage uncertainties. In this way, the careful crafting of consensus positions can open opportunity structures to insert oneself as the staging posts of risk management processes and to assert one's own competencies as indispensable. In this context, the seemingly unstoppable acceleration of technological developments, which more than anything else makes cyber risk work unique, proves both prospect and threat to such market-making strategies. On the one hand, early investments can consolidate interpretative authority. On the other hand, however, the 'high paced rhythm' of cybersecurity knowledge might nullify this forward-looking action. To stabilize authority positions, and to link problems to tasks, representations of risks are frequently inscribed into market devices through which the linkages between risk definitions and prescriptive action become institutionalized.

For all these reasons, markets and experts matter for both the constitution of cybersecurity as an object of concern, and for the structuring of cybersecurity practices. Concurrently, however, states, and public actors more generally, have been showcased to play active roles in these processes too. The key transnational forum for the organization of cybersecurity capacity building, for example, was established by a collaborative undertaking of the Dutch and British governments, and both countries have maintained central positions within it throughout. Similarly, the European Union Agency for Cybersecurity has initiated collaborative forums to support the calibration of cyber risk underwriting and insurance. Both examples illustrate how public actors are far from impotent in asserting forms of public authority within the organization of cyber risk. Indeed, when acting skillfully and strategically the new Realpolitik of cyber risk and control can open novel avenues for states to assert their role in shaping global and domestic rules and practices. Especially for smaller states, this is an opportunity to 'punch above one's weight'. Estonia is a prime example of this. My contention here is that such influence no longer derives naturally from rational-legal rule and bargaining power, although these aspects can remain important. Especially in the transnational sphere, but also in uncertain and interdependent contexts more generally, both public and private actors derive interpretive authority by engaging in the politics of interpretation, linking problems to solutions, and asserting oneself as the indispensable actors to deliver on the thence defined goal.

Necessarily, this research can only be a starting point. In searching for variation across cases, I maintained a focus on private actors. How such *Deutungskämpfe* over diagnostic and prescriptive authority play out in different contexts, remains an issue for further exploration. I am confident that the here provided examples are valid representations of the respective issue areas. Through rigorous data collection and continuous triangulation efforts, the findings have continuously been subjected to 'trials of strength'. However, further investigations are needed. What I hope to have achieved is to provide some inspiration for future work that seeks to explore the relationships between cybersecurity, risk, authority, and knowledge construction.

Co-Author Statements

Article 3: Linked Ecologies for Inscription-Building in Unstable Markets: The Emergence of Cyber Risk Insurance



Updated: 16.12.2020

CBS COPENHAGEN BUSINESS SCHOOL HANDELSHØJSKOLEN

MEMORANDUM OF UNDERSTANDING FOR CO-AUTHORSHIP

The following parties:

The PhD student

Name: Johann Ole Willers

Address: Nørrebrogade 237, 5. tv; 2200 København N

The co-author

Name: Leonard Seabrooke

Address: Hvilevej 13, 2900 Hellerup

(the above parties also individually referred to as a "Party" and collectively as the "Parties")

1. Co-authorship

1.1 This Memorandum of Understanding (hereinafter referred to as "the MoU") contains the Parties' understanding regarding the Parties' collaboration on a joint research article or manuscript ("the work").

1.2 The contribution of the co-author may be, but not limited to:

a) Formulation/identification of the scientific problem to be investigated and its operationalization into an appropriate set of research questions to be answered through empirical research and/or conceptual development.

b) Planning of the research, including selection of methods and method development.

c) Involvement in data collection and data analysis.

d) Presentation, interpretation and discussion of the analysis in the form of an article or manuscript.

1.3 By signing this MoU, the Parties agree to sign CBS' co-author statement upon completion of the work. The MoU is non-terminable and will expire upon submission of the PhD thesis.

1.4 The co-author statement contains a specific description of the co-author's contribution to the work alongside the acknowledgement and consent of the co-writer, that the work will be a part of the PhD student's thesis and that the work will be published electronically and in a limited edition in print as a part of the PhD thesis by the CBS Library in connection with the PhD defence.

2. Signatures

For the PhD student

Place: Copenhagen Date: 22.09.2021

Name: Johann Ole Willers

Signature:

For the co-author

Place: Copenhagen Date: 27/9/21

Title: Professor

Name: Leonard Seabrooke

Signature:

Page 1 of 1

Updated: 27.11.2020

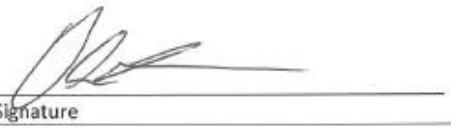
CBS
COPENHAGEN
BUSINESS SCHOOL
HANDELSHØJSKOLEN

CO-AUTHOR STATEMENT

Title of paper	Linked ecologies for inscription-building in wearable markets: The emergence of cyber risk insurance
Journal and date (if published)	na

1. Formulation/identification of the scientific problem to be investigated and its operationalization into an appropriate set of research questions to be answered through empirical research and/or conceptual development
Description of contribution: Identification of research area and identification of empirical material on which to base the study.
2. Planning of the research, including selection of methods and method development
Description of contribution: Identification of empirical materials and operationalization into a live case.
3. Involvement in data collection and data analysis
Description of contribution: Interviews were conducted by Johann Ole Willers Literature analysis was conducted by Johann Ole Willers Analysis of data was a shared undertaking.
4. Presentation, interpretation and discussion of the analysis in the form of an article or manuscript
Description of contribution: Article-writing was done collectively across all sections.

Publication
Please note that the article will be published electronically and in a limited edition in print as a part of the PhD thesis by the CBS library in connection with the PhD defence.

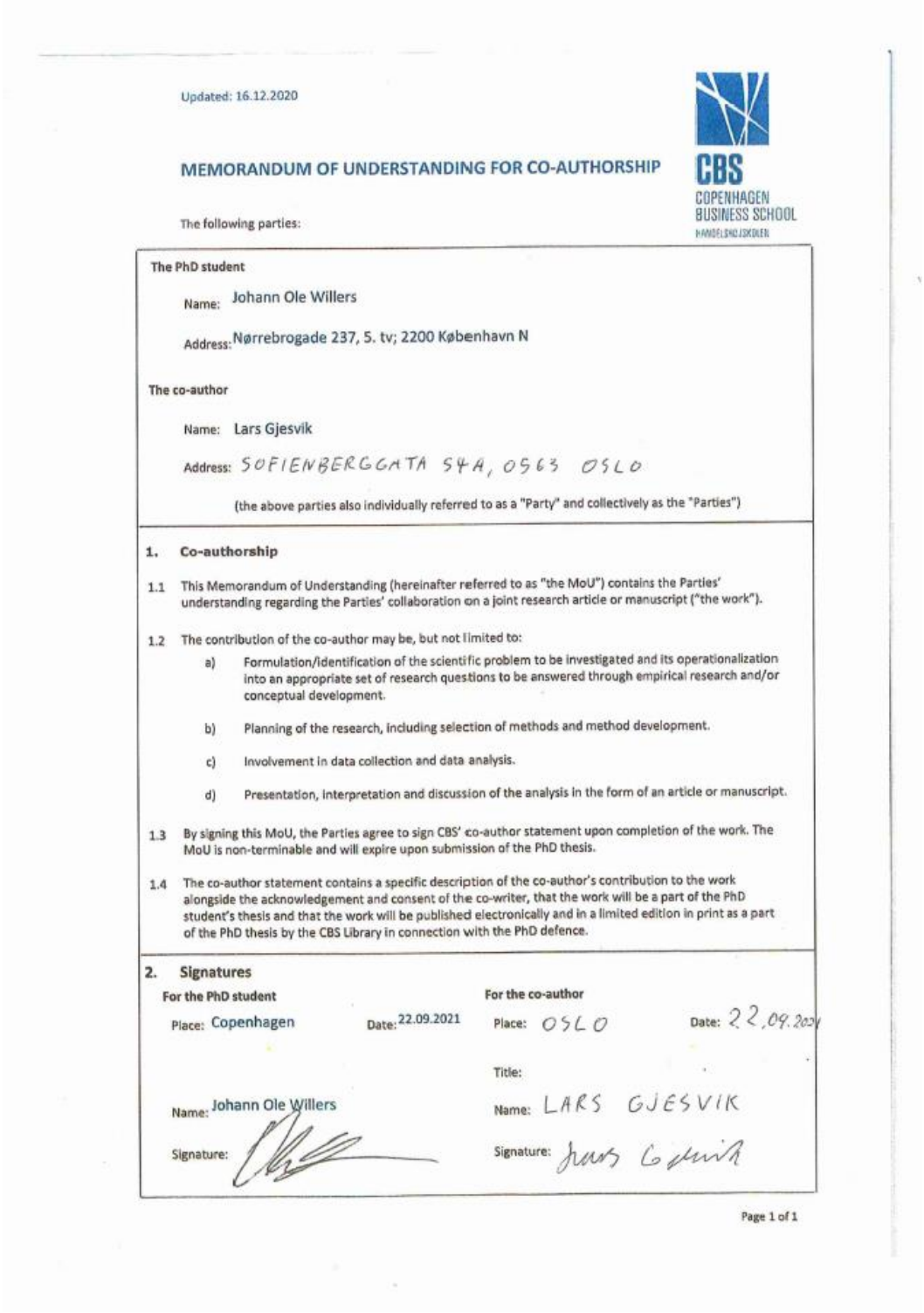
1. Co-author (PhD student)	Johann Ole Willers Name
I hereby declare that the above information is correct	
22.09.2021 Date	 Signature

2. Co-author	Professor Leonard Seabrooke Name
I hereby declare that the above information is correct	
27/9/21 Date	 Signature

3. Co-author	Name
I hereby declare that the above information is correct	
Date	Signature

4. Co-author	Name
I hereby declare that the above information is correct	
Date	Signature

Article 4: The Globalization of the Surveillance Industry



Updated: 16.12.2020

MEMORANDUM OF UNDERSTANDING FOR CO-AUTHORSHIP

CBS COPENHAGEN BUSINESS SCHOOL HANDELSHØJSKOLEN

The following parties:

The PhD student

Name: Johann Ole Willers

Address: Nørrebrogade 237, 5. tv; 2200 København N

The co-author

Name: Lars Gjesvik

Address: SOFIENBERGGATA 54A, 0563 OSLO

(the above parties also individually referred to as a "Party" and collectively as the "Parties")

1. Co-authorship

1.1 This Memorandum of Understanding (hereinafter referred to as "the MoU") contains the Parties' understanding regarding the Parties' collaboration on a joint research article or manuscript ("the work").

1.2 The contribution of the co-author may be, but not limited to:

a) Formulation/identification of the scientific problem to be investigated and its operationalization into an appropriate set of research questions to be answered through empirical research and/or conceptual development.

b) Planning of the research, including selection of methods and method development.

c) Involvement in data collection and data analysis.

d) Presentation, interpretation and discussion of the analysis in the form of an article or manuscript.

1.3 By signing this MoU, the Parties agree to sign CBS' co-author statement upon completion of the work. The MoU is non-terminable and will expire upon submission of the PhD thesis.

1.4 The co-author statement contains a specific description of the co-author's contribution to the work alongside the acknowledgement and consent of the co-writer, that the work will be a part of the PhD student's thesis and that the work will be published electronically and in a limited edition in print as a part of the PhD thesis by the CBS Library in connection with the PhD defence.

