Journal of Risk Research

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rjrr20

Making cyber security more resilient: adding social considerations to technological fixes

Myriam Dunn Cavelty, Christine Eriksen & Benjamin Scharte

To cite this article: Myriam Dunn Cavelty, Christine Eriksen & Benjamin Scharte (2023): Making cyber security more resilient: adding social considerations to technological fixes, Journal of Risk Research, DOI: 10.1080/13669877.2023.2208146

To link to this article: https://doi.org/10.1080/13669877.2023.2208146

Published online: 08 May 2023.

JOURNAL OF RISK RESEARCH
https://doi.org/10.1080/13669877.2023.2208146

Routledge
Taylor & Francis Group

Making cyber security more resilient: adding social considerations to technological fixes

Myriam Dunn Cavelty[a], Christine Eriksen[a] and Benjamin Scharte[b]

[a]Center for Security Studies, ETH Zürich, Zürich, Switzerland; [b]International Center for Ethics in the Sciences and Humanities, University of Tübingen, Tübingen, Germany

ABSTRACT

How can a focus on socio-technical vulnerability and uncertainty make cyber security more resilient? In this article, we provide a conceptual discussion of how to increase cyber resilience. First, we show how cyber security and resilience thinking co-evolved through their connection to critical infrastructures, and how the ensuing dominant technical focus inevitably always falls short due to the diverse societal values that underpin their critical social functions. We argue that a sole focus on aggregate systems neglects the important differences in how cyber threats are experienced and dealt with by individuals. Second, we draw on insights from social resilience and disaster management literature to establish a better link between individuals and cyber systems. We focus on two key aspects of cyber security that highlight its social nature: vulnerability and uncertainty. Instead of thinking of cyber security as a "technical problem + humans," we suggest cyber security should be conceptualized as a "social problem + technology." We conclude by highlighting three ways forward for researchers, policymakers, and practitioners: interdisciplinary research, public debate about a set of normative questions, and the need for an uncertainty discourse in politics and policymaking.

ARTICLE HISTORY
Received 10 June 2022
Accepted 5 April 2023

KEYWORDS
Cyber resilience; vulnerability; (embodied) uncertainty; affluence-vulnerability interface; risk; systemic inequality

1. Introduction

Since the late 1990s, the concept of resilience has become a guiding principle of crisis and disaster management in different policy areas, including the realm of "high politics" or national security (Walker and Cooper 2011). Its surging popularity happens against the backdrop of societies experiencing more complexity and thus more uncertainty in many relevant aspects of life. Referring in its most basic form to the ability of "a system" to prepare for, adapt to, and recover from a severe shock or disruption (Gaillard 2010), resilience thinking appears well suited to take on a solutions-focused role in times marked by multiple uncertainties. It also offers the conceptual means to understand society as a networked system, which exists in a complex relationship with unpredictable and dynamically changing built and natural environments (Dunn Cavelty et al. 2015).

One policy field where resilience thinking has also taken root is cyber security – an area where human and technical systems meet and interact, creating multiple dependencies. The most fundamental threat, as perceived by cyber security policymakers, is the possibility of major,

CONTACT Myriam Dunn Cavelty dunn@sipo.gess.ethz.ch Center for Security Studies, ETH Zürich, Zürich, Switzerland

unexpected, or unpreventable disruptions of vital systems and services – critical infrastructures – with potentially grave, even catastrophic, consequences for society. *Cyber resilience* has therefore emerged as a companion concept to cyber security. It strives to supplement the prevention of cyber incidents with approaches that keep the impact of successful attacks low while also ensuring the provision of important services after the attack occurs.

Although cyber resilience is theoretically compelling, and despite the announcement by many organizations that becoming cyber resilient is one of their goals, it remains a vague and elusive concept that is hard to implement (Dupont 2019). On the one hand, resilience is notoriously difficult to operationalize and measure (Prior and Hagmann 2014). On the other hand, the concept has flaws that need to be addressed before cyber resilience can be expected to achieve its full potential. In this article, we address one of the key criticisms: Because resilience is a concept designed for "systems," it is possible to neglect social factors – most notably the variability in individuals' and communities' coping capacities, which drive adaptive processes and outcomes (Joseph 2013; Cretney 2014; Doorn 2017). Indeed, the predominant technical understandings of cyber security and cyber resilience can lead to an extreme form of "systems thinking" that might obscure human factors. This line of thinking is increasingly problematic the more the harmful effects of cyber insecurities are felt throughout societies. We therefore ask: how can an additional focus on socio-technical vulnerability and uncertainty enhance cyber security and cyber resilience?

We answer this question through a conceptual discussion. First, we show how cyber security and resilience thinking co-evolved through their connection to critical infrastructures. Critical infrastructures are considered critical because they fulfil crucial social functions that are based on societal values; the dominant technical focus therefore inevitably always falls short. Even socio-technical conceptualizations of cyberspace are insufficient on their own: if only aggregate systems are the centre of attention, it is difficult to consider important differences in how cyber threats are experienced and dealt with by individuals. In the second part, we suggest that insights from social resilience and disaster management literature help to provide a better link between individuals and systems. We focus on two key aspects of cyber security that highlight its social nature: vulnerability and uncertainty. Instead of thinking of cyber security as a "technical problem + humans," cyber security should be conceptualized as a "social problem + technology." We conclude by highlighting three ways forward: interdisciplinary research, public debate about a set of normative questions, and the need for an uncertainty discourse in politics and policymaking.

2. "Systems" at the heart of cyber security and resilience thinking

In many ways, the conceptual contexts of cyber security and resilience thinking are interrelated and mutually reinforcing due to their common concern with the threat to, and functionality of, critical infrastructures or critical systems more generally. In this section, we first outline how the changing "risk-scape" after the end of the Cold War brought technical systems to the forefront as so-called "referent objects of security" (Buzan, Waever, and de Wilde 1998). The focus on critical infrastructures was complicit in turning cyber security into the national security issue it is today. Second, we discuss cyberspace as a socio-technical system, which connects humans and machines in complex ways, and needs resilience. These complex connections are the reason why cyber security cannot be reduced to a singular matter of technology: technical systems are embedded into, and derived from, social practices and human choices. Yet, even if we add the "social" to the "technical," a sole focus on "systems" comes with a price that politics cannot ignore: systemic thinking aggregates needs on a societal level, with limited attention paid to the injustices inherent to most systems, lived experiences of inequality, or diverse local mechanisms and capacities for coping.

