Routledge
Taylor & Francis Group

Information, Communication & Society

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rics20

Failing better in the infosphere: ontological uncertainties and the essence of security in cyberspace

Noran Shafik Fouad

To cite this article: Noran Shafik Fouad (22 Apr 2025): Failing better in the infosphere: ontological uncertainties and the essence of security in cyberspace, Information, Communication & Society, DOI: 10.1080/1369118X.2025.2492574

To link to this article: https://doi.org/10.1080/1369118X.2025.2492574

Published online: 22 Apr 2025.

INFORMATION, COMMUNICATION & SOCIETY
https://doi.org/10.1080/1369118X.2025.2492574

Routledge
Taylor & Francis Group

Failing better in the infosphere: ontological uncertainties and the essence of security in cyberspace

Noran Shafik Fouad

Digital Politics, School of History, Politics and Philosophy, Manchester Metropolitan University, Manchester, UK

ABSTRACT

The operation of digital information systems poses complex challenges for cybersecurity policies and practices. These include the uncertainties associated with vulnerability analysis, intrusion detection, attribution and damage analysis, and the lack of comprehensive technical knowledge about such systems. This article theorises uncertainties as an ontological property of *information*, which co-produces peculiar conceptualisations of 'defence' and 'security' in cybersecurity, in contrast to other security fields. Using interdisciplinary insights from the philosophy of information, information theory, and cybernetics, the article conceptualises cybersecurity as an ontologically informational field – i.e., an infosphere – that is essentially constituted, conceptualised, experienced, and managed through 'information'. It goes on to investigate the characteristics, temporalities, and trajectories of uncertainties in cybersecurity that cannot be reduced to the empirical challenge of 'not knowing', and that are intrinsic to the existence of information and the operation of information systems, beyond the ways such uncertainties are tamed or governed by 'human' actors. This information-theoretic approach ultimately demonstrates how ontological uncertainties co-produce a specific logic of defence in the infosphere that does not postulate a pre-defined enemy or an attack, and an understanding of security as a moving target, in which progress is defined as 'failing better'.

ARTICLE HISTORY
Received 28 November 2024
Accepted 9 April 2025

KEYWORDS
Cybersecurity; information; infosphere; uncertainty; ontology; philosophy of information

Introduction

Since its emergence as a critical issue in contemporary security and politics, cybersecurity has posed significant challenges to traditional approaches of security and defence within International Relations (IR) and Security Studies. Many such approaches attribute agency exclusively to the human subject, thus linking the capacity to act to traits like intentionality, desires, and decision-making – qualities traditionally viewed as unique to humans (Braun et al., 2018; McDonald & Mitchell, 2017; Mitchell, 2014). However, analyses of security that are rooted solely in human subjectivity often fail to account

CONTACT Noran Shafik Fouad n.fouad@mmu.ac.uk Manchester Metropolitan University, Geoffrey Manton Building, 4 Rosamund Street, West Manchester, M15 6LL, UK

for the contingency and unpredictability introduced by non-human 'things', particularly information technologies, and their capacity to challenge human control and intentionality (Fouad, 2022). As put by Miller, 'things that people make, make people' (Miller, 2005, p. 38). Although technological artefacts are created by humans, they can evolve beyond their creators' intentions, shaping various aspects of human existence, including experiences and practices of security.

Cybersecurity too is marked by complex and 'multidimensional' uncertainties that challenge human control (Dunn Cavelty & Wenger, 2022). These pertain to, for example, the attribution of cyber attacks to exact sources (Schulzke, 2018); the relative capabilities or 'cyber power' of actors/adversaries (Valeriano et al., 2018); the scale of damage resulting from cyber incidents (Brantly, 2021); and whether a specific state-sponsored cyber operation is offensive or 'defensive' (Buchanan, 2016). Many cybersecurity literatures analyse such uncertainties as 'operational challenges', caused by the complex nature of cybersecurity environments and their peculiar characteristics (Kaminska, 2021). These characteristics include, for instance, the wide variety of potential cyber attacks (Geers, 2011); the low entry barriers for malicious actors (Weinstein, 2014); the challenges of public-private partnerships (Carr, 2016); and the absence of acceptable international norms for states' behaviour in cyberspace (Moynihan, 2021). As a result, cybersecurity practices are now centred around the management of uncertainties in both the operation of information systems and in policymaking and governance (Lewallen, 2021). This is what Slayton refers to as 'uncertain governance', in which a regime of cyber insecurity is created and normalised (Slayton, 2021). Uncertain governance is also rooted in an understanding that uncertainty is pervasive and that accidents are inevitable in complex sociotechnical systems (Perrow, 1999).