2. Signatures

For the PhD student

Place: Copenhagen Date: 22.09.2021

Name: Johann Ole Willers

Signature:

For the co-author

Place: OSLO Date: 22.09.2021

Title:

Name: LARS GJESVIK

Signature: Lars Gjesvik

Page 1 of 1

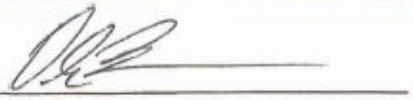
Updated: 27.11.2020

CO-AUTHOR STATEMENT

Title of paper	The Globalization of the Surveillance Industry
Journal and date (if published)	na

1. Formulation/identification of the scientific problem to be investigated and its operationalization into an appropriate set of research questions to be answered through empirical research and/or conceptual development
Description of contribution: Identification of research area and identification of empirical material on which to base the study.
2. Planning of the research, including selection of methods and method development
Description of contribution: Identification of empirical materials and operationalization into historical analysis. Co-development of methods and coding schemes.
3. Involvement in data collection and data analysis
Description of contribution: Conference data were collected collectively. Materials were coded 50/50 between the two authors. Interviews were generally conducted with both authors present.
4. Presentation, interpretation and discussion of the analysis in the form of an article or manuscript
Description of contribution: Article-writing was done collectively across all sections.

Publication
Please note that the article will be published electronically and in a limited edition in print as a part of the PhD thesis by the CBS library in connection with the PhD defence.

1. Co-author (PhD student)	Johann Ole Willers Name
I hereby declare that the above information is correct	
22.09.2021 Date	 Signature

2. Co-author	Lars Gjesvik Name
I hereby declare that the above information is correct	
22.09.2021 Date	Lars Gjesvik Signature

3. Co-author	 Name
I hereby declare that the above information is correct	
 Date	 Signature

4. Co-author	 Name
I hereby declare that the above information is correct	
 Date	 Signature

TITLER I PH.D.SERIEN:

2004

1. Martin Grieger
Internet-based Electronic Marketplaces and Supply Chain Management

2. Thomas Basbøll
LIKENESS
A Philosophical Investigation

3. Morten Knudsen
Beslutningens vaklen
En systemteoretisk analyse of moderniseringen af et amtskommunalt sundhedsvæsen 1980-2000

4. Lars Bo Jeppesen
Organizing Consumer Innovation
A product development strategy that is based on online communities and allows some firms to benefit from a distributed process of innovation by consumers

5. Barbara Dragsted
SEGMENTATION IN TRANSLATION AND TRANSLATION MEMORY SYSTEMS
An empirical investigation of cognitive segmentation and effects of integrating a TM system into the translation process

6. Jeanet Hardis
Sociale partnerskaber
Et socialkonstruktivistisk casestudie af partnerskabsaktørers virkelighedsopfattelse mellem identitet og legitimitet

7. Henriette Hallberg Thygesen
System Dynamics in Action

8. Carsten Mejer Plath
Strategisk Økonomistyring

9. Annemette Kjærgaard
Knowledge Management as Internal Corporate Venturing
– a Field Study of the Rise and Fall of a Bottom-Up Process

10. Knut Arne Hovdal
De profesjonelle i endring
Norsk ph.d., ej til salg gennem Samfundslitteratur

11. Søren Jeppesen
Environmental Practices and Greening Strategies in Small Manufacturing Enterprises in South Africa
– A Critical Realist Approach

12. Lars Frode Frederiksen
Industriel forskningsledelse
– på sporet af mønstre og samarbejde i danske forskningsintensive virksomheder

13. Martin Jes Iversen
The Governance of GN Great Nordic
– in an age of strategic and structural transitions 1939-1988

14. Lars Pynt Andersen
The Rhetorical Strategies of Danish TV Advertising
A study of the first fifteen years with special emphasis on genre and irony

15. Jakob Rasmussen
Business Perspectives on E-learning

16. Sof Thrane
The Social and Economic Dynamics of Networks
– a Weberian Analysis of Three Formalised Horizontal Networks

17. Lene Nielsen
Engaging Personas and Narrative Scenarios – a study on how a user-centered approach influenced the perception of the design process in the e-business group at AstraZeneca

18. S.J Valstad
Organisationsidentitet
Norsk ph.d., ej til salg gennem Samfundslitteratur

19. Thomas Lyse Hansen
Six Essays on Pricing and Weather risk in Energy Markets

20. Sabine Madsen
Emerging Methods – An Interpretive Study of ISD Methods in Practice

21. Evis Sinani
The Impact of Foreign Direct Investment on Efficiency, Productivity Growth and Trade: An Empirical Investigation

22. Bent Meier Sørensen
Making Events Work Or, How to Multiply Your Crisis

23. Pernille Schnoor
Brand Ethos
Om troværdige brand- og virksomhedsidentiteter i et retorisk og diskursteoretisk perspektiv

24. Sidsel Fabech
Von welchem Österreich ist hier die Rede?
Diskursive forhandlinger og magtkampe mellem rivaliserende nationale identitetskonstruktioner i østrigske pressediskurser

25. Klavs Odgaard Christensen
Sprogpolitik og identitetsdannelse i flersprogede forbundsstater
Et komparativt studie af Schweiz og Canada

26. Dana B. Minbaeva
Human Resource Practices and Knowledge Transfer in Multinational Corporations

27. Holger Højlund
Markedets politiske fornuft
Et studie af velfærdens organisering i perioden 1990-2003

28. Christine Mølgaard Frandsen
A.s erfaring
Om mellemværendets praktik i en transformation af mennesket og subjektiviteten

29. Sine Nørholm Just
The Constitution of Meaning – A Meaningful Constitution?
Legitimacy, identity, and public opinion in the debate on the future of Europe

2005

1. Claus J. Varnes
Managing product innovation through rules – The role of formal and structured methods in product development

2. Helle Hedegaard Hein
Mellem konflikt og konsensus – Dialogudvikling på hospitalsklinikker

3. Axel Rosenø
Customer Value Driven Product Innovation – A Study of Market Learning in New Product Development

4. Søren Buhl Pedersen
Making space
An outline of place branding

5. Camilla Funck Ellehave
Differences that Matter
An analysis of practices of gender and organizing in contemporary workplaces

6. Rigmor Madeleine Lond
Styring af kommunale forvaltninger

7. Mette Aagaard Andreassen
Supply Chain versus Supply Chain Benchmarking as a Means to Managing Supply Chains

8. Caroline Aggestam-Pontoppidan
From an idea to a standard
The UN and the global governance of accountants' competence

9. Norsk ph.d.

10. Vivienne Heng Ker-ni
An Experimental Field Study on the

Effectiveness of Grocer Media Advertising
Measuring Ad Recall and Recognition, Purchase Intentions and Short-Term Sales

11. Allan Mortensen
Essays on the Pricing of Corporate Bonds and Credit Derivatives

12. Remo Stefano Chiari
Figure che fanno conoscere
Itinerario sull'idea del valore cognitivo e espressivo della metafora e di altri tropi da Aristotele e da Vico fino al cognitivismo contemporaneo

13. Anders McIlquham-Schmidt
Strategic Planning and Corporate Performance
An integrative research review and a meta-analysis of the strategic planning and corporate performance literature from 1956 to 2003

14. Jens Geersbro
The TDF – PMI Case
Making Sense of the Dynamics of Business Relationships and Networks

15 Mette Andersen
Corporate Social Responsibility in Global Supply Chains
Understanding the uniqueness of firm behaviour

16. Eva Boxenbaum
Institutional Genesis: Micro – Dynamic Foundations of Institutional Change

17. Peter Lund-Thomsen
Capacity Development, Environmental Justice NGOs, and Governance: The Case of South Africa

18. Signe Jarlov
Konstruktioner af offentlig ledelse

19. Lars Stæhr Jensen
Vocabulary Knowledge and Listening Comprehension in English as a Foreign Language
An empirical study employing data elicited from Danish EFL learners

20. Christian Nielsen
Essays on Business Reporting
Production and consumption of strategic information in the market for information

21. Marianne Thejls Fischer
Egos and Ethics of Management Consultants

22. Annie Bekke Kjær
Performance management i Proces-innovation
– belyst i et social-konstruktivistisk perspektiv

23. Suzanne Dee Pedersen
GENTAGELSENS METAMORFOSE
Om organisering af den kreative gøren i den kunstneriske arbejdspraksis

24. Benedikte Dorte Rosenbrink
Revenue Management
Økonomiske, konkurrencemæssige & organisatoriske konsekvenser

25. Thomas Riise Johansen
Written Accounts and Verbal Accounts
The Danish Case of Accounting and Accountability to Employees

26. Ann Fogelgren-Pedersen
The Mobile Internet: Pioneering Users' Adoption Decisions

27. Birgitte Rasmussen
Ledelse i fællesskab – de tillidsvalgtes fornyende rolle

28. Gitte Thit Nielsen
Remerger
– skabende ledelseskræfter i fusion og opkøb

29. Carmine Gioia
A MICROECONOMETRIC ANALYSIS OF MERGERS AND ACQUISITIONS

30. Ole Hinz
Den effektive forandringsleder: pilot, pædagog eller politiker?
Et studie i arbejdslederes meningstilskrivninger i forbindelse med vellykket gennemførelse af ledelsesinitierede forandringsprojekter

31. Kjell-Åge Gotvassli
Et praksisbasert perspektiv på dynamiske
læringsnettverk i toppidretten
Norsk ph.d., ej til salg gennem Samfundslitteratur

32. Henriette Langstrup Nielsen
Linking Healthcare
An inquiry into the changing performances of web-based technology for asthma monitoring

33. Karin Tweddell Levinsen
Virtuel Uddannelsespraksis
Master i IKT og Læring – et casestudie i hvordan proaktiv proceshåndtering kan forbedre praksis i virtuelle læringsmiljøer

34. Anika Liversage
Finding a Path
Labour Market Life Stories of Immigrant Professionals

35. Kasper Elmquist Jørgensen
Studier i samspillet mellem stat og erhvervsliv i Danmark under
1. verdenskrig

36. Finn Janning
A DIFFERENT STORY
Seduction, Conquest and Discovery

37. Patricia Ann Plackett
Strategic Management of the Radical Innovation Process
Leveraging Social Capital for Market Uncertainty Management

2006

1. Christian Vintergaard
Early Phases of Corporate Venturing

2. Niels Rom-Poulsen
Essays in Computational Finance

3. Tina Brandt Husman
Organisational Capabilities, Competitive Advantage & Project-Based Organisations
The Case of Advertising and Creative Good Production

4. Mette Rosenkrands Johansen
Practice at the top
– how top managers mobilise and use non-financial performance measures

5. Eva Parum
Corporate governance som strategisk kommunikations- og ledelsesværktøj

6. Susan Aagaard Petersen
Culture's Influence on Performance Management: The Case of a Danish Company in China

7. Thomas Nicolai Pedersen
The Discursive Constitution of Organizational Governance – Between unity and differentiation
The Case of the governance of environmental risks by World Bank environmental staff

8. Cynthia Selin
Volatile Visions: Transactons in Anticipatory Knowledge

9. Jesper Banghøj
Financial Accounting Information and Compensation in Danish Companies

10. Mikkel Lucas Overby
Strategic Alliances in Emerging High-Tech Markets: What's the Difference and does it Matter?

11. Tine Aage
External Information Acquisition of Industrial Districts and the Impact of Different Knowledge Creation Dimensions

A case study of the Fashion and Design Branch of the Industrial District of Montebelluna, NE Italy

12. Mikkel Flyverbom
Making the Global Information Society Governable
On the Governmentality of Multi-Stakeholder Networks