2.1. Critical infrastructures and social aspects of security politics

How security challenges are viewed has changed during the 21st century from a security paradigm during the Cold War that was informed by the concept of threats – problems that are 'consciously and actively created by one security actor […] for another' (Bailes 2007, 2), to a security politics that deals with a myriad of threats that are often indirect, unintended, or unexpected. Catastrophic events, such as the 9/11 terrorist attacks in 2001, the global financial crisis of 2008, the Fukushima earthquake-tsunami-nuclear disaster in 2011, and the COVID-19 pandemic, have enhanced the political significance (and associated wilful ignorance) of "unknown unknowns", "low probability high impact events," "black swans," "unexampled events," "ruptures," "shocks," or "tipping points," to name a few of the pertinent catchwords (Aven 2013; Elliott 2013).

Given the once "stable" knowledge of known enemies and their intent, the classic goal of security used to be a 'protective or preservative measure […] around a valued subject or object' (Dillon and Lobo-Guerrero 2008, 276). Yet, the higher the uncertainty is about which threats or risks to prioritize, the more difficult it becomes to attain this traditional goal. The destabilization of threat knowledge has therefore raised a new set of core questions: For example, what do we do if there are too many valued subjects and/or objects and not enough resources to protect them all? Or, what if the value is to be found in networked processes or services that make the identification of clearly delineated, protection-worthy objects difficult? Even worse, what if we decide to protect an object against a particular type and intensity of threat and get it wrong? If we consider that security politics are about 'interactions through which values are allocated authoritatively for a society' (Easton 1965, 21), it becomes clear that any type of security is always about assigning legitimate claims to protection to some security objects and political subjects, but not to others.

The difficulty of dealing with these questions explains the reframing of security goals towards a fostering of resilient systems. Under a resilience paradigm decision-makers are partially relieved from having to make difficult decisions about what type of threats to prioritize. Just as important, resilience thinking accepts that disruptions or shocks are inevitable, however good our preventive measures may be. Such a conceptualization of security marks a decisive shift away from the idea that it is possible to predict the type, intensity, place, and time of adverse events (Linkov et al. 2014). Resilience thinking appeals as an approach 'that foregrounds the limits of predictive knowledge and insists on the prevalence of the unexpected' (Walker and Cooper 2011, 147). It fits well with the call for security governance practices that are organized around principles of uncertainty, improvisation, and decentralization (Williams 2008), which are also found in approaches for the regulation of emerging technologies (Farrand, et al. 2020; Farrand and Carrapico 2022).

The key to accepting resilience thinking as a solution to a wide set of problems is to conceptualize society as a social "system" that is supported by, yet again, "systems," but of a technological nature. Technical infrastructures as a security concern first converged with cyber security concerns in the late 1990s when "vital systems" – or critical infrastructures – became a focal point of national security (Collier and Lakoff 2008; Dunn Cavelty 2008). Critical infrastructures refer to physical infrastructures, but also assets, services, and key institutions, such as markets, governmental entities, or even individuals that are crucial to the function and development of society. They are regarded as "critical" – in the sense of being vital, crucial, or essential – because their prolonged unavailability would, likely, result in social instability and major crisis. This way, technical systems and social values become intricately intertwined to the point where they can no longer be separated.

However, the focus on these vital systems centres on *non-human* aspects. In addition, security politics have often been criticized for being attached to abstract concepts, such as the survival of the state, emergency logics, and undemocratic tendencies (Buzan, Waever, and de Wilde 1998; Bourbeau 2018). Security for the "state" is not always security for "the people": in extreme cases,

actions by the state can have negative consequences for parts of its population – directly or indirectly. This brings notions of "national security" into direct opposition to notions of "human security" (Dunn Cavelty 2014). It also biases the debate towards big impact events, such as the destruction of critical infrastructures through cyber-means, when more standard national security centric practices, such as surveillance, arguably have a bigger impact (Deibert 2018). Security for "the system" is therefore not necessarily security "for the human." Can we solve this problem by paying attention to a different type of system that includes social aspects?

2.2. Complex socio-technical systems and resilience

Cyberspace as a technological environment consists of, and depends on, digital technology that is constantly evolving with the diffusion and broad application of new developments that shape cyberspace on an ongoing basis. Yet, a focus just on technology ignores three crucial aspects of cyberspace. First, like all technology, cyberspace is entirely built by humans. This means that the interests and ideas of certain people decisively shape the development and design of technologies. Technologies do not hold meaning on their own or act by themselves; they are part of an assemblage of people, discursive processes, and other material or immaterial things. Furthermore, economic forces shape many aspects of technical innovation as well as the availability of concepts and services to counter certain risks. Second, cyberspace is not an independent system but intertwined with other systems, such as the energy network. In turn, many critical systems depend on information and communication technologies to function, creating co-dependency. All these infrastructures and their respective interdependencies matter because they are crucial for society. Third, cyberspace consists of multiple interactions between the underlying technology and its human users and operators. It is their *interaction* with technology – and with each other by means of technologies – that creates cyberspace in the first place. This is even truer for cyber security (or the lack thereof), which is only relevant with respect to its effects on people and what they value.

These three aspects make cyberspace a *socio-technical system*, where human and societal actions and interests, plus technologies, and the interaction of these different parts, make up the system (Sawyer and Jarrahi 2014). Systemic resilience is the concept applied to complex socio-technical systems that grow more complex over time (Linkov et al. 2014). Systemic resilience theory shows that complex systems require adaptive capacity and flexibility to thrive despite serious adversities (Folke 2006; Holling 1996; Jackson and Ferris 2013). To adapt to unexpected disruptions, systems need to be complex, making complexity a necessary precondition for resilience (Hiermaier and Scharte 2019; Thoma et al. 2016). This is important for the notion of cyber resilience because on their own, computers, smartphones, and servers are not complex adaptive systems but simply complicated technologies. Cyber-attacks can disable them, especially if an attack is carried out in an unforeseen way, and with means that were not envisaged when the attacked asset was designed. To build resilience against such attacks, the system boundaries need to include people who can adapt the system to the attack. These systems need to be *cyber resilient*.