Nevertheless, in cybersecurity literature, uncertainty and risk management are predominantly framed in terms of a human actor 'not knowing' certain aspects of the security environments they are dealing with. Put differently, managing or governing uncertainty in cybersecurity is often understood to be the result of information that is missing, incomplete, or ambiguous, which in turn impacts all aspects of decision making (Dekker & Alevizos, 2024). This perception aligns with broader security and risk literatures in IR, which conceptualise concepts of risk and uncertainty as neo-liberal constructs (O'Malley, 2012). Several security studies contend that risk has changed the international security agenda (Rasmussen, 2004); shifted the focus of strategic studies to risk-based instead of threat-based security strategies (M. J. Williams, 2008); and moved security practices from the management of insecurity to the management of uncertainty (Kessler & Daase, 2008). Here, some critical security scholars draw on Foucault's concept of *governmentality* to frame risk as a 'social technology', or part of a neoliberal rationality. As such, they see risk as being constituted by various material and discursive practices to render the uncertain future 'knowable' and 'actionable' (Aradau & Van Munster, 2007). Yet, as Best argues, viewing risk and uncertainty as 'forms of rationality' is problematic, since it overlooks the indeterminacies of social life, the limits of human understanding, and the bounds of human capacities to make the uncertain *calculable* and *manageable* (Best, 2008). This argument is equally applicable to cybersecurity. As Backman and Stevens put it, conceptualising risk as a form of rationality fails to capture the multiplicity and complexity of risk and the ways it is manifested in cybersecurity practices (Backman & Stevens, 2024).

Against this background, this article presents a novel approach that theorises uncertainties in cybersecurity by employing the multi-disciplinary literature on the philosophy of information, information theory, and cybernetics. The relevance of this approach is based on an assumption that cybersecurity is ontologically informational, or an infosphere that it is constituted, experienced, and managed through *information* (Fouad, 2025). Attending to information adds important insights to the theorisation of uncertainty in cybersecurity, not as an operational challenge of 'not knowing', but rather as an ontological property intrinsic to information systems. This information-theoretic approach to uncertainty allows for the study of the non-linearities of cybersecurity that go beyond human actors' control or rationality. Hence, uncertainty as such, as well as its temporalities and trajectories, is given more weight in the analysis than the ways it is tamed or governed by a human actor. This approach also demonstrates how ontological uncertainties co-produce a specific logic of defence in cybersecurity that is not dependent on a pre-defined enemy or an attack, and an understanding of security as a moving target, in which progress is defined as 'failing better'. This approach, the article argues, challenges existing constructivist theoretical explorations of cybersecurity that assumes a high level of human control in constructing 'security' and 'threats'. It also problematises many cybersecurity practices that have been largely normalised and legitimised as forms of state defence, such as 'defend forward' and 'active cyber defence'.

To unpack these arguments, the article proceeds in three sections. The first section lays the foundations for studying the informational ontology of cybersecurity and for theorising the field as an *infosphere.* It explains how the different categories of information are manifested in the logics and operations of computer systems, and in turn, in the policies and practices designed to secure them. The second section explains how an information-theoretic framework to the study of cybersecurity can offer important insights to the analysis of its complex uncertainties. It builds on the concept of entropy in information theory and cybernetics, defined as uncertainty, disorder, or noise, to analyse uncertainties in the operation of information systems as ontological phenomenon. The third section applies this theoretical analysis of ontological uncertainties to cybersecurity, exploring how they reshape conventional logics of security, defence, and risk in the infosphere. It further examines how an information-theoretic approach challenges the assumption of human control embedded in constructivist cybersecurity studies and in some cyber operations, using 'defend forward' as a case study.