13. Anette Grønning
Personen bag
Tilstedevær i e-mail som interaktionsform mellem kunde og medarbejder i dansk forsikringskontekst

14. Jørn Helder
One Company – One Language?
The NN-case

15. Lars Bjerregaard Mikkelsen
Differing perceptions of customer value
Development and application of a tool for mapping perceptions of customer value at both ends of customer-supplier dyads in industrial markets

16. Lise Granerud
Exploring Learning
Technological learning within small manufacturers in South Africa

17. Esben Rahbek Pedersen
Between Hopes and Realities:
Reflections on the Promises and Practices of Corporate Social Responsibility (CSR)

18. Ramona Samson
The Cultural Integration Model and European Transformation.
The Case of Romania

2007

1. Jakob Vestergaard
Discipline in The Global Economy
Panopticism and the Post-Washington Consensus

2. Heidi Lund Hansen
Spaces for learning and working
A qualitative study of change of work, management, vehicles of power and social practices in open offices

3. Sudhanshu Rai
Exploring the internal dynamics of software development teams during user analysis
A tension enabled Institutionalization Model; "Where process becomes the objective"

4. Norsk ph.d.
Ej til salg gennem Samfundslitteratur

5. Serden Ozcan
EXPLORING HETEROGENEITY IN ORGANIZATIONAL ACTIONS AND OUTCOMES
A Behavioural Perspective

6. Kim Sundtoft Hald
Inter-organizational Performance Measurement and Management in Action
– An Ethnography on the Construction of Management, Identity and Relationships

7. Tobias Lindeberg
Evaluative Technologies
Quality and the Multiplicity of Performance

8. Merete Wedell-Wedellsborg
Den globale soldat
Identitetsdannelse og identitetsledelse i multinationale militære organisationer

9. Lars Frederiksen
Open Innovation Business Models
Innovation in firm-hosted online user communities and inter-firm project ventures in the music industry
– A collection of essays

10. Jonas Gabrielsen
Retorisk toposlære – fra statisk 'sted' til persuasiv aktivitet

11. Christian Moldt-Jørgensen
Fra meningsløs til meningsfuld evaluering.
Anvendelsen af studentertilfredshedsmålinger på de korte og mellemlange videregående uddannelser set fra et psykodynamisk systemperspektiv

12. Ping Gao
Extending the application of actor-network theory
Cases of innovation in the telecommunications industry

13. Peter Mejlby
Frihed og fængsel, en del af den samme drøm?
Et phronetisk baseret casestudie af frigørelsens og kontrollens sameksistens i værdibaseret ledelse!

14. Kristina Birch
Statistical Modelling in Marketing

15. Signe Poulsen
Sense and sensibility:
The language of emotional appeals in insurance marketing

16. Anders Bjerre Trolle
Essays on derivatives pricing and dynamic asset allocation

17. Peter Feldhütter
Empirical Studies of Bond and Credit Markets

18. Jens Henrik Eggert Christensen
Default and Recovery Risk Modeling and Estimation

19. Maria Theresa Larsen
Academic Enterprise: A New Mission for Universities or a Contradiction in Terms?
Four papers on the long-term implications of increasing industry involvement and commercialization in academia

20. Morten Wellendorf
Postimplementering af teknologi i den offentlige forvaltning
Analyser af en organisations kontinuerlige arbejde med informationsteknologi

21. Ekaterina Mhaanna
Concept Relations for Terminological Process Analysis

22. Stefan Ring Thorbjørnsen
Forsvaret i forandring
Et studie i officerers kapabiliteter under påvirkning af omverdenens forandringspres mod øget styring og læring

23. Christa Breum Amhøj
Det selvskabte medlemskab om managementstaten, dens styringsteknologier og indbyggere

24. Karoline Bromose
Between Technological Turbulence and Operational Stability
– An empirical case study of corporate venturing in TDC

25. Susanne Justesen
Navigating the Paradoxes of Diversity in Innovation Practice
– A Longitudinal study of six very different innovation processes – in practice

26. Luise Noring Henler
Conceptualising successful supply chain partnerships
– Viewing supply chain partnerships from an organisational culture perspective

27. Mark Mau
Kampen om telefonen
Det danske telefonvæsen under den tyske besættelse 1940-45

28. Jakob Halskov
The semiautomatic expansion of existing terminological ontologies using knowledge patterns discovered

on the WWW – an implementation and evaluation

29. Gergana Koleva
European Policy Instruments Beyond Networks and Structure: The Innovative Medicines Initiative

30. Christian Geisler Asmussen
Global Strategy and International Diversity: A Double-Edged Sword?

31. Christina Holm-Petersen
Stolthed og fordom
Kultur- og identitetsarbejde ved skabelsen af en ny sengeafdeling gennem fusion

32. Hans Peter Olsen
Hybrid Governance of Standardized States
Causes and Contours of the Global Regulation of Government Auditing

33. Lars Bøge Sørensen
Risk Management in the Supply Chain

34. Peter Aagaard
Det unikkes dynamikker
De institutionelle mulighedsbetingelser bag den individuelle udforskning i professionelt og frivilligt arbejde

35. Yun Mi Antorini
Brand Community Innovation
An Intrinsic Case Study of the Adult Fans of LEGO Community

36. Joachim Lynggaard Boll
Labor Related Corporate Social Performance in Denmark
Organizational and Institutional Perspectives

2008

1. Frederik Christian Vinten
Essays on Private Equity

2. Jesper Clement
Visual Influence of Packaging Design on In-Store Buying Decisions

3. Marius Brostrøm Kousgaard
Tid til kvalitetsmåling?
– Studier af indrulleringsprocesser i forbindelse med introduktionen af kliniske kvalitetsdatabaser i speciallægepraksissektoren

4. Irene Skovgaard Smith
Management Consulting in Action
Value creation and ambiguity in client-consultant relations

5. Anders Rom
Management accounting and integrated information systems
How to exploit the potential for management accounting of information technology

6. Marina Candi
Aesthetic Design as an Element of Service Innovation in New Technology-based Firms

7. Morten Schnack
Teknologi og tværfaglighed
– en analyse af diskussionen omkring indførelse af EPJ på en hospitalsafdeling

8. Helene Balslev Clausen
Juntos pero no revueltos – un estudio sobre emigrantes norteamericanos en un pueblo mexicano

9. Lise Justesen
Kunsten at skrive revisionsrapporter. En beretning om forvaltningsrevisionens beretninger

10. Michael E. Hansen
The politics of corporate responsibility: CSR and the governance of child labor and core labor rights in the 1990s

11. Anne Roepstorff
Holdning for handling – en etnologisk undersøgelse af Virksomheders Sociale Ansvar/CSR

12. Claus Bajlum
Essays on Credit Risk and Credit Derivatives

13. Anders Bojesen
The Performative Power of Competence – an Inquiry into Subjectivity and Social Technologies at Work

14. Satu Reijonen
Green and Fragile
A Study on Markets and the Natural Environment

15. Ilduara Busta
Corporate Governance in Banking
A European Study

16. Kristian Anders Hvass
A Boolean Analysis Predicting Industry Change: Innovation, Imitation & Business Models
The Winning Hybrid: A case study of isomorphism in the airline industry

17. Trine Paludan
De uvidende og de udviklingsparate
Identitet som mulighed og restriktion blandt fabriksarbejdere på det aftayloriserede fabriksgulv

18. Kristian Jakobsen
Foreign market entry in transition economies: Entry timing and mode choice

19. Jakob Elming
Syntactic reordering in statistical machine translation

20. Lars Brømsøe Termansen
Regional Computable General Equilibrium Models for Denmark
Three papers laying the foundation for regional CGE models with agglomeration characteristics

21. Mia Reinholt
The Motivational Foundations of Knowledge Sharing

22. Frederikke Krogh-Meibom
The Co-Evolution of Institutions and Technology
– A Neo-Institutional Understanding of Change Processes within the Business Press – the Case Study of Financial Times

23. Peter D. Ørberg Jensen
OFFSHORING OF ADVANCED AND HIGH-VALUE TECHNICAL SERVICES: ANTECEDENTS, PROCESS DYNAMICS AND FIRMLEVEL IMPACTS

24. Pham Thi Song Hanh
Functional Upgrading, Relational Capability and Export Performance of Vietnamese Wood Furniture Producers

25. Mads Vangkilde
Why wait?
An Exploration of first-mover advantages among Danish e-grocers through a resource perspective

26. Hubert Buch-Hansen
Rethinking the History of European Level Merger Control
A Critical Political Economy Perspective

2009

1. Vivian Lindhardsen
From Independent Ratings to Communal Ratings: A Study of CWA Raters' Decision-Making Behaviours

2. Guðrið Weihe
Public-Private Partnerships: Meaning and Practice

3. Chris Nøkkentved
Enabling Supply Networks with Collaborative Information Infrastructures
An Empirical Investigation of Business Model Innovation in Supplier Relationship Management

4. Sara Louise Muhr
Wound, Interrupted – On the Vulnerability of Diversity Management

5. Christine Sestoft
Forbrugeradfærd i et Stats- og Livsformsteoretisk perspektiv

6. Michael Pedersen
Tune in, Breakdown, and Reboot: On the production of the stress-fit self-managing employee

7. Salla Lutz
Position and Reposition in Networks – Exemplified by the Transformation of the Danish Pine Furniture Manufacturers

8. Jens Forssbæck
Essays on market discipline in commercial and central banking

9. Tine Murphy
Sense from Silence – A Basis for Organised Action
How do Sensemaking Processes with Minimal Sharing Relate to the Reproduction of Organised Action?

10. Sara Malou Strandvad
Inspirations for a new sociology of art: A sociomaterial study of development processes in the Danish film industry

11. Nicolaas Mouton
On the evolution of social scientific metaphors:
A cognitive-historical enquiry into the divergent trajectories of the idea that collective entities – states and societies, cities and corporations – are biological organisms.

12. Lars Andreas Knutsen
Mobile Data Services:
Shaping of user engagements

13. Nikolaos Theodoros Korfiatis
Information Exchange and Behavior
A Multi-method Inquiry on Online Communities

14. Jens Albæk
Forestillinger om kvalitet og tværfaglighed på sygehuse
– skabelse af forestillinger i læge- og plejegrupperne angående relevans af nye idéer om kvalitetsudvikling gennem tolkningsprocesser

15. Maja Lotz
The Business of Co-Creation – and the Co-Creation of Business

16. Gitte P. Jakobsen
Narrative Construction of Leader Identity in a Leader Development Program Context

17. Dorte Hermansen
"Living the brand" som en brandorienteret dialogisk praxis:
Om udvikling af medarbejdernes brandorienterede dømmekraft

18. Aseem Kinra
Supply Chain (logistics) Environmental Complexity

19. Michael Nørager
How to manage SMEs through the transformation from non innovative to innovative?

20. Kristin Wallevik
Corporate Governance in Family Firms
The Norwegian Maritime Sector

21. Bo Hansen Hansen
Beyond the Process
Enriching Software Process Improvement with Knowledge Management

22. Annemette Skot-Hansen
Franske adjektivisk afledte adverbier, der tager præpositionssyntagmer indledt med præpositionen à som argumenter
En valensgrammatisk undersøgelse

23. Line Gry Knudsen
Collaborative R&D Capabilities
In Search of Micro-Foundations

24. Christian Scheuer
Employers meet employees
Essays on sorting and globalization

25. Rasmus Johnsen
The Great Health of Melancholy
A Study of the Pathologies of Performativity

26. Ha Thi Van Pham
Internationalization, Competitiveness Enhancement and Export Performance of Emerging Market Firms:
Evidence from Vietnam