Despite the seemingly "natural" fit between cyber security and resilience thinking, scholarly attention to the concept is sparse across many disciplines. Web of Science and Scopus only list around 500 entries each.[1] In comparison, resilience by itself has over 150,000 entries in each database, and cyber security has between 25,000 and 30,000. Most publications are from key technical disciplines, mainly computer science and electrical engineering, which echoes the overall disciplinary leaning of cyber security research (Dunn Cavelty 2018; Dunn Cavelty and Wenger 2020). Overall, authors consider cyber resilience to be 'the capacity to withstand, recover from and adapt to the external shocks caused by cyber risks' (Dupont 2019, 1). The cyber part of this resilience construct relates to the type of risk and not necessarily only to the systems

that are attacked. A few authors explicitly state that 'cyber resilience should be considered in the context of complex systems that comprise not only physical and information but also cognitive and social domains' (Kott and Linkov 2019, 2), although actual scholarly literature that considers such cyber resilience angles is scarce (cf. Herrington and Aldrich 2013). Some attempts to measure cyber resilience exist (for a recent overview, see Llansó and McNeil 2021), but most only refer to small-scale computer systems with no consideration for scalability.

This under-conceptualization is mirrored in attempts to bring resilience thinking into the realm of politics. Cyber resilience has drawn the attention of different stakeholders over the years, featuring prominently in a variety of cyber security related policies.[2] For example, the EU's key cyber security entity – the European Union Agency for Cybersecurity (ENISA) has championed cyber resilience for several years, choosing a predominantly technical risk management approach (Dunn Cavelty and Smeets 2023; see also Christou 2016; Carrapico and Barrinha 2017). However, even if these policies and legislations claim to enhance resilience, they do not advance its conceptualization, if they engage with it beyond standard definitions at all. That, so we purport, is a big part of the problem: Unless cyber resilience is discussed conceptually and dissected critically, it will remain a buzzword with little substance. In what follows, we draw on thoughts from social resilience and disaster management research that help to engage more deeply and meaningfully with cyber resilience, correcting for its neglect of social factors.

3. The social nature of cyber vulnerability and uncertainty

Key questions any decision-maker needs to ask are: Who should cyber security be for? What kind of cyber security do we want and need (cf. Dwyer et al. 2022)? Unfortunately, these questions cannot be answered based on logic alone since cyber security is a "wicked problem." Wicked problems cannot be solved easily because no single satisfactory solution exists: different stakeholders have different opinions and goals (Dunn Cavelty and Egloff 2019). Wicked problems are 'transboundary in nature, occur at multiple levels across sectors, between institutions, and will impact all actors, both public and private, in complex, interconnected, and often highly politicised ways' (Carr and Lesniewska 2020, 392; see also Carrapico and Farrand 2017). In practice, this also means that cyber *insecurity* does not manifest the same way for everyone. This insight is gaining traction across other academic disciplines with recent research, for example, on the psychological impacts of cyber operations (Shandler, Gross, and Canetti 2023) and on harm brought about by technology-mediated coercive control mechanisms demonstrating the need to 'focus on harms to people (particularly marginalised people) rather than devices or systems' (Slupska 2022, 9). Literature that focuses on digital inequalities also highlight underlying issues that are to blame for keeping global cyberspace insecure (Dodel and Mesch 2018; Calderaro and Craig 2020).

The link between aggregated systems and individuals can be made by focusing on vulnerability and uncertainty, which are key concepts both in cyber security and in social resilience and disaster management research. If we are to take seriously the notion that we are dealing with a socio-technical problem that cannot be broken apart into separate technical and social sub-systems, then we must develop an understanding of the socio-technical dimensions of vulnerability and uncertainty that consider social diversity. Building on recent conceptual work, we offer two extensions: (a) understanding cyber resilience through an affluence-vulnerability lens, and (b) seeing embodied uncertainty in cyber systems.

3.1. Cyber resilience through an affluence-vulnerability lens

The perception that cyberspace is creating and perpetuating insecurity, with potentially grave consequences, is shaped by cyber incidents. A cyber incident can be defined as a disruption

that challenges the normal operation of digital technologies. Wilful disruption of the digital domain is possible due to so-called vulnerabilities: weaknesses 'in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source' (Committee on National Security Systems 2010, 81). There are many vulnerabilities in the information infrastructure, which was not built with security in mind. Furthermore, there are significant market-driven obstacles to IT-security, rooted in the incentive structures of hardware and software production (Anderson and Moore 2006), and strategic exploitation of vulnerabilities *via* cyberspace for political gain (Buchanan 2020; Maschmeyer 2022).

Removing all vulnerabilities from the information infrastructure and preventing new ones is impossible. Hence, cyber security is built on the availability of technical security measures, which can neutralize vulnerabilities or help spot threat actors that have exploited a vulnerability. The global cyber security market has witnessed robust growth over the last few years with revenue increasing from US$83 billion in 2016 to US$173.50 billion in 2023, with an annual growth rate of over 10% (Statistica 2023). In 2022, one of the market leaders for threat intelligence and cyber security solutions reported that the median "dwell time," the time an attacker can stay in a computer system without being discovered, was down to 21 days, a massive 184 days less than in 2014 (Mandiant 2022). A closer look at the data shows that there are large differences when it comes to regions, which correlated with the amount of money spent on advanced (expensive) cyber defence solutions. Given these numbers, should we assume a direct positive link between economic prowess or affluence and coping capacity? After all, the richer an organisation or country is, the better they can arguably afford to buy defence solutions. On an average aggregated level, this equation is true. Yet, it masks the huge differences in threat exposure by company size, sector, and region.

From a social vulnerability point of view, the assumption that an unlimited supply of money or material affluence will necessarily result in greater security and increased resilience is flawed (Eriksen et al. 2020). Affluence is typically understood as the ability of an individual or community to achieve a financial status that enables a corresponding level of access to material resources and assets (Adger 2006; Smit and Wandel 2006). According to Adger and Kelly (1999, 256), 'the extent to which individuals, groups or communities are "entitled" to make use of resources determines the ability of that particular population to cope with and adapt to stress.' This view typically assumes that if we manage to increase the material wealth of an individual, organisation, or nation, an increase in resilience will necessarily follow due to the availability of, for example, advanced infrastructure, technology, and social services. This is clearly often the case, as these material resources can (at least theoretically) be easily converted into risk-mitigating adaptations, such as cyber defence mechanisms.