(1) Cybersecurity as an infosphere:

The 'cyber' terminology has long been a source of ambiguity in academic and policy discussions on the security of computers and networks (Futter, 2018). Some scholars argue that the term 'cyberspace' has proven little relevance to socio-scientific analysis, even if widely used (Stevens, 2015). This terminology has been a subject of criticism too because of its inherent Western-centric roots (Nakayama, 2022). Given their ambiguity, terms like cyberspace and cybersecurity are rarely used in technical communities, in which 'information security' or 'infosec' are used instead to discuss the security of digital information systems or simply: computers and networks. However, arguably, the relevance of 'cybersecurity' as a concept lies in its ability to encompass the political and socio-technical nature of the field, and elements of human behaviour and ambitions, transcending the purely technical focus implied by 'infosec' (Stevens, 2023).

Beyond conceptual and semantic contentions, there remains limited theorisation of the ontological makeup of cybersecurity and its inherent informational nature. Arguing that cybersecurity is informational is not a call for replacing the 'cyber' terminology with informational language in academic or policy debates. Rather, attending to information aims at reaching a level of theoretical abstraction to analyse the foundation of cybersecurity and the ways in which it is essentially constituted, experienced, and managed through information. Understanding this informational nature is essential for any attempt to theorise the various empirical challenges in cybersecurity that go beyond the discursive usage of particular terms. But what is information? Although the term is widely used, there is no agreed upon definition or understanding of what information precisely is. The concept of information is considered foundational in many sciences, including mathematics, physics, biology, and several other fields, albeit with little agreement on how to accurately define it. That is one reason why there is currently no such thing as a 'theory of information' with universal applicability (Deacon, 2010).

It was in Norbert Wiener's work on cybernetics that the first use of information as a scientific term first appeared (Wiener, 1948). Cybernetics was a scientific field that emerged in the 1940s amidst the transformations in practices and theories of warfare because of developments in computers and machines. Defined by Wiener as 'the science of control and communication in the animal and the machine', cybernetics examined human-machine interactions and the complex feedback loops of inputs and outputs that enable the operation of self-adaptive systems. The roots of information is also linked to Claude Shannon's theory of communication in 1948 (Shannon, 1948). Shannon is considered today as 'the father of information theory', with some studies going even further to contend he 'invented the information age' (Soni & Goodman, 2017). Even though Weiner and Shannon dealt with information as a measurable entity that should be maximised in communication channels by reducing noise, and hence did not actually define or theorise it, many of the existing philosophical arguments about information draw on their work in some way or another (Burgin, 2010).

An important field that evolved to interrogate the nature of information is the newly-emerging field of philosophy of information (Adriaans & van Benthem, 2008; Floridi, 2010, 2014, 2016). Building upon multi-disciplinary contributions from physicists, mathematicians, computer scientists, biologists, linguists, among others, the philosophy of information presents information 'as a major category of thought within philosophy itself' (Adriaans & van Benthem, 2008, p. 3). The development of such philosophical explorations is closely linked to the evolution of information and communication technologies (ICTs), and especially computing and internetworking technologies, which put information at the forefront of philosophy as a significant force in the functioning of our world. Given its multi-disciplinarity, the philosophy of information introduces diverse approaches to defining information. As noted by Floridi, information is 'a polymorphic phenomenon and a polysemantic concept' (Floridi, 2009, p. 3). It has been approached as 'interpretation, power, narrative, message or medium, conversation, construction, a commodity, and so on' (Floridi, 2016, pp. 2–3).