27. Henriette Balieu
Kontrolbegrebets betydning for kausativalternationen i spansk
En kognitiv-typologisk analyse

2010

1. Yen Tran
Organizing Innovationin Turbulent Fashion Market
Four papers on how fashion firms create and appropriate innovation value

2. Anders Raastrup Kristensen
Metaphysical Labour
Flexibility, Performance and Commitment in Work-Life Management

3. Margrét Sigrún Sigurdardottir
Dependently independent
Co-existence of institutional logics in the recorded music industry

4. Ásta Dis Óladóttir
Internationalization from a small domestic base:
An empirical analysis of Economics and Management

5. Christine Secher
E-deltagelse i praksis – politikernes og forvaltningens medkonstruktion og konsekvenserne heraf

6. Marianne Stang Våland
What we talk about when we talk about space:
End User Participation between Processes of Organizational and Architectural Design

7. Rex Degnegaard
Strategic Change Management
Change Management Challenges in the Danish Police Reform

8. Ulrik Schultz Brix
Værdi i rekruttering – den sikre beslutning
En pragmatisk analyse af perception og synliggørelse af værdi i rekrutterings- og udvælgelsesarbejdet

9. Jan Ole Similä
Kontraktsledelse
Relasjonen mellom virksomhetsledelse og kontraktshåndtering, belyst via fire norske virksomheter

10. Susanne Boch Waldorff
Emerging Organizations: In between local translation, institutional logics and discourse

11. Brian Kane
Performance Talk
Next Generation Management of Organizational Performance

12. Lars Ohnemus
Brand Thrust: Strategic Branding and Shareholder Value
An Empirical Reconciliation of two Critical Concepts

13. Jesper Schlamovitz
Håndtering af usikkerhed i film- og byggeprojekter

14. Tommy Moesby-Jensen
Det faktiske livs forbindtlighed
Førsokratisk informeret, ny-aristotelisk ἦθος-tænkning hos Martin Heidegger

15. Christian Fich
Two Nations Divided by Common Values
French National Habitus and the Rejection of American Power

16. Peter Beyer
Processer, sammenhængskraft og fleksibilitet
Et empirisk casestudie af omstillingsforløb i fire virksomheder

17. Adam Buchhorn
Markets of Good Intentions
Constructing and Organizing Biogas Markets Amid Fragility and Controversy

18. Cecilie K. Moesby-Jensen
Social læring og fælles praksis
Et mixed method studie, der belyser læringskonsekvenser af et lederkursus for et praksisfællesskab af offentlige mellemledere

19. Heidi Boye
Fødevarer og sundhed i senmodernismen
– En indsigt i hyggefænomenet og de relaterede fødevarepraksisser

20. Kristine Munkgård Pedersen
Flygtige forbindelser og midlertidige mobiliseringer
Om kulturel produktion på Roskilde Festival

21. Oliver Jacob Weber
Causes of Intercompany Harmony in Business Markets – An Empirical Investigation from a Dyad Perspective

22. Susanne Ekman
Authority and Autonomy
Paradoxes of Modern Knowledge Work

23. Anette Frey Larsen
Kvalitetsledelse på danske hospitaler
– Ledelsernes indflydelse på introduktion og vedligeholdelse af kvalitetsstrategier i det danske sundhedsvæsen

24. Toyoko Sato
Performativity and Discourse: Japanese Advertisements on the Aesthetic Education of Desire

25. Kenneth Brinch Jensen
Identifying the Last Planner System
Lean management in the construction industry

26. Javier Busquets
Orchestrating Network Behavior for Innovation

27. Luke Patey
The Power of Resistance: India's National Oil Company and International Activism in Sudan

28. Mette Vedel
Value Creation in Triadic Business Relationships. Interaction, Interconnection and Position

29. Kristian Tørning
Knowledge Management Systems in Practice – A Work Place Study

30. Qingxin Shi
An Empirical Study of Thinking Aloud Usability Testing from a Cultural Perspective

31. Tanja Juul Christiansen
Corporate blogging: Medarbejderes kommunikative handlekraft

32. Malgorzata Ciesielska
Hybrid Organisations.
A study of the Open Source – business setting

33. Jens Dick-Nielsen
Three Essays on Corporate Bond Market Liquidity

34. Sabrina Speiermann
Modstandens Politik
Kampagnestyring i Velfærdsstaten.
En diskussion af trafikkampagners styringspotentiale

35. Julie Uldam
Fickle Commitment. Fostering political engagement in 'the flighty world of online activism'

36. Annegrete Juul Nielsen
Traveling technologies and transformations in health care

37. Athur Mühlen-Schulte
Organising Development
Power and Organisational Reform in the United Nations Development Programme

38. Louise Rygaard Jonas
Branding på butiksgulvet
Et case-studie af kultur- og identitetsarbejdet i Kvickly

2011

1. Stefan Fraenkel
Key Success Factors for Sales Force Readiness during New Product Launch
A Study of Product Launches in the Swedish Pharmaceutical Industry

2. Christian Plesner Rossing
International Transfer Pricing in Theory and Practice

3. Tobias Dam Hede
Samtalekunst og ledelsesdisciplin
– en analyse af coachingsdiskursens genealogi og governmentality

4. Kim Pettersson
Essays on Audit Quality, Auditor Choice, and Equity Valuation

5. Henrik Merkelsen
The expert-lay controversy in risk research and management. Effects of institutional distances. Studies of risk definitions, perceptions, management and communication

6. Simon S. Torp
Employee Stock Ownership:
Effect on Strategic Management and Performance

7. Mie Harder
Internal Antecedents of Management Innovation

8. Ole Helby Petersen
Public-Private Partnerships: Policy and Regulation – With Comparative and Multi-level Case Studies from Denmark and Ireland

9. Morten Krogh Petersen
'Good' Outcomes. Handling Multiplicity in Government Communication

10. Kristian Tangsgaard Hvelplund
Allocation of cognitive resources in translation - an eye-tracking and key-logging study

11. Moshe Yonatany
The Internationalization Process of Digital Service Providers

12. Anne Vestergaard
Distance and Suffering
Humanitarian Discourse in the age of Mediatization

13. Thorsten Mikkelsen
Personligsheds indflydelse på forretningsrelationer

14. Jane Thostrup Jagd
Hvorfor fortsætter fusionsbølgen udover "the tipping point"?
– en empirisk analyse af information og kognitioner om fusioner

15. Gregory Gimpel
Value-driven Adoption and Consumption of Technology: Understanding Technology Decision Making

16. Thomas Stengade Sønderskov
Den nye mulighed
Social innovation i en forretningsmæssig kontekst

17. Jeppe Christoffersen
Donor supported strategic alliances in developing countries

18. Vibeke Vad Baunsgaard
Dominant Ideological Modes of Rationality: Cross functional

integration in the process of product innovation

19. Throstur Olaf Sigurjonsson
Governance Failure and Icelands's Financial Collapse

20. Allan Sall Tang Andersen
Essays on the modeling of risks in interest-rate and inflation markets

21. Heidi Tscherning
Mobile Devices in Social Contexts

22. Birgitte Gorm Hansen
Adapting in the Knowledge Economy Lateral Strategies for Scientists and Those Who Study Them

23. Kristina Vaarst Andersen
Optimal Levels of Embeddedness The Contingent Value of Networked Collaboration

24. Justine Grønbæk Pors
Noisy Management A History of Danish School Governing from 1970-2010

25. Stefan Linder
Micro-foundations of Strategic Entrepreneurship Essays on Autonomous Strategic Action

26. Xin Li
Toward an Integrative Framework of National Competitiveness An application to China

27. Rune Thorbjørn Clausen
Værdifuld arkitektur Et eksplorativt studie af bygningers rolle i virksomheders værdiskabelse

28. Monica Viken
Markedsundersøkelser som bevis i varemerke- og markedsføringsrett

29. Christian Wymann
Tattooing The Economic and Artistic Constitution of a Social Phenomenon

30. Sanne Frandsen
Productive Incoherence A Case Study of Branding and Identity Struggles in a Low-Prestige Organization

31. Mads Stenbo Nielsen
Essays on Correlation Modelling

32. Ivan Häuser
Følelse og sprog Etablering af en ekspressiv kategori, eksemplificeret på russisk

33. Sebastian Schwenen
Security of Supply in Electricity Markets

2012

1. Peter Holm Andreasen
The Dynamics of Procurement Management - A Complexity Approach

2. Martin Haulrich
Data-Driven Bitext Dependency Parsing and Alignment

3. Line Kirkegaard
Konsulenten i den anden nat En undersøgelse af det intense arbejdsliv

4. Tonny Stenheim
Decision usefulness of goodwill under IFRS

5. Morten Lind Larsen
Produktivitet, vækst og velfærd Industrirådet og efterkrigstidens Danmark 1945 - 1958

6. Petter Berg
Cartel Damages and Cost Asymmetries

7. Lynn Kahle
Experiential Discourse in Marketing A methodical inquiry into practice and theory

8. Anne Roelsgaard Obling
Management of Emotions in Accelerated Medical Relationships

9. Thomas Frandsen
Managing Modularity of Service Processes Architecture

10. Carina Christine Skovmøller
CSR som noget særligt
Et casestudie om styring og meningsskabelse i relation til CSR ud fra en intern optik

11. Michael Tell
Fradragsbeskæring af selskabers finansieringsudgifter
En skatteretlig analyse af SEL §§ 11, 11B og 11C

12. Morten Holm
Customer Profitability Measurement Models
Their Merits and Sophistication across Contexts

13. Katja Joo Dyppel
Beskatning af derivater
En analyse af dansk skatteret

14. Esben Anton Schultz
Essays in Labor Economics
Evidence from Danish Micro Data

15. Carina Risvig Hansen
"Contracts not covered, or not fully covered, by the Public Sector Directive"

16. Anja Svejgaard Pors
Iværksættelse af kommunikation
- patientfigurer i hospitalets strategiske kommunikation

17. Frans Bévort
Making sense of management with logics
An ethnographic study of accountants who become managers

18. René Kallestrup
The Dynamics of Bank and Sovereign Credit Risk

19. Brett Crawford
Revisiting the Phenomenon of Interests in Organizational Institutionalism
The Case of U.S. Chambers of Commerce

20. Mario Daniele Amore
Essays on Empirical Corporate Finance

21. Arne Stjernholm Madsen
The evolution of innovation strategy
Studied in the context of medical device activities at the pharmaceutical company Novo Nordisk A/S in the period 1980-2008

22. Jacob Holm Hansen
Is Social Integration Necessary for Corporate Branding?
A study of corporate branding strategies at Novo Nordisk

23. Stuart Webber
Corporate Profit Shifting and the Multinational Enterprise

24. Helene Ratner
Promises of Reflexivity
Managing and Researching Inclusive Schools

25. Therese Strand
The Owners and the Power: Insights from Annual General Meetings

26. Robert Gavin Strand
In Praise of Corporate Social Responsibility Bureaucracy

27. Nina Sormunen
Auditor's going-concern reporting
Reporting decision and content of the report

28. John Bang Mathiasen
Learning within a product development working practice:
- an understanding anchored in pragmatism

29. Philip Holst Riis
Understanding Role-Oriented Enterprise Systems: From Vendors to Customers

30. Marie Lisa Dacanay
Social Enterprises and the Poor
Enhancing Social Entrepreneurship and Stakeholder Theory

31. Fumiko Kano Glückstad
Bridging Remote Cultures: Cross-lingual concept mapping based on the information receiver's prior-knowledge

32. Henrik Barslund Fosse
Empirical Essays in International Trade

33. Peter Alexander Albrecht
Foundational hybridity and its reproduction
Security sector reform in Sierra Leone

34. Maja Rosenstock
CSR - hvor svært kan det være? Kulturanalytisk casestudie om udfordringer og dilemmaer med at forankre Coops CSR-strategi

35. Jeanette Rasmussen
Tweens, medier og forbrug
Et studie af 10-12 årige danske børns brug af internettet, opfattelse og forståelse af markedsføring og forbrug

36. Ib Tunby Gulbrandsen
'This page is not intended for a US Audience'
A five-act spectacle on online communication, collaboration & organization.