However, as Eriksen et al. (2020) argue, if we understand affluence to have only a mitigating influence, we are likely to miss circumstances where vulnerabilities and forms of social risk exist as a consequence of policies aimed at increasing economic growth and/or technological development. In some cases, increasing material affluence and access to resources may exacerbate pre-existing, and produce new, risks and vulnerabilities (Eadie and Su 2018). Well-developed infrastructure, which we associate with technological advancement, often leads to segregation and inequality (Graham and Marvin 2001; Thomalla et al. 2018), such as the everyday reliance on electronic payment methods or digital prowess that often exclude older generations, or urban infrastructure technologies that splinter neighbourhood cohesion. Even when the knowledge to mitigate cyber vulnerabilities exist, many people, organisations, and countries do not have the technological, economic, and/or political means to act on or implement cyber security measures that match technological advancements. A problem of growing inequity is evident in all countries – high, medium and low income, especially in the context of rapid urban development processes that are often dependent on digital technologies.

The affluence-vulnerability interface (AVI) – a concept developed to understand disaster resilience (Eriksen and Simon 2017), provides an analytical lens that can illuminate how digital

technologies are simultaneously embodiments of societal knowledge, sites of power relations, and behaviour shaping (Behren 2013). Understanding cyber resilience through the AVI lens provides opportunities to examine how cyber security affects social inequalities linked to access and distribution, which are distorted by affluence. Evidence from disaster resilience research demonstrates that risks and vulnerabilities factors are not improving proportional to levels of economic and technological development (Eriksen and Simon 2017; Aldrich 2012; Collins 2010). For example, participation patterns in digital mapping exercises for disaster preparedness, response, and recovery rarely reflect the true needs or makeup of culturally and socioeconomically diverse societies (Haworth, Eriksen, and McKinnon 2019). Instead, they reflect where power lies – usually with dominant groups with digital access and no fear of discrimination (Haworth et al. 2018).

Disaster risk reduction policies have evolved in the past decades from a sole emphasis on the mechanical and structural aspects of hazard mitigation to the guiding principle of disaster resilience. Here, resilience as a concept puts a strong emphasis on distributed capacities for disaster prevention, preparedness, and recovery, and explicitly recognizes the need for social vulnerability analysis (Wisner et al. 2004; Tierney 2014; UN 2015; UNDRR 2015). This is important in the context of cyber resilience. It explains why assessments focusing only on financial wealth and material coping capacity are insufficient to explain cyber (in)security, as they do not acknowledge systemic injustices caused by, for example, political marginalization and distrust, or alternative forms of resources.

Rather, resources influencing the resilience of organisations and their staff can be material (e.g. finances, assets, technologies), psychosocial (e.g. emotions, social networks, social cohesion, beliefs, trust, local knowledge) and institutional (e.g. political power, governance functionality) (Eriksen et al. 2020; Sword-Daniels et al. 2018). Material and psychosocial resources may interact to influence institutional resources and social vulnerabilities, for example, when tools, know-how, and social cohesion rally staff to work together under pressure to solve urgent problems with potentially catastrophic social outcomes. The continuing care of critically ill patients in hospitals during power outages or cyber-attacks on computer-reliant devices is a case in point. Meanwhile, the existence, capacity, and accountability of government institutions (local to international) have a strong influence on coping capacity and trust. For example, as countries closed their borders and disinformation about the seriousness of the SARS-CoV-2 virus plagued online media in early 2020, the European Union Civil Protection Mechanism relied on digital communication, air-travel infrastructures, trust, and existing international collaborators to facilitate the repatriation of stranded citizens.

In order to plan for and respond to future cyber threats, knowledge about material coping capacity must be complemented with an understanding of psychosocial coping capacity – that is, other forms of capital, such as different forms of social capital (Aldrich 2012). Psychosocial attributes are often underemphasized in the drive for techno-economic advancement that aids risk management, yet they play an important role in building and upholding cyber resilience. Using qualitative research methods to understand such attributes provides substantial evidence, which can contextualise and add depth to the trends and indicators that emerge from the quantitative data used in traditional risk analysis (Eriksen et al. 2020). From archival analysis, in-depth interviews, focus groups, participatory mapping, and participatory observation, to scenario-based exercises, qualitative research methods can elicit insights on material, psychosocial, and institutional resources that underpin coping capacity at a range of scales.

The key formative psychosocial conditions in the context of cyber resilience are arguably trust and social cohesion (cf. Lewis and Weigert 1985). Trust exists independently of material affluence but has the capacity to undermine even the most powerful of techno-economic systems. On the one hand, a lack of trust by governments or powerful entities in others (e.g. activists, organisations, or foreign powers), increases the perceived need for greater cyber security. On the other hand, a lack of trust by activists, organisations, foreign powers, etc. in a

particular government or powerful entity can result in individuals infiltrating (hacking into) cyber security systems, which perpetuates the need by those in power to acquire more cyber security. Distrust thus becomes a positive feedback loop that can heighten or undermine cyber resilience. Social cohesion, particularly characteristics like "sense of community" and "collective problem solving," can act as psychosocial resources that support the development of material resources, mitigative behaviour, and knowledge coproduction.

3.2. Understanding embodied uncertainty in cyber systems

Given the known and unknown number of vulnerabilities at any given time, vulnerability is not only the crux of digital insecurity, it is also indirectly responsible for the pervasive uncertainty that is endemic in cyber security. One part of this uncertainty is *epistemic*. It relates to absent and/or conflicting knowledge, which hampers the assessment of probabilities and consequences, the two elements needed for classical risk analysis (Renn, Klinke, and van Asselt 2011). Another part of this uncertainty is *ontologically intrinsic* because it is linked to human actions and reactions. This type of uncertainty is considered "unknowable knowledge" and is irreducible because humans 'are part of the problem, system and potential solutions' (Sword-Daniels et al. 2018, 291). Both types of uncertainty shape the cyber security discourse, whereby the second type often is a cause of the first type.