In relation to cybersecurity, information can be divided into three categories: syntactic information, in the form of bits, signs, and signals; semantic information, or the ideas and meanings conveyed through those bits and signals; and pragmatic information, which is realised when the ideas conveyed are new to the recipient (Deacon, 2010; Fouad, 2022). The syntactic conceptualisation of information formed the core of Shannon's information theory. Shannon viewed information as an entirely mathematical concept and considered the meaning that signals carry to be irrelevant to communication as an engineering problem (Lombardi, 2016). Therefore, some theorists argue that Shannon's theory is better defined as the 'mathematical theory of communication' rather than 'theory of information'. In contrast to Shannon, many scholars regard semantics, i.e., the meaning, relevance, and reliability of information, to be a significant characteristic that distinguish information from data; assuming that data becomes information when meaning is added (Ratzan, 2004).

These categories of information are essential to the conceptualisation and management of cybersecurity. Most cyber threats involve the use of computers and networks, in the form of alteration of codes or the use of malicious software (malware). For that reason, one study considered syntactic information to be the 'centre of gravity in cybersecurity', that distinguishes cyber threats from conventional ones (Friis & Ringsmose, 2016). Importantly, the significance and scale of damage caused by cyber attacks is often dependent on the semantics of information they compromise, be it for example, personal identity, intellectual propriety, business-related information, military secrets, etc. It is also common for some cyber operations to combine both layers, the semantic and syntactic, in case of disinformation campaigns in which compromised devices are used to spread false information. Finally, pragmatic information too forms the core of cyber offence and defence practices, since knowledge about vulnerabilities may enable fixing or exploiting them. As said by a vulnerabilities' seller and noted by one study 'we don't sell weapons, we sell information' (Fidler, 2016, p. 280).

On a more foundational level, all the sciences and technologies that constitute what we know as 'cyberspace' have information at their centre. For example, computer science is often defined as 'the body of knowledge of information-transforming processes' or simply as 'the study of information' (Primiero, 2016). In fact, the idea that computation is a 'science of information' goes back to the 1960s, when computing was defined as 'the systematic study of the ontologies and epistemology of information structures' (Primiero, 2016, p. 104). Computers are generally seen as information storing and processing machines. Such information could be represented in bits (zeros and ones), switch settings (on and off) or voltages (high and low) (Dunn, 2008). Technically, a computer requires binary digits of ones and zeros or on and off states of electrical magnetic input (e.g., pulses of light) to operate at the physical level, which is often conceptualised as *structural* information. There are also *operational* and *instructional* information that connects the physical structure to particular operations through programming languages and user-friendly interfaces that facilitate the relation between users and machines. That is to say, all elements of the operation of computing devices involve information, be it bits, codes, programming languages, algorithms, or even the intention of a computer engineer (Fresco & Wolf, 2016; Primiero, 2016).

In short, if cybersecurity is defined as the security of computers and networks, which are primarily information systems that evolved through information sciences, then it may well be argued that cybersecurity is fundamentally *informational*. On that basis, this article conceptualises cybersecurity as an infosphere; a concept drawn from Floridi's work (Floridi, 2009, 2010, 2013, 2014). Floridi described the infosphere as an informational environment in which various information entities interact in online and offline spaces (Floridi, 2014). Floridi used the infosphere to describe the entire world in which ICTs not only improve human life or re-engineer it, but also 're-ontologise it'. Re-ontologisation here refers to the fundamental transformations that human existence and reality have encountered in what is often called the 'information revolution'. In such world, our existence is not only connected to ICTs, but in many ways, fundamentally dependent on them in spheres where the dividing lines between online and off-line existences have eroded. This dependence has created complex insecurities; as Floridi puts it, 'Only those who live by the digit may die by the digit' (Floridi, 2014, p. 4). In the infosphere, humans transform into informational organisms, or inforgs, in interacting with other non-human, informational machines. In these interactions, humans may not be fully in control of how technologies are interacting with one another, especially with the rapid evolution of the internet of things (IoTs). As a result, security and politics are no longer just about managing people's lives, but also fundamentally about managing the 'life cycle of information' and the ways it is transmitted, processed, and used (Durante, 2017).