37. Kasper Aalling Teilmann
Interactive Approaches to Rural Development

38. Mette Mogensen
The Organization(s) of Well-being and Productivity
(Re)assembling work in the Danish Post

39. Søren Friis Møller
From Disinterestedness to Engagement
Towards Relational Leadership In the Cultural Sector

40. Nico Peter Berhausen
Management Control, Innovation and Strategic Objectives – Interactions and Convergence in Product Development Networks

41. Balder Onarheim
Creativity under Constraints
Creativity as Balancing 'Constrainedness'

42. Haoyong Zhou
Essays on Family Firms

43. Elisabeth Naima Mikkelsen
Making sense of organisational conflict
An empirical study of enacted sensemaking in everyday conflict at work

2013

1. Jacob Lyngsie
Entrepreneurship in an Organizational Context

2. Signe Groth-Brodersen
Fra ledelse til selvet
En socialpsykologisk analyse af forholdet imellem selvledelse, ledelse og stress i det moderne arbejdsliv

3. Nis Høyrup Christensen
Shaping Markets: A Neoinstitutional Analysis of the Emerging Organizational Field of Renewable Energy in China

4. Christian Edelvold Berg
As a matter of size
THE IMPORTANCE OF CRITICAL MASS AND THE CONSEQUENCES OF SCARCITY FOR TELEVISION MARKETS

5. Christine D. Isakson
Coworker Influence and Labor Mobility
Essays on Turnover, Entrepreneurship and Location Choice in the Danish Maritime Industry

6. Niels Joseph Jerne Lennon
Accounting Qualities in Practice
Rhizomatic stories of representational faithfulness, decision making and control

7. Shannon O'Donnell
Making Ensemble Possible
How special groups organize for collaborative creativity in conditions of spatial variability and distance

8. Robert W. D. Veitch
Access Decisions in a Partly-Digital World
Comparing Digital Piracy and Legal Modes for Film and Music

9. Marie Mathiesen
Making Strategy Work
An Organizational Ethnography

10. Arisa Shollo
The role of business intelligence in organizational decision-making

11. Mia Kaspersen
The construction of social and environmental reporting

12. Marcus Møller Larsen
The organizational design of offshoring

13. Mette Ohm Rørdam
EU Law on Food Naming
The prohibition against misleading names in an internal market context

14. Hans Peter Rasmussen
GIV EN GED!
Kan giver-idealtyper forklare støtte til velgørenhed og understøtte relationsopbygning?

15. Ruben Schachtenhaufen
Fonetisk reduktion i dansk

16. Peter Koerver Schmidt
Dansk CFC-beskatning
I et internationalt og komparativt perspektiv

17. Morten Froholdt
Strategi i den offentlige sektor
En kortlægning af styringsmæssig kontekst, strategisk tilgang, samt anvendte redskaber og teknologier for udvalgte danske statslige styrelser

18. Annette Camilla Sjørup
Cognitive effort in metaphor translation
An eye-tracking and key-logging study

19. Tamara Stucchi
The Internationalization of Emerging Market Firms:
A Context-Specific Study

20. Thomas Lopdrup-Hjorth
"Let's Go Outside":
The Value of Co-Creation

21. Ana Alačovska
Genre and Autonomy in Cultural Production
The case of travel guidebook production

22. Marius Gudmand-Høyer
Stemningssindssygdommenes historie i det 19. århundrede
Omtydningen af melankolien og manien som bipolære stemningslidelser i dansk sammenhæng under hensyn til dannelsen af det moderne følelseslivs relative autonomi.
En problematiserings- og erfarings-analytisk undersøgelse

23. Lichen Alex Yu
Fabricating an S&OP Process
Circulating References and Matters of Concern

24. Esben Alfort
The Expression of a Need
Understanding search

25. Trine Pallesen
Assembling Markets for Wind Power
An Inquiry into the Making of Market Devices

26. Anders Koed Madsen
Web-Visions
Repurposing digital traces to organize social attention

27. Lærke Højgaard Christiansen
BREWING ORGANIZATIONAL RESPONSES TO INSTITUTIONAL LOGICS

28. Tommy Kjær Lassen
EGENTLIG SELVLEDELSE
En ledelsesfilosofisk afhandling om selvledelsens paradoksale dynamik og eksistentielle engagement

29. Morten Rossing
Local Adaption and Meaning Creation in Performance Appraisal

30. Søren Obed Madsen
Lederen som oversætter
Et oversættelsesteoretisk perspektiv på strategisk arbejde

31. Thomas Høgenhaven
Open Government Communities
Does Design Affect Participation?

32. Kirstine Zinck Pedersen
Failsafe Organizing?
A Pragmatic Stance on Patient Safety

33. Anne Petersen
Hverdagslogikker i psykiatrisk arbejde
En institutionsetnografisk undersøgelse af hverdagen i psykiatriske organisationer

34. Didde Maria Humle
Fortællinger om arbejde

35. Mark Holst-Mikkelsen
Strategieksekvering i praksis
– barrierer og muligheder!

36. Malek Maalouf
Sustaining lean
Strategies for dealing with organizational paradoxes

37. Nicolaj Tofte Brenneche
Systemic Innovation In The Making
The Social Productivity of Cartographic Crisis and Transitions in the Case of SEEIT

38. Morten Gylling
The Structure of Discourse
A Corpus-Based Cross-Linguistic Study

39. Binzhang YANG
Urban Green Spaces for Quality Life
- Case Study: the landscape architecture for people in Copenhagen

40. Michael Friis Pedersen
Finance and Organization:
The Implications for Whole Farm Risk Management

41. Even Fallan
Issues on supply and demand for environmental accounting information

42. Ather Nawaz
Website user experience
A cross-cultural study of the relation between users´ cognitive style, context of use, and information architecture of local websites

43. Karin Beukel
The Determinants for Creating Valuable Inventions

44. Arjan Markus
External Knowledge Sourcing and Firm Innovation
Essays on the Micro-Foundations of Firms' Search for Innovation

2014

1. Solon Moreira
Four Essays on Technology Licensing and Firm Innovation

2. Karin Strzeletz Ivertsen
Partnership Drift in Innovation Processes
A study of the Think City electric car development

3. Kathrine Hoffmann Pii
Responsibility Flows in Patient-centred Prevention

4. Jane Bjørn Vedel
Managing Strategic Research
An empirical analysis of science-industry collaboration in a pharmaceutical company

5. Martin Gylling
Processuel strategi i organisationer
Monografi om dobbeltheden i tænkning af strategi, dels som vidensfelt i organisationsteori, dels som kunstnerisk tilgang til at skabe i erhvervsmæssig innovation

6. Linne Marie Lauesen
Corporate Social Responsibility in the Water Sector: How Material Practices and their Symbolic and Physical Meanings Form a Colonising Logic

7. Maggie Qiuzhu Mei
LEARNING TO INNOVATE: The role of ambidexterity, standard, and decision process

8. Inger Høedt-Rasmussen
Developing Identity for Lawyers Towards Sustainable Lawyering

9. Sebastian Fux
Essays on Return Predictability and Term Structure Modelling

10. Thorbjørn N. M. Lund-Poulsen
Essays on Value Based Management

11. Oana Brindusa Albu
Transparency in Organizing: A Performative Approach

12. Lena Olaison
Entrepreneurship at the limits

13. Hanne Sørum
DRESSED FOR WEB SUCCESS? An Empirical Study of Website Quality in the Public Sector

14. Lasse Folke Henriksen
Knowing networks How experts shape transnational governance

15. Maria Halbinger
Entrepreneurial Individuals Empirical Investigations into Entrepreneurial Activities of Hackers and Makers

16. Robert Spliid
Kapitalfondenes metoder og kompetencer

17. Christiane Stelling
Public-private partnerships & the need, development and management of trusting A processual and embedded exploration

18. Marta Gasparin
Management of design as a translation process

19. Kåre Moberg
Assessing the Impact of Entrepreneurship Education From ABC to PhD

20. Alexander Cole
Distant neighbors Collective learning beyond the cluster

21. Martin Møller Boje Rasmussen
Is Competitiveness a Question of Being Alike? How the United Kingdom, Germany and Denmark Came to Compete through their Knowledge Regimes from 1993 to 2007

22. Anders Ravn Sørensen
Studies in central bank legitimacy, currency and national identity Four cases from Danish monetary history

23. Nina Bellak
Can Language be Managed in International Business? Insights into Language Choice from a Case Study of Danish and Austrian Multinational Corporations (MNCs)

24. Rikke Kristine Nielsen
Global Mindset as Managerial Meta-competence and Organizational Capability: Boundary-crossing Leadership Cooperation in the MNC The Case of 'Group Mindset' in Solar A/S.

25. Rasmus Koss Hartmann
User Innovation inside government Towards a critically performative foundation for inquiry

26. Kristian Gylling Olesen
Flertydig og emergerende ledelse i folkeskolen
Et aktør-netværksteoretisk ledelses-studie af politiske evalueringsreformers betydning for ledelse i den danske folkeskole

27. Troels Riis Larsen
Kampen om Danmarks omdømme 1945-2010
Omdømmearbejde og omdømmepolitik

28. Klaus Majgaard
Jagten på autenticitet i offentlig styring

29. Ming Hua Li
Institutional Transition and Organizational Diversity:
Differentiated internationalization strategies of emerging market state-owned enterprises

30. Sofie Blinkenberg Federspiel
IT, organisation og digitalisering:
Institutionelt arbejde i den kommunale digitaliseringsproces

31. Elvi Weinreich
Hvilke offentlige ledere er der brug for når velfærdstænkningen flytter sig – er Diplomuddannelsens lederprofil svaret?