Traditionally, IT-security is grounded in risk management practices that aim to protect the confidentiality, integrity, and availability of data and information (the so-called CIA-Triad). The key risk factors are the threats to the system as well as the vulnerabilities that can be exploited by attacking the CIA-Triad. The standard risk formula in IT-security is 'a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence' (Brooks et al. 2017, 21). However, traditional quantitative risk analysis and risk management approaches are inadequate for upholding safety and security against the unexpected, unknown, large-scale disruptions in complex socio-technical systems. The main limitation of these measures is their reliance on principles informed by reductionism: that is, specific scenarios with defined probabilities and exact assessments of possible damages to determine specific mitigation measures (Linkov et al. 2014).

Furthermore, risk management approaches cannot be applied when data is not available, is incomplete, or is just "not to be known." Indeed, for cyber risks, both the likelihood of events and the value of its consequences are hard to measure, as the cyber risk landscape changes dynamically with different threat actors innovating rapidly. Put differently, 'the current lack of quantification and consistent measurement of cyber risk is a direct result of in-sufficient quality data points and data sharing' (Ruan 2017, 78). Indicative of the lack of quality risk data are the struggles of the insurance industry to develop the cyber security market segment (World Economic Forum 2015). The problem is partly rooted in data collection, where the absence of a common point of reference (or a common understanding of risk categories) has created inconsistent measurements of cyber risk over time. Because human actors use the information infrastructure in innovative ways, calculation of probabilities of events based on previous experience is tricky if not impossible. Non-linearity and "objective unknowability" limit the usefulness of classical, probabilistic risk analysis (Chandler 2014, 49). Therefore, the 'current lack of quantification' that Ruan (2017, 78) talks about, might very well turn into a permanent one, challenging traditional actuarial models in insurance (Amin 2019; Lobo-Guerrero 2011).

Another issue is the partial invisibility of cyber risk exposure. Companies prefer to remain silent on cyber incidents and associated losses if they can, while forensic investigators are forbidden from sharing details of incidents (Ruan 2017, 78).[3] Furthermore, publicly available knowledge about threats is biased. A recent study on commercial threat intelligence reports

shows that threats to civil society organisations are grossly underrepresented, due to the commercial incentives to threat intelligence companies to mainly focus on threats that interest affluent governments and companies (Maschmeyer, Deibert, and Lindsay 2021). Also, insufficient risk data is related to great difficulties in pricing different damage categories. Foremost are the intangibles, such as ideas that have not yet been monetized, or secondary effects like reputational damage that arise from the mishandling of cyber incidents. Different actors also perceive values, loss, and gain differently, and the consequences may be distributed unevenly across time and space (Eiser et al. 2012).

Because uncertainties arise from the very nature of cyber threats, which are ever changing due to technological development, human innovation, and how they interact, it is helpful to better understand the pervasiveness of uncertainty in cyber systems. To this end, we use the concept of "embodied uncertainty" to unpack how everyday uncertainties and risks are embodied, but not currently accounted for, in cyber systems. This broadens the original concept, which was coined by social scientists to explore and accept how uncertainty and risk are prevailing conditions of everyday life (Sword-Daniels et al. 2018).

Embodied uncertainty is arguably the crux of cyber resilience, as individuals, organisations, institutions, and societies constantly deal with and embody risk, for example, in the form of the multiple layers of uncertainty associated with cyber threats. The exact time, location, intensity, and frequency of potential cyber-attacks are constant unknowns, which make estimations of likelihood, vulnerability, severity, and resource needs uncertain – or even, as argued above, impossible. Such uncertainty is not universally observed, known, and measured, but is subjectively interpreted by those who live at-risk, and those who attempt to manage it. It leads to individual and collective interpretations of risks and associated decisions regarding if and how to prepare and respond.

The uncertainty discourse in risk studies focuses mostly on scientific uncertainty as it relates to absent or conflicting knowledge, and how that uncertainty contributes to difficulties in assessing probabilities and consequences. As such, scientific enquiry is considered to be a pathway to reducing epistemic uncertainty over time. However, as the work of Sword-Daniels et al. (2018) shows in the context of living with complexity and environmental change, uncertainty is not simply an absence of knowledge. It may prevail where substantial information is available, particularly when new knowledge reveals new uncertainties, and information is interpreted or characterised in very different ways.

Because humans are both the creators of information technologies, and particularly vulnerable to attacks on its functionality, accepting uncertainty is not just a matter of understanding the supply-demand logic of cyber security. Rather, it is about understanding processes that are non-linear, indeterminate, and complex. It is through these processes that uncertainty is experienced, internalised, and becomes embedded within decision-making and social norms over time. The resulting range of beliefs and behaviours are diverse, ranging from pro-active mitigation to denial, wilful ignorance to fatalism, individualism to social cohesion, defence to attack strategies, and so on depending on the psychosocial drivers.

Embodying uncertainty is common to all – from individuals, organisations, and institutions to societies. Yet, it is differentially internalised. In situations with high uncertainty, internalised characteristics influence how multiple dimensions are individually or collectively experienced, interpreted, and acted upon depending on material, psychosocial, and organisational resources. By analysing its embodiment through in-depth evidence best obtained through the qualitative research methods outlined above, the broadened concept of uncertainty presented by Sword-Daniels et al. (2018) promotes a shift in thinking towards accepting (rather than reducing) uncertainty. By focusing on the lived experience of cyber threats and cyber security within uncertain contexts, we accept uncertainty as a persistent condition of daily life in many forms, scales, and levels of conscious and unconscious relationships and interdependencies. It enables us to consider potentially catastrophic outcomes and what our individual, collective, national,

or international responses might be. Such consideration holds valuable lessons for thinking about the resilience of digital infrastructure.

4. Conclusion

Cyberspace as a complex socio-technical system is in need of cyber resilience as an additional concept to enhance cyber security. The very complexity of cyberspace allows for implementing suitable, technological principles to enhance resilience. These can help create adaptive capacities needed to cope with unexpected and surprising disruptions. While the current architecture of the internet is a fitting starting point for further discussion on how to build cyber resilience, it is equally important to think cyber security beyond the technical elements of cyberspace and bring it "down" – conceptually and operationally – to the people. This will enable engagement with deliberative, fair, and transparent negotiating processes about the ways we want to protect our vital systems and critical infrastructures – including cyberspace.

Our exploration of how to make cyber security more resilient leads us to three concluding points that will assist a greater appreciation of – and ideally also present solutions to – how socially diverse people, organisations, and institutions experience exposure, vulnerability, and adaptive capacity differently due to historical and structural inequalities. The first point concerns academia, the second involves normative questions for society at large, and the third relates to policymaking.

First, this article is a call for more interdisciplinary research. Though this is easier said than done, taking socio-technical system-interaction seriously is non-negotiable. The dynamic and complex interaction between different sub-systems makes the management of cyber threats difficult. For example, insecurity in information infrastructure emerges from economic incentive structures. Opportunities for exploiting digital technologies vary due to technological possibilities and political or economic cost-benefit calculations. New laws and regulations influence technological innovation and vice versa. Decades of trying to make cyberspace more secure by fixing partial, isolated aspects of dynamic systems have yielded suboptimal results or have, at times, created additional insecurities and uncertainties. Inspiring examples from other domains are helpful for fostering an interdisciplinary endeavour for cyber resilience. Here, social-ecological resilience research offers valuable insights. With its roots in systems ecology, scholars quickly came to realize that to fully understand their research subjects, they needed to incorporate findings from other disciplines. This led to the formation of the Resilience Alliance,[4] an interdisciplinary network of scholars formed to explore the dynamics, resilience, and coping capacity of social-ecological systems. Taking cyber resilience seriously could mean a similar call for an interdisciplinary approach.

Second, a public debate is needed about the normative desirability of resilience or cyber resilience. Important questions include: Under which conditions is it good to build resilience? What should the systems that we want to make resilient look like? Who is responsible for resilience in cyberspace, and who can provide it? How can we assign responsibilities without overwhelming those deemed to be responsible? How can we make citizens literate in cyber resilience? Society should engage in a transparent negotiation process to facilitate how technologies are used. Whatever the result of public negotiations, a deliberative, fair, and transparent process is a critical precondition for building resilience, as it facilitates the formative psychosocial conditions of trust and social cohesion.

Third, a political discourse of uncertainty is needed to generate more legitimacy for the possibility of failure. In a world of complex systems, there can be no security in an absolute sense. In fact, the opposite is true. Incidents are deemed to happen because they simply cannot be avoided. Public policy must more actively recognize and communicate that some policy

measure could be successful but that others might result in failure due to unintended consequences brought on by the interactions within and between complex systems. "Freeing up" policy design processes to plan for success as well as failure can potentially render unintended consequences that are beneficial to complex systems management (Little 2012, 14). While we must expect disturbances in vital systems in the future, we should not accept outright disasters. Some of the disturbances may well turn into crises. As resilience thinking shows us, crisis can be turning points rather than an end state, where the aversion of disaster is possible and opportunities arise to right the wrong of historical and structural injustices. If societies become more fault tolerant psychologically and more resilient overall, the likelihood for catastrophe in general, and catastrophic system failure in particular, can be substantially reduced.

Notes

1. Databases checked on 20.02.2023 for the period 2009-2022. Search terms: "(all fields) cyber-resilien* OR cyberresilien*".
2. Important policies include the European Union's NIS Directive (2022/2555), the EU Cybersecurity Act (Regulation 2019/881), the Critical Entities Resilience Directive (CER) (2022/2557), and the proposed EU Cyber Resilience Act.
3. The EU has implemented legislation, most prominently through the GDPR, that targets this behaviour, seeking disclosure in exchange for immunity from liability, identification of best practices and information-sharing as ways of securing resilience in targeted sectors (we thank one of the reviewers for highlighting this point).
4. http://www.resalliance.org/about

Disclosure statement

This research received no external funding. The authors declare no conflict of interest.

References

Adger, N. W. 2006. "Vulnerability." *Global Environmental Change* 16 (3): 268–281. doi:10.1016/j.gloenvcha.2006.02.006.

Adger, N. W., and M. P. Kelly. 1999. "Social Vulnerability to Climate Change and the Architecture of Entitlements." *Mitigation and Adaptation Strategies for Global Change* 4 (3/4): 253–266. doi:10.1023/A:1009601904210.

Aldrich, D. 2012. *Building Resilience: Social Capital in Post-Disaster Recovery*. Chicago: University of Chicago Press.

Amin, Z. 2019. "A Practical Road Map for Assessing Cyber Risk." *Journal of Risk Research* 22 (1): 32–43. doi:10.1080/13669877.2017.1351467.

Anderson, R., and T. Moore. 2006. "The Economics of Information Security." *Science (New York, N.Y.)* 314 (5799): 610–613. doi:10.1126/science.1130992.

Aven, T. 2013. "On the Meaning of a Black Swan in a Risk Context." *Safety Science* 57: 44–51. doi:10.1016/j.ssci.2013.01.016.

Bailes, A. J. K. 2007. "Introduction: A World of Risk." In *SIPRI Yearbook 2007: Armaments, Disarmament and International Security*, 1–20. Stockholm: SIPRI.

Behren, M. C. 2013. "Foucault and Technology." *History and Technology* 29: 54–104.

Bourbeau, P. 2018. *On Resilience: Genealogy, Logics, and World Politics*. Cambridge: Cambridge University Press.

Brooks, S., M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeu. 2017. "An Introduction to Privacy Engineering and Risk Management in Federal Systems." NISTIR 8062. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

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

Buzan, B., O. Waever, and J. de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

Calderaro, A., and A. J. S. Craig. 2020. "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building." *Third World Quarterly* 41 (6): 917–938. doi:10.1080/01436597.2020.1729729.

Carr, M., and F. Lesniewska. 2020. "Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance." *International Relations* 34 (3): 391–412. doi:10.1177/0047117820948247.

Carrapico, H., and B. Farrand. 2017. "Dialogue, Partnership and Empowerment for Network and Information Security': The Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers." *Crime, Law and Social Change* 67 (3): 245–263. doi:10.1007/s10611-016-9652-4.

Carrapico, H., and A. Barrinha. 2017. "The EU as a Coherent Actor in the Field of Cyber Security." *JCMS: Journal of Common Market Studies* 55 (6): 1254–1272. doi:10.1111/jcms.12575.

Chandler, D. 2014. "Beyond Neoliberalism: Resilience, the New Art of Governing Complexity." *Resilience* 2 (1): 47–63. doi:10.1080/21693293.2013.878544.

Christou, G. 2016. "Cybersecurity in the European Union Resilience and Adaptability in Governance Policy." London Palgrave Macmillan.