32. Ellen Mølgaard Korsager
Self-conception and image of context in the growth of the firm – A Penrosian History of Fiberline Composites

33. Else Skjold
The Daily Selection

34. Marie Louise Conradsen
The Cancer Centre That Never Was
The Organisation of Danish Cancer Research 1949-1992

35. Virgilio Failla
Three Essays on the Dynamics of Entrepreneurs in the Labor Market

36. Nicky Nedergaard
Brand-Based Innovation
Relational Perspectives on Brand Logics and Design Innovation Strategies and Implementation

37. Mads Gjedsted Nielsen
Essays in Real Estate Finance

38. Kristin Martina Brandl
Process Perspectives on Service Offshoring

39. Mia Rosa Koss Hartmann
In the gray zone
With police in making space for creativity

40. Karen Ingerslev
Healthcare Innovation under The Microscope
Framing Boundaries of Wicked Problems

41. Tim Neerup Themsen
Risk Management in large Danish public capital investment programmes

2015

1. Jakob Ion Wille
Film som design
Design af levende billeder i film og tv-serier

2. Christiane Mossin
Interzones of Law and Metaphysics
Hierarchies, Logics and Foundations of Social Order seen through the Prism of EU Social Rights

3. Thomas Tøth
TRUSTWORTHINESS: ENABLING GLOBAL COLLABORATION
An Ethnographic Study of Trust, Distance, Control, Culture and Boundary Spanning within Offshore Outsourcing of IT Services

4. Steven Højlund
Evaluation Use in Evaluation Systems – The Case of the European Commission

5. Julia Kirch Kirkegaard
AMBIGUOUS WINDS OF CHANGE – OR FIGHTING AGAINST WINDMILLS IN CHINESE WIND POWER
A CONSTRUCTIVIST INQUIRY INTO CHINA'S PRAGMATICS OF GREEN MARKETISATION MAPPING CONTROVERSIES OVER A POTENTIAL TURN TO QUALITY IN CHINESE WIND POWER

6. Michelle Carol Antero
A Multi-case Analysis of the Development of Enterprise Resource Planning Systems (ERP) Business Practices

Morten Friis-Olivarius
The Associative Nature of Creativity

7. Mathew Abraham
New Cooperativism:
A study of emerging producer organisations in India

8. Stine Hedegaard
Sustainability-Focused Identity: Identity work performed to manage, negotiate and resolve barriers and tensions that arise in the process of constructing or ganizational identity in a sustainability context

9. Cecilie Glerup
Organizing Science in Society – the conduct and justification of resposible research

10. Allan Salling Pedersen
Implementering af ITIL® IT-governance - når best practice konflikter med kulturen Løsning af implementerings-problemer gennem anvendelse af kendte CSF i et aktionsforskningsforløb.

11. Nihat Misir
A Real Options Approach to Determining Power Prices

12. Mamdouh Medhat
MEASURING AND PRICING THE RISK OF CORPORATE FAILURES

13. Rina Hansen
Toward a Digital Strategy for Omnichannel Retailing

14. Eva Pallesen
In the rhythm of welfare creation
A relational processual investigation moving beyond the conceptual horizon of welfare management

15. Gouya Harirchi
In Search of Opportunities: Three Essays on Global Linkages for Innovation

16. Lotte Holck
Embedded Diversity: A critical ethnographic study of the structural tensions of organizing diversity

17. Jose Daniel Balarezo
Learning through Scenario Planning

18. Louise Pram Nielsen
Knowledge dissemination based on terminological ontologies. Using eye tracking to further user interface design.

19. Sofie Dam
PUBLIC-PRIVATE PARTNERSHIPS FOR INNOVATION AND SUSTAINABILITY TRANSFORMATION
An embedded, comparative case study of municipal waste management in England and Denmark

20. Ulrik Hartmyer Christiansen
Follwoing the Content of Reported Risk Across the Organization

21. Guro Refsum Sanden
Language strategies in multinational corporations. A cross-sector study of financial service companies and manufacturing companies.

22. Linn Gevoll
Designing performance management for operational level
- A closer look on the role of design choices in framing coordination and motivation

23. Frederik Larsen
Objects and Social Actions – on Second-hand Valuation Practices

24. Thorhildur Hansdottir Jetzek
The Sustainable Value of Open Government Data
Uncovering the Generative Mechanisms of Open Data through a Mixed Methods Approach

25. Gustav Toppenberg
Innovation-based M&A – Technological-Integration Challenges – The Case of Digital-Technology Companies

26. Mie Plotnikof
Challenges of Collaborative Governance
An Organizational Discourse Study of Public Managers' Struggles with Collaboration across the Daycare Area

27. Christian Garmann Johnsen
Who Are the Post-Bureaucrats? A Philosophical Examination of the Creative Manager, the Authentic Leader and the Entrepreneur

28. Jacob Brogaard-Kay
Constituting Performance Management A field study of a pharmaceutical company

29. Rasmus Ploug Jenle
Engineering Markets for Control: Integrating Wind Power into the Danish Electricity System

30. Morten Lindholst
Complex Business Negotiation: Understanding Preparation and Planning

31. Morten Grynings
TRUST AND TRANSPARENCY FROM AN ALIGNMENT PERSPECTIVE

32. Peter Andreas Norn
Byregimer og styringsevne: Politisk lederskab af store byudviklingsprojekter

33. Milan Miric
Essays on Competition, Innovation and Firm Strategy in Digital Markets

34. Sanne K. Hjordrup
The Value of Talent Management Rethinking practice, problems and possibilities

35. Johanna Sax
Strategic Risk Management – Analyzing Antecedents and Contingencies for Value Creation

36. Pernille Rydén
Strategic Cognition of Social Media

37. Mimmi Sjöklint
The Measurable Me - The Influence of Self-tracking on the User Experience

38. Juan Ignacio Staricco
Towards a Fair Global Economic Regime? A critical assessment of Fair Trade through the examination of the Argentinean wine industry

39. Marie Henriette Madsen
Emerging and temporary connections in Quality work

40. Yangfeng CAO
Toward a Process Framework of Business Model Innovation in the Global Context
Entrepreneurship-Enabled Dynamic Capability of Medium-Sized Multinational Enterprises

41. Carsten Scheibye
Enactment of the Organizational Cost Structure in Value Chain Configuration A Contribution to Strategic Cost Management

2016

1. Signe Sofie Dyrby
Enterprise Social Media at Work

2. Dorte Boesby Dahl
The making of the public parking attendant
Dirt, aesthetics and inclusion in public service work

3. Verena Girschik
Realizing Corporate Responsibility Positioning and Framing in Nascent Institutional Change

4. Anders Ørding Olsen
IN SEARCH OF SOLUTIONS
Inertia, Knowledge Sources and Diversity in Collaborative Problem-solving

5. Pernille Steen Pedersen
Udkast til et nyt copingbegreb
En kvalifikation af ledelsesmuligheder for at forebygge sygefravær ved psykiske problemer.

6. Kerli Kant Hvass
Weaving a Path from Waste to Value: Exploring fashion industry business models and the circular economy

7. Kasper Lindskow
Exploring Digital News Publishing Business Models – a production network approach

8. Mikkel Mouritz Marfelt
The chameleon workforce: Assembling and negotiating the content of a workforce

9. Marianne Bertelsen
Aesthetic encounters
Rethinking autonomy, space & time in today's world of art

10. Louise Hauberg Wilhelmsen
EU PERSPECTIVES ON INTERNATIONAL COMMERCIAL ARBITRATION

11. Abid Hussain
On the Design, Development and Use of the Social Data Analytics Tool (SODATO): Design Propositions, Patterns, and Principles for Big Social Data Analytics

12. Mark Bruun
Essays on Earnings Predictability

13. Tor Bøe-Lillegraven
BUSINESS PARADOXES, BLACK BOXES, AND BIG DATA: BEYOND ORGANIZATIONAL AMBIDEXTERITY

14. Hadis Khonsary-Atighi
ECONOMIC DETERMINANTS OF DOMESTIC INVESTMENT IN AN OIL-BASED ECONOMY: THE CASE OF IRAN (1965-2010)

15. Maj Lervad Grasten
Rule of Law or Rule by Lawyers?
On the Politics of Translation in Global Governance

16. Lene Granzau Juel-Jacobsen
SUPERMARKEDETS MODUS OPERANDI – en hverdagssociologisk undersøgelse af forholdet mellem rum og handlen og understøtte relationsopbygning?

17. Christine Thalsgård Henriques
In search of entrepreneurial learning – Towards a relational perspective on incubating practices?

18. Patrick Bennett
Essays in Education, Crime, and Job Displacement

19. Søren Korsgaard
Payments and Central Bank Policy

20. Marie Kruse Skibsted
Empirical Essays in Economics of Education and Labor

21. Elizabeth Benedict Christensen
The Constantly Contingent Sense of Belonging of the 1.5 Generation Undocumented Youth
An Everyday Perspective

22. Lasse J. Jessen
Essays on Discounting Behavior and Gambling Behavior

23. Kalle Johannes Rose
Når stifterviljen dør…
Et retsøkonomisk bidrag til 200 års juridisk konflikt om ejendomsretten

24. Andreas Søeborg Kirkedal
Danish Stød and Automatic Speech Recognition

25. Ida Lunde Jørgensen
Institutions and Legitimations in Finance for the Arts

26. Olga Rykov Ibsen
An empirical cross-linguistic study of directives: A semiotic approach to the sentence forms chosen by British, Danish and Russian speakers in native and ELF contexts

27. Desi Volker
Understanding Interest Rate Volatility

28. Angeli Elizabeth Weller
Practice at the Boundaries of Business Ethics & Corporate Social Responsibility

29. Ida Danneskiold-Samsøe
Levende læring i kunstneriske organisationer
En undersøgelse af læringsprocesser mellem projekt og organisation på Aarhus Teater

30. Leif Christensen
Quality of information – The role of internal controls and materiality

31. Olga Zarzecka
Tie Content in Professional Networks

32. Henrik Mahncke
De store gaver
- Filantropiens gensidighedsrelationer i teori og praksis

33. Carsten Lund Pedersen
Using the Collective Wisdom of Frontline Employees in Strategic Issue Management

34. Yun Liu
Essays on Market Design

35. Denitsa Hazarbassanova Blagoeva
The Internationalisation of Service Firms

36. Manya Jaura Lind
Capability development in an off-shoring context: How, why and by whom

37. Luis R. Boscán F.
Essays on the Design of Contracts and Markets for Power System Flexibility

38. Andreas Philipp Distel
Capabilities for Strategic Adaptation: Micro-Foundations, Organizational Conditions, and Performance Implications

39. Lavinia Bleoca
The Usefulness of Innovation and Intellectual Capital in Business Performance: The Financial Effects of Knowledge Management vs. Disclosure

40. Henrik Jensen
Economic Organization and Imperfect Managerial Knowledge: A Study of the Role of Managerial Meta-Knowledge in the Management of Distributed Knowledge

41. Stine Mosekjær
The Understanding of English Emotion Words by Chinese and Japanese Speakers of English as a Lingua Franca An Empirical Study

42. Hallur Tor Sigurdarson
The Ministry of Desire - Anxiety and entrepreneurship in a bureaucracy

43. Kätlin Pulk
Making Time While Being in Time
A study of the temporality of organizational processes

44. Valeria Giacomin
Contextualizing the cluster Palm oil in Southeast Asia in global perspective (1880s–1970s)

45. Jeanette Willert
Managers' use of multiple Management Control Systems: The role and interplay of management control systems and company performance

46. Mads Vestergaard Jensen
Financial Frictions: Implications for Early Option Exercise and Realized Volatility

47. Mikael Reimer Jensen
Interbank Markets and Frictions

48. Benjamin Faigen
Essays on Employee Ownership

49. Adela Michea
Enacting Business Models
An Ethnographic Study of an Emerging Business Model Innovation within the Frame of a Manufacturing Company.

50. Iben Sandal Stjerne
Transcending organization in temporary systems
Aesthetics' organizing work and employment in Creative Industries

51. Simon Krogh
Anticipating Organizational Change

52. Sarah Netter
Exploring the Sharing Economy

53. Lene Tolstrup Christensen
State-owned enterprises as institutional market actors in the marketization of public service provision:
A comparative case study of Danish and Swedish passenger rail 1990–2015

54. Kyoung(Kay) Sun Park
Three Essays on Financial Economics

2017

1. Mari Bjerck
Apparel at work. Work uniforms and women in male-dominated manual occupations.

2. Christoph H. Flöthmann
Who Manages Our Supply Chains? Backgrounds, Competencies and Contributions of Human Resources in Supply Chain Management

3. Aleksandra Anna Rzeźnik
Essays in Empirical Asset Pricing

4. Claes Bäckman
Essays on Housing Markets

5. Kirsti Reitan Andersen
Stabilizing Sustainability in the Textile and Fashion Industry

6. Kira Hoffmann
Cost Behavior: An Empirical Analysis of Determinants and Consequences of Asymmetries

7. Tobin Hanspal
Essays in Household Finance

8. Nina Lange
Correlation in Energy Markets

9. Anjum Fayyaz
Donor Interventions and SME Networking in Industrial Clusters in Punjab Province, Pakistan

10. Magnus Paulsen Hansen
Trying the unemployed. Justification and critique, emancipation and coercion towards the 'active society'. A study of contemporary reforms in France and Denmark

11. Sameer Azizi
Corporate Social Responsibility in Afghanistan
– a critical case study of the mobile telecommunications industry

12. Malene Myhre
The internationalization of small and medium-sized enterprises: A qualitative study

13. Thomas Presskorn-Thygesen
The Significance of Normativity – Studies in Post-Kantian Philosophy and Social Theory

14. Federico Clementi
Essays on multinational production and international trade

15. Lara Anne Hale
Experimental Standards in Sustainability Transitions: Insights from the Building Sector

16. Richard Pucci
Accounting for Financial Instruments in an Uncertain World Controversies in IFRS in the Aftermath of the 2008 Financial Crisis

17. Sarah Maria Denta
Kommunale offentlige private partnerskaber Regulering I skyggen af Farumsagen

18. Christian Östlund
Design for e-training

19. Amalie Martinus Hauge
Organizing Valuations – a pragmatic inquiry

20. Tim Holst Celik
Tension-filled Governance? Exploring the Emergence, Consolidation and Reconfiguration of Legitimatory and Fiscal State-crafting

21. Christian Bason
Leading Public Design: How managers engage with design to transform public governance

22. Davide Tomio
Essays on Arbitrage and Market Liquidity

23. Simone Stæhr
Financial Analysts' Forecasts Behavioral Aspects and the Impact of Personal Characteristics

24. Mikkel Godt Gregersen
Management Control, Intrinsic Motivation and Creativity – How Can They Coexist

25. Kristjan Johannes Suse Jespersen
Advancing the Payments for Ecosystem Service Discourse Through Institutional Theory

26. Kristian Bondo Hansen
Crowds and Speculation: A study of crowd phenomena in the U.S. financial markets 1890 to 1940

27. Lars Balslev
Actors and practices – An institutional study on management accounting change in Air Greenland

28. Sven Klingler
Essays on Asset Pricing with Financial Frictions

29. Klement Ahrensbach Rasmussen
Business Model Innovation The Role of Organizational Design

30. Giulio Zichella
Entrepreneurial Cognition. Three essays on entrepreneurial behavior and cognition under risk and uncertainty

31. Richard Ledborg Hansen
En forkærlighed til det eksisterende – mellemlederens oplevelse af forandringsmodstand i organisatoriske forandringer

32. Vilhelm Stefan Holsting
Militært chefvirke: Kritik og retfærdiggørelse mellem politik og profession

33. Thomas Jensen
Shipping Information Pipeline: An information infrastructure to improve international containerized shipping

34. Dzmitry Bartalevich
Do economic theories inform policy? Analysis of the influence of the Chicago School on European Union competition policy

35. Kristian Roed Nielsen
Crowdfunding for Sustainability: A study on the potential of reward-based crowdfunding in supporting sustainable entrepreneurship

36. Emil Husted
There is always an alternative: A study of control and commitment in political organization

37. Anders Ludvig Sevelsted
Interpreting Bonds and Boundaries of Obligation. A genealogy of the emergence and development of Protestant voluntary social work in Denmark as shown through the cases of the Copenhagen Home Mission and the Blue Cross (1850 – 1950)

38. Niklas Kohl
Essays on Stock Issuance

39. Maya Christiane Flensborg Jensen
BOUNDARIES OF PROFESSIONALIZATION AT WORK An ethnography-inspired study of care workers' dilemmas at the margin

40. Andreas Kamstrup
Crowdsourcing and the Architectural Competition as Organisational Technologies

41. Louise Lyngfeldt Gorm Hansen
Triggering Earthquakes in Science, Politics and Chinese Hydropower - A Controversy Study

2018

1. Vishv Priya Kohli
Combatting Falsifi cation and Counterfeiting of Medicinal Products in the E uropean Union – A Legal Analysis

2. Helle Haurum
Customer Engagement Behavior in the context of Continuous Service Relationships

3. Nis Grünberg
The Party -state order: Essays on China's political organization and political economic institutions

4. Jesper Christensen
A Behavioral Theory of Human Capital Integration

5. Poula Marie Helth
Learning in practice

6. Rasmus Vendler Toft-Kehler
Entrepreneurship as a career? An investigation of the relationship between entrepreneurial experience and entrepreneurial outcome

7. Szymon Furtak
Sensing the Future: Designing sensor-based predictive information systems for forecasting spare part demand for diesel engines

8. Mette Brehm Johansen
Organizing patient involvement. An ethnographic study

9. Iwona Sulinska
Complexities of Social Capital in Boards of Directors

10. Cecilie Fanøe Petersen
Award of public contracts as a means to conferring State aid: A legal analysis of the interface between public procurement law and State aid law

11. Ahmad Ahmad Barirani
Three Experimental Studies on Entrepreneurship

12. Carsten Allerslev Olsen
Financial Reporting Enforcement: Impact and Consequences

13. Irene Christensen
New product fumbles – Organizing for the Ramp-up process

14. Jacob Taarup-Esbensen
Managing communities – Mining MNEs' community risk management practices

15. Lester Allan Lasrado
Set-Theoretic approach to maturity models

16. Mia B. Münster
Intention vs. Perception of Designed Atmospheres in Fashion Stores

17. Anne Sluhan
Non-Financial Dimensions of Family Firm Ownership: How Socioemotional Wealth and Familiness Influence Internationalization

18. Henrik Yde Andersen
Essays on Debt and Pensions

19. Fabian Heinrich Müller
Valuation Reversed – When Valuators are Valuated. An Analysis of the Perception of and Reaction to Reviewers in Fine-Dining

20. Martin Jarmatz
Organizing for Pricing

21. Niels Joachim Christfort Gormsen
Essays on Empirical Asset Pricing

22. Diego Zunino
Socio-Cognitive Perspectives in Business Venturing

23. Benjamin Asmussen
Networks and Faces between Copenhagen and Canton, 1730-1840

24. Dalia Bagdziunaite
Brains at Brand Touchpoints A Consumer Neuroscience Study of Information Processing of Brand Advertisements and the Store Environment in Compulsive Buying

25. Erol Kazan
Towards a Disruptive Digital Platform Model

26. Andreas Bang Nielsen
Essays on Foreign Exchange and Credit Risk

27. Anne Krebs
Accountable, Operable Knowledge Toward Value Representations of Individual Knowledge in Accounting

28. Matilde Fogh Kirkegaard
A firm- and demand-side perspective on behavioral strategy for value creation: Insights from the hearing aid industry

29. Agnieszka Nowinska
SHIPS AND RELATION-SHIPS Tie formation in the sector of shipping intermediaries in shipping

30. Stine Evald Bentsen
The Comprehension of English Texts by Native Speakers of English and Japanese, Chinese and Russian Speakers of English as a Lingua Franca. An Empirical Study.

31. Stine Louise Daetz
Essays on Financial Frictions in Lending Markets

32. *Christian Skov Jensen*
Essays on Asset Pricing

33. Anders Kryger
Aligning future employee action and corporate strategy in a resource-scarce environment

34. Maitane Elorriaga-Rubio
The behavioral foundations of strategic decision-making: A contextual perspective

35. Roddy Walker
Leadership Development as Organisational Rehabilitation: Shaping Middle-Managers as Double Agents

36. Jinsun Bae
Producing Garments for Global Markets Corporate social responsibility (CSR) in Myanmar's export garment industry 2011–2015

37. Queralt Prat-i-Pubill
Axiological knowledge in a knowledge driven world. Considerations for organizations.

38. Pia Mølgaard
Essays on Corporate Loans and Credit Risk

39. Marzia Aricò
Service Design as a Transformative Force: Introduction and Adoption in an Organizational Context

40. Christian Dyrlund Wåhlin-Jacobsen
Constructing change initiatives in workplace voice activities Studies from a social interaction perspective

41. Peter Kalum Schou
Institutional Logics in Entrepreneurial Ventures: How Competing Logics arise and shape organizational processes and outcomes during scale-up

42. Per Henriksen
Enterprise Risk Management Rationaler og paradokser i en moderne ledelsesteknologi

43. Maximilian Schellmann
The Politics of Organizing Refugee Camps

44. Jacob Halvas Bjerre
Excluding the Jews: The Aryanization of Danish-German Trade and German Anti-Jewish Policy in Denmark 1937-1943

45. Ida Schrøder
Hybridising accounting and caring: A symmetrical study of how costs and needs are connected in Danish child protection work

46. Katrine Kunst
Electronic Word of Behavior: Transforming digital traces of consumer behaviors into communicative content in product design

47. Viktor Avlonitis
Essays on the role of modularity in management: Towards a unified perspective of modular and integral design

48. Anne Sofie Fischer
Negotiating Spaces of Everyday Politics: -An ethnographic study of organizing for social transformation for women in urban poverty, Delhi, India

2019

1. Shihan Du
   ESSAYS IN EMPIRICAL STUDIES BASED ON ADMINISTRATIVE LABOUR MARKET DATA

2. Mart Laatsit
   Policy learning in innovation policy: A comparative analysis of European Union member states

3. Peter J. Wynne
   Proactively Building Capabilities for the Post-Acquisition Integration of Information Systems

4. Kalina S. Staykova
   Generative Mechanisms for Digital Platform Ecosystem Evolution

5. Ieva Linkeviciute
   Essays on the Demand-Side Management in Electricity Markets

6. Jonatan Echebarria Fernández
   Jurisdiction and Arbitration Agreements in Contracts for the Carriage of Goods by Sea – Limitations on Party Autonomy

7. Louise Thorn Bøttkjær
   Votes for sale. Essays on clientelism in new democracies.

8. Ditte Vilstrup Holm
   The Poetics of Participation: the organizing of participation in contemporary art

9. Philip Rosenbaum
   Essays in Labor Markets – Gender, Fertility and Education

10. Mia Olsen
    Mobile Betalinger - Succesfaktorer og Adfærdsmæssige Konsekvenser

11. Adrián Luis Mérida Gutiérrez
    Entrepreneurial Careers: Determinants, Trajectories, and Outcomes

12. Frederik Regli
    Essays on Crude Oil Tanker Markets

13. Cancan Wang
    Becoming Adaptive through Social Media: Transforming Governance and Organizational Form in Collaborative E-government

14. Lena Lindbjerg Sperling
    Economic and Cultural Development: Empirical Studies of Micro-level Data

15. Xia Zhang
    Obligation, face and facework: An empirical study of the communicative act of cancellation of an obligation by Chinese, Danish and British business professionals in both L1 and ELF contexts

16. Stefan Kirkegaard Sløk-Madsen
    Entrepreneurial Judgment and Commercialization

17. Erin Leitheiser
    The Comparative Dynamics of Private Governance
    The case of the Bangladesh Ready-Made Garment Industry

18. Lone Christensen
    STRATEGIIMPLEMENTERING: STYRINGSBESTRÆBELSER, IDENTITET OG AFFEKT

19. Thomas Kjær Poulsen
    Essays on Asset Pricing with Financial Frictions

20. Maria Lundberg
    Trust and self-trust in leadership identity constructions: A qualitative exploration of narrative ecology in the discursive aftermath of heroic discourse