Collier, S. J., and A. Lakoff. 2008. "The Vulnerability of Vital Systems: How 'Critical Infrastructure' Became a Security Problem." In *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation*, eds. M. Dunn and S. Kristensen. London: Routledge.

Collins, T. W. 2010. "Marginalization, Facilitation, and the Production of Unequal Risk: The 2006 Paso Del Norte Floods." *Antipode* 42 (2): 258–288. doi:10.1111/j.1467-8330.2009.00755.x.

Committee on National Security Systems. 2010. National Information Assurance (IA) Glossary, CNSS Instruction No. 4009. https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

Cretney, R. 2014. "Resilience for Whom? Emerging Critical Geographies of Socio-Ecological Resilience." *Geography Compass* 8 (9): 627–640. doi:10.1111/gec3.12154.

Deibert, R. 2018. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32 (4): 411–424. doi:10.1017/S0892679418000618.

Dillon, M., and L. Lobo-Guerrero. 2008. "Biopolitics of Security in the 21st Century: An Introduction." *Review of International Studies* 34 (2): 265–292. doi:10.1017/S0260210508008024.

Dodel, M., and G. Mesch. 2018. "Inequality in Digital Skills and the Adoption of Online Safety Behaviors." *Information, Communication & Society* 21 (5): 712–728. doi:10.1080/1369118X.2018.1428652.

Doorn, N. 2017. "Resilience Indicators: Opportunities for Including Distributive Justice Concerns in Disaster Management." *Journal of Risk Research* 20 (6): 711–731. doi:10.1080/13669877.2015.1100662.

Dunn Cavelty, M., M. Kaufmann, and K. Søby Kristensen. 2015. "Resilience and (in)Security: Practices, Subjects, Temporalities." *Security Dialogue* 46 (1): 3–14. doi:10.1177/0967010614559637.

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

Dunn Cavelty, M. 2014. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics* 20 (3): 701–715. doi:10.1007/s11948-014-9551-y.

Dunn Cavelty, M. 2018. "Cybersecurity Research Meets Science and Technology Studies." *Politics and Governance* 6 (2): 22–30. doi:10.17645/pag.v6i2.1385.

Dunn Cavelty, M., and M. Smeets. 2023. "Regulatory Cybersecurity Governance in the Making: The Formation of ENISA and Its Struggle for Epistemic Authority." *Journal of European Public Policy* 1–23. doi:10.1080/13501763.2023.2173274.

Dunn Cavelty, M., and F. J. Egloff. 2019. "The Politics of Cybersecurity: Balancing Different Roles of the State." *St Antony's International Review* 15: 37–57.

Dunn Cavelty, M., and A. Wenger. 2020. "Cybersecurity Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41 (1): 5–32. doi:10.1080/13523260.2019.1678855.

Dupont, B. 2019. "The Cyber-Resilience of Financial Institutions: Significance and Applicability." *Journal of Cybersecurity* 5 (1): tyz013. doi:10.1093/cybsec/tyz013.

Dwyer, A. C., C. Stevens, I. Pijnenburg Muller, M. Dunn Cavelty, L. Coles-Kemp, and P. Thornton. 2022. "What Can a Critical Cybersecurity Do?." *International Political Sociology* 16(3): olac013. doi:10.1093/ips/olac013.

Eadie, P., and Y. Su. 2018. "Post-Disaster Social Capital: Trust, Equity, Bayanihan and Typhoon Yolanda." *Disaster Prevention and Management: An International Journal* 27 (3): 334–345. doi:10.1108/DPM-02-2018-0060.

Easton, D. 1965. *A Systems Analysis of Political Life*. New York: John Wiley.

Eiser, R. J., A. Bostrom, I. Burton, D. M. Johnston, J. McClure, D. Paton, J. van der Pligt, and M. P. White. 2012. "Risk Interpretation and Action: A Conceptual Framework for Responses to Natural Hazards." *International Journal of Disaster Risk Reduction* 1: 5–16. doi:10.1016/j.ijdrr.2012.05.002.

Elliott, D. 2013. *Fukushima: Impacts and Implications*. London: Palgrave Macmillan.

Eriksen, C., and G. Simon. 2017. "The Affluence-Vulnerability Interface: Intersecting Scales of Risk, Privilege and Disaster." *Environment and Planning A: Economy and Space* 49 (2): 293–313. doi:10.1177/0308518X16669511.

Eriksen, C., G. Simon, F. Roth, S. J. Lakhina, B. Wisner, C. Adler, F. Thomalla, et al. 2020. "Rethinking the Interplay Between Affluence and Vulnerability to Aid Climate Change Adaptive Capacity." *Climatic Change* 162 (1): 25–39. doi:10.1007/s10584-020-02819-x.

Farrand, B, et al. 2020. "Managing Security Uncertainty with Emerging Technologies: The Example of the Governance of Neuroprosthetic Research." In *Emerging Security Technologies and EU Governance: Actors, Practices and Processes*, ed. Calcara. Abingdon, Oxon: Routledge, 192–205.

Farrand, B., and H. Carrapico. 2022. "Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity." *European Security* 31 (3): 435–453. doi:10.1080/09662839.2022.2102896.

Folke, C. 2006. "Resilience: The Emergence of a Perspective for Social-Ecological Systems Analyses." *Global Environmental Change* 16 (3): 253–267. doi:10.1016/j.gloenvcha.2006.04.002.

Gaillard, J.-C. 2010. "Vulnerability, Capacity and Resilience: Perspectives for Climate and Development Policy." *Journal of International Development* 22 (2): 218–232. doi:10.1002/jid.1675.

Graham, S., and S. Marvin. 2001. *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*. New York: Routledge.

Haworth, B. T., E. Bruce, J. Whittaker, and R. Read. 2018. "The Good, the Bad, and the Uncertain: Contributions of Volunteered Geographic Information to Community Disaster Resilience." *Frontiers in Earth Science* 6:183. doi:10.3389/feart.2018.00183.

Haworth, B., C. Eriksen, and S. McKinnon. 2019. "Online Tools can Help People in Disasters, but do they Represent Everyone?" *The Conversation* 30 May 2019. https://theconversation.com/online-tools-can-help-people-in-disasters-but-do-they-represent-everyone-116810

Herrington, L., and R. Aldrich. 2013. "The Future of Cyber-Resilience in an Age of Global Complexity." *Politics* 33 (4): 299–310. doi:10.1111/1467-9256.12035.

Hiermaier, S., and B. Scharte. 2019. "Fault-Tolerant Systems." In *Digital Transformation*, ed. R. Neugebauer, 285–300. Berlin: Springer.

Holling, C. S. 1996. "Engineering Resilience Versus Ecological Resilience." In *Engineering within Ecological Constraints*, ed. P. E. Schulze, 31–43. Washington DC: National Academy Press.

Jackson, S., and T. L. J. Ferris. 2013. "Resilience Principles for Engineered Systems." *Systems Engineering* 16 (2): 152–164. doi:10.1002/sys.21228.

Joseph, J. 2013. "Resilience as Embedded Neoliberalism: A Governmentality Approach." *Resilience* 1 (1): 38–52. doi:10.1080/21693293.2013.765741.

Kott, A., and I. Linkov. 2019. *Cyber Resilience of Systems and Networks*. Cham: Springer.

Lewis, J. D., and A. J. Weigert. 1985. "Trust as a Social Reality." *Social Forces* 63 (4): 967–985. doi:10.2307/2578601.

Linkov, I., T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. H. Lambert, et al. 2014. "Changing the Resilience Paradigm." *Nature Climate Change* 4 (6): 407–409. doi:10.1038/nclimate2227.

Little, A. 2012. "Political Action, Error and Failure: The Epistemological Limits of Complexity." *Political Studies* 60 (1): 3–19. doi:10.1111/j.1467-9248.2011.00901.x.

Llansó, T., and M. McNeil. 2021. "Towards an Organizationally-Relevant Quantification of Cyber Resilience." Proceedings of the 54th Hawaii International Conference on System Sciences. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/eae8138b-0a79-4753-90ee-f3accfb98ea3/content. doi:10.24251/HICSS.2021.849.

Lobo-Guerrero, L. 2011. *Insuring Security: Biopolitics, Security and Risk*. London: Routledge.

Mandiant. 2022. M-Trends report. https://www.mandiant.com/m-trends

Maschmeyer, L. 2022. "A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict." *Journal of Strategic Studies*. doi:10.1080/01402390.2022.2104253.

Maschmeyer, L., R. J. Deibert, and J. R. Lindsay. 2021. "A Tale of Two Cybers – How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society." *Journal of Information Technology & Politics* 18 (1): 1–20. doi:10.1080/19331681.2020.1776658.

Prior, T., and J. Hagmann. 2014. "Measuring Resilience: Methodological and Political Challenges of a Trend Security Concept." *Journal of Risk Research* 17 (3): 281–298. doi:10.1080/13669877.2013.808686.

Renn, O., A. Klinke, and M. van Asselt. 2011. "Coping with Complexity, Uncertainty and Ambiguity in Risk Governance: A Synthesis." *Ambio* 40 (2): 231–246. doi:10.1007/s13280-010-0134-0.

Ruan, K. 2017. "Introducing Cybernomics: A Unifying Economic Framework for Measuring Cyber Risk." *Computers & Security* 65: 77–89. doi:10.1016/j.cose.2016.10.009.

Sawyer, S., and M. H. Jarrahi. 2014. "Sociotechnical Approaches to the Study of Information Systems." Chapter 5 in *Computing Handbook: Information Systems and Information Technology*, eds. H. Topi, and A. Tucker, 3rd Ed. New York: Chapman and Hall/CRC. doi:10.1201/b16768.

Shandler, R., M. Gross, and D. Canetti. 2023. "Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis." *Journal of Global Security Studies* 8 (1): ogac042. doi:10.1093/jogss/ogac042.

Slupska, J. 2022. "Safer (Cyber)Spaces: Reconfiguring Digital Security Towards Solidarity." PhD Thesis. https://ora.ouls.ox.ac.uk/objects/uuid:9e2484a0-a29a-4623-84ff-22379fb0dfec/files/dms35t913n.

Smit, B., and J. Wandel. 2006. "Adaptation, Adaptive Capacity and Vulnerability." *Global Environmental Change* 16 (3): 282–292. doi:10.1016/j.gloenvcha.2006.03.008.

Statistica 2023. Technology Market Insights, Cybersecurity. Accessed March 2023. https://www.statista.com/outlook/tmo/cybersecurity/worldwide#cost.

Sword-Daniels, V., C. Eriksen, E. E. Hudson-Doyle, R. Alaniz, C. Adler, T. Schenk, and S. Vallance. 2018. "Embodied Uncertainty: Living with Complexity and Natural Hazards." *Journal of Risk Research* 21 (3): 290–307. doi:10.1080/13669877.2016.1200659.

Thoma, K., B. Scharte, D. Hiller, and T. Leismann. 2016. "Resilience Engineering as Part of Security Research: Definitions, Concepts and Science Approaches." *European Journal for Security Research* 1 (1): 3–19. doi:10.1007/s41125-016-0002-4.

Thomalla, F., M. Boyland, K. Johnson, J. Ensor, H. Tuhkanen, Å. Gerger Swartling, G. Han, J. Forrester, and D. Wahl. 2018. "Transforming Development and Disaster Risk." *Sustainability* 10 (5): 1458. doi:10.3390/su10051458.

Tierney, K. 2014. *The Social Roots of Risk: Producing Disasters, Promoting Resilience*. Stanford: Stanford University Press.

UN. 2015. *The 17 Sustainable Development Goals (SDGs) of the 2030 Agenda for Sustainable Development*. Geneva: United Nations. https://www.un.org/sustainabledevelopment/.

UNDRR. 2015. *Sendai Framework for Disaster Risk Reduction 2015–2030*. Geneva: United Nations Office for Disaster Risk Reduction. https://www.unisdr.org/we/coordinate/sendai-framework.

Walker, J., and M. Cooper. 2011. "Genealogies of Resilience: From Systems Ecology to the Political Economy of Crisis Adaptation." *Security Dialogue* 42 (2): 143–160. doi:10.1177/0967010611399616.

Williams, M. J. 2008. "(In)Security Studies, Reflexive Modernization and the Risk Society." *Cooperation and Conflict* 43 (1): 57–79. doi:10.1177/0010836707086737.

Wisner, B., P. Blaikie, T. Cannon, and I. Davis. 2004. *At Risk: Natural Hazards, People's Vulnerability and Disasters*. London: Routledge.