21. Tina Joanes
Sufficiency for sustainability Determinants and strategies for reducing clothing consumption

22. Benjamin Johannes Flesch
Social Set Visualizer (SoSeVi): Design, Development and Evaluation of a Visual Analytics Tool for Computational Set Analysis of Big Social Data

23. Henriette Sophia Groskopff
Tvede Schleimann
Creating innovation through collaboration – Partnering in the maritime sector

24. Kristian Steensen Nielsen
The Role of Self-Regulation in Environmental Behavior Change

25. Lydia L. Jørgensen
Moving Organizational Atmospheres

26. Theodor Lucian Vladasel
Embracing Heterogeneity: Essays in Entrepreneurship and Human Capital

27. Seidi Suurmets
Contextual Effects in Consumer Research: An Investigation of Consumer Information Processing and Behavior via the Applicati on of Eye-tracking Methodology

28. Marie Sundby Palle Nickelsen
Reformer mellem integritet og innovation: Reform af reformens form i den danske centraladministration fra 1920 til 2019

29. Vibeke Kristine Scheller
The temporal organizing of same-day discharge: A tempography of a Cardiac Day Unit

30. Qian Sun
Adopting Artificial Intelligence in Healthcare in the Digital Age: Perceived Challenges, Frame Incongruence, and Social Power

31. Dorthe Thorning Mejlhede
Artful change agency and organizing for innovation – the case of a Nordic fintech cooperative

32. Benjamin Christoffersen
Corporate Default Models: Empirical Evidence and Methodical Contributions

33. Filipe Antonio Bonito Vieira
Essays on Pensions and Fiscal Sustainability

34. Morten Nicklas Bigler Jensen
Earnings Management in Private Firms: An Empirical Analysis of Determinants and Consequences of Earnings Management in Private Firms

2020

1. Christian Hendriksen
Inside the Blue Box: Explaining industry influence in the International Maritime Organization

2. Vasileios Kosmas
Environmental and social issues in global supply chains: Emission reduction in the maritime transport industry and maritime search and rescue operational response to migration

3. Thorben Peter Simonsen
The spatial organization of psychiatric practice: A situated inquiry into 'healing architecture'

4. Signe Bruskin
The infinite storm: An ethnographic study of organizational change in a bank

5. Rasmus Corlin Christensen
Politics and Professionals: Transnational Struggles to Change International Taxation

6. Robert Lorenz Törmer
The Architectural Enablement of a Digital Platform Strategy

7. Anna Kirkebæk Johansson Gosovic
Ethics as Practice: An ethnographic study of business ethics in a multi-national biopharmaceutical company

8. Frank Meier
Making up leaders in leadership development

9. Kai Basner
Servitization at work: On proliferation and containment

10. Anestis Keremis
Anti-corruption in action: How is anti-corruption practiced in multinational companies?

11. Marie Larsen Ryberg
Governing Interdisciolinarity: Stakes and translations of interdisciplinarity in Danish high school education.

12. Jannick Friis Christensen
Queering organisation(s): Norm-critical orientations to organising and researching diversity

13. Thorsteinn Sigurdur Sveinsson
Essays on Macroeconomic Implications of Demographic Change

14. Catherine Casler
Reconstruction in strategy and organization: For a pragmatic stance

15. Luisa Murphy
Revisiting the standard organization of multi-stakeholder initiatives (MSIs): The case of a meta-MSI in Southeast Asia

16. Friedrich Bergmann
Essays on International Trade

17. Nicholas Haagensen
European Legal Networks in Crisis: The Legal Construction of Economic Policy

18. Charlotte Biil
Samskabelse med en sommerfugle-model: Hybrid ret i forbindelse med et partnerskabsprojekt mellem 100 selvejende daginstitutioner, deres paraplyorganisation, tre kommuner og CBS

19. Andreas Dimmelmeier
The Role of Economic Ideas in Sustainable Finance: From Paradigms to Policy

20. Maibrith Kempka Jensen
Ledelse og autoritet i interaktion - En interaktionsbaseret undersøgelse af autoritet i ledelse i praksis

21. Thomas Burø
LAND OF LIGHT: Assembling the Ecology of Culture in Odsherred 2000-2018

22. Prins Marcus Valiant Lantz
Timely Emotion: The Rhetorical Framing of Strategic Decision Making

23. Thorbjørn Vittenhof Fejerskov
Fra værdi til invitationer - offentlig værdiskabelse gennem affekt, potentialitet og begivenhed

24. Lea Acre Foverskov
Demographic Change and Employment: Path dependencies and institutional logics in the European Commission

25. Anirudh Agrawal
A Doctoral Dissertation

26. Julie Marx
Households in the housing market

27. Hadar Gafni
Alternative Digital Methods of Providing Entrepreneurial Finance

28. Mathilde Hjerrild Carlsen
Ledelse af engagementer: En undersøgelse af samarbejde mellem folkeskoler og virksomheder i Danmark

29. Suen Wang
Essays on the Gendered Origins and Implications of Social Policies in the Developing World

30. Stine Hald Larsen
The Story of the Relative: A Systems-Theoretical Analysis of the Role of the Relative in Danish Eldercare Policy from 1930 to 2020

31. Christian Casper Hofma
Immersive technologies and organizational routines: When head-mounted displays meet organizational routines

32. Jonathan Feddersen
The temporal emergence of social relations: An event-based perspective of organising

33. Nageswaran Vaidyanathan
ENRICHING RETAIL CUSTOMER EXPERIENCE USING AUGMENTED REALITY

2021

1. Vanya Rusinova
The Determinants of Firms' Engagement in Corporate Social Responsibility: Evidence from Natural Experiments

2. Lívia Lopes Barakat
Knowledge management mechanisms at MNCs:
The enhancing effect of absorptive capacity and its effects on performance and innovation

3. Søren Bundgaard Brøgger
Essays on Modern Derivatives Markets

4. Martin Friis Nielsen
Consuming Memory: Towards a conceptualization of social media platforms as organizational technologies of consumption

05. Fei Liu
Emergent Technology Use in Consumer Decision Journeys: A Process-as-Propensity Approach

06. Jakob Rømer Barfod
Ledelse i militære højrisikoteams

07. Elham Shafiei Gol
Creative Crowdwork Arrangements

08. Árni Jóhan Petersen
Collective Imaginary as (Residual) Fantasy: A Case Study of the Faroese Oil Bonanza

09. Søren Bering
"Manufacturing, Forward Integration and Governance Strategy"

10. Lars Oehler
Technological Change and the Decomposition of Innovation:
Choices and Consequences for Latecomer Firm Upgrading: The Case of China's Wind Energy Sector

11. Lise Dahl Arvedsen
Leadership in interaction in a virtual context:
A study of the role of leadership processes in a complex context, and how such processes are accomplished in practice

12. Jacob Emil Jeppesen
Essays on Knowledge networks, scientific impact and new knowledge adoption

13. Kasper Ingeman Beck
Essays on Chinese State-Owned Enterprises:
Reform, Corporate Governance and Subnational Diversity

14. Sönnich Dahl Sönnichsen
Exploring the interface between public demand and private supply for implementation of circular economy principles

15. Benjamin Knox
Essays on Financial Markets and Monetary Policy

16. Anita Eskesen
Essays on Utility Regulation: Evaluating Negotiation-Based Approaches inthe Context of Danish Utility Regulation

17. Agnes Guenther
Essays on Firm Strategy and Human Capital

18. Sophie Marie Cappelen
Walking on Eggshells: The balancing act of temporal work in a setting of culinary change

19. Manar Saleh Alnamlah
About Gender Gaps in Entrepreneurial Finance

20. Kirsten Tangaa Nielsen
Essays on the Value of CEOs and Directors

21. Renée Ridgway
Re:search - the Personalised Subject vs. the Anonymous User

22. Codrina Ana Maria Lauth
IMPACT Industrial Hackathons: Findings from a longitudinal case study on short-term vs long-term IMPACT implementations from industrial hackathons within Grundfos

23. Wolf-Hendrik Uhlbach
Scientist Mobility: Essays on knowledge production and innovation

24. Tomaz Sedej
Blockchain technology and inter-organizational relationships

25. Lasse Bundgaard
Public Private Innovation Partnerships: Creating Public Value & Scaling Up Sustainable City Solutions

26. Dimitra Makri Andersen
Walking through Temporal Walls: Rethinking NGO Organizing for Sustainability through a Temporal Lens on NGO-Business Partnerships

27. Louise Fjord Kjærsgaard
Allocation of the Right to Tax Income from Digital Products and Services: A legal analysis of international tax treaty law

28. Sara Dahlman
Marginal alternativity: Organizing for sustainable investing

29. Henrik Gundelach
Performance determinants: An Investigation of the Relationship between Resources, Experience and Performance in Challenging Business Environments

30. Tom Wraight
Confronting the Developmental State: American Trade Policy in the Neoliberal Era

31. Mathias Fjællegaard Jensen
Essays on Gender and Skills in the Labour Market

32. Daniel Lundgaard
Using Social Media to Discuss Global Challenges: Case Studies of the Climate Change Debate on Twitter

33. Jonas Sveistrup Søgaard
Designs for Accounting Information Systems using Distributed Ledger Technology

34. Sarosh Asad
CEO narcissism and board composition: Implications for firm strategy and performance

35. Johann Ole Willers
Experts and Markets in Cybersecurity On Definitional Power and the Organization of Cyber Risks

TITLER I ATV PH.D.-SERIEN

1992

1. Niels Kornum
Servicesamkørsel – organisation, økonomi og planlægningsmetode

1995

2. Verner Worm
Nordiske virksomheder i Kina
Kulturspecifikke interaktionsrelationer ved nordiske virksomhedsetableringer i Kina

1999

3. Mogens Bjerre
Key Account Management of Complex Strategic Relationships
An Empirical Study of the Fast Moving Consumer Goods Industry

2000

4. Lotte Darsø
Innovation in the Making
Interaction Research with heterogeneous Groups of Knowledge Workers creating new Knowledge and new Leads

2001

5. Peter Hobolt Jensen
Managing Strategic Design Identities
The case of the Lego Developer Network

2002

6. Peter Lohmann
The Deleuzian Other of Organizational Change – Moving Perspectives of the Human

7. Anne Marie Jess Hansen
To lead from a distance: The dynamic interplay between strategy and strategizing – A case study of the strategic management process

2003

8. Lotte Henriksen
Videndeling
– om organisatoriske og ledelsesmæssige udfordringer ved videndeling i praksis

9. Niels Christian Nickelsen
Arrangements of Knowing: Coordinating Procedures Tools and Bodies in Industrial Production – a case study of the collective making of new products

2005

10. Carsten Ørts Hansen
Konstruktion af ledelsesteknologier og effektivitet

TITLER I DBA PH.D.-SERIEN

2007

1. Peter Kastrup-Misir
Endeavoring to Understand Market Orientation – and the concomitant co-mutation of the researched, the re searcher, the research itself and the truth

2009

1. Torkild Leo Thellefsen
Fundamental Signs and Significance effects
A Semeiotic outline of Fundamental Signs, Significance-effects, Knowledge Profiling and their use in Knowledge Organization and Branding

2. Daniel Ronzani
When Bits Learn to Walk Don't Make Them Trip. Technological Innovation and the Role of Regulation by Law in Information Systems Research: the Case of Radio Frequency Identification (RFID)

2010

1. Alexander Carnera
Magten over livet og livet som magt
Studier i den biopolitiske ambivalens