Arguing that cybersecurity is an infosphere is ultimately an acknowledgment of the informational essence of the *cyber*, its technologies, and its sciences beyond linguistic and semantic contestations. It is also an argument that cybersecurity threats, like Floridi's infosphere, are driven by growing dependencies on ICTs and that cybersecurity is a field of contingencies that ultimately escape the span of absolute human control. Thinking about cybersecurity through an information-theoretic framework, using insights from information sciences that have direct links to the evolution of its technologies, is essential to understand the complexities and peculiarities of the field. Such an approach develops a necessary level of abstraction that speaks to the fundamental being of cybersecurity and the nature of uncertainties it encompasses, which this article argues are more ontological than operational, as will be shown next.

(2) Informational uncertainties

Uncertainty and risk are two key concepts in neoliberal thinking and policy making in the modern age (Best, 2008; O'Malley, 2012), even if both concepts remain wider than neoliberalism. Many studies argue that risk has transformed security away from threats, urgency, and traditional defence towards an emphasis on precaution, preparedness, and resilience (Hammerstad & Boas, 2015; Kessler & Daase, 2008; Rasmussen, 2004; Williams, 2008). Other studies adopt a more critical approach by analysing how risk frameworks grant decision makers exceptional powers that solidify state sovereignty (Aalberts & Werner, 2011; Stockdale, 2013) and how risk has been commercialised by private companies (Krahmann, 2011). Specifically, building on Foucault's concept of *governmentality*, these contributions analyse risk as a 'social technology' as part of a neo-liberal rationality, put forward to govern the 'ungovernable' (Aradau et al., 2008). Regardless of whether risk has replaced security or transformed the international security agenda, the common understanding is that risk has become central to contemporary theorisation and conceptualisation of security and insecurity.

Uncertainty has a central position in thinking about risk and security transformations too. As Booth and Wheeler put it, in the twenty-first century, uncertainty is turning out to be ‘intense, multilevel and multidirectional’, and therefore affecting every aspect of our societies (Booth & Wheeler, 2023). Although there is no single definition for uncertainty, it is often conceptualised as a form of ‘not knowing’, especially in relation to future events, whereas risk is seen as the method to tame and govern such uncertainty. Specifically, a distinction is made between uncertainty and risk, assuming that uncertainty cannot be predicted or estimated, whereas risk is identifiable and quantifiable (Best, 2008). Uncertainty is also regarded as a line of distinction between security and risk: risk is concerned with manging *uncertainty*, and security is concerned with managing *insecurity* (Kessler & Daase, 2008).

In cybersecurity research, analysis of uncertainty can be found in literatures that use risk-based approaches in studying empirical cases of cybersecurity practices (Backman, 2023). They analyse, for example, the uncertainties that hinder countries’ application of punishment as a response to cyber attacks (Kaminska, 2021); the challenges of determining the actors with responsibility to take decisions in cybersecurity policymaking (Lewallen, 2021); the uncertainties regarding the pace and scope of ‘socio-technological transformations’ (Dunn Cavelty & Wenger, 2022); and the conflicting advice given to private sector entities on potential cyber threats and the necessary security measures to address them (Renaud & Weir, 2016). But is there more to uncertainties in cybersecurity than being an operational challenge or a form of non-knowledge? In the following, this article explains how an information-theoretic framework to the study of cybersecurity can offer important insights to the analysis of its complex uncertainties.

The development of information theory and the evolution of the philosophical ideas around information has always been linked to the concept of uncertainty, which is sometimes referred to as *entropy*. Entropy appeared as key concept in physical sciences in the nineteenth century, particularly in thermodynamics, before later moving to Shannon’s mathematical theory of communication (Shannon, 1948), and to Wiener’s cybernetics (Wiener, 1948). Shannon defined entropy as uncertainty and assumed that information in any system is a measure of its entropy. According to Shannon, when entropy (uncertainty) increases in a system, the amount of information it contains also increases. But how can the level of information be directly proportional to uncertainty? Understanding this ostensibly counterintuitive argument requires and understanding of how Shannon conceptualised information according to probability theory.

In probability theory, the existence of information is linked to the surprise factor. If a certain event is certain or highly probable (e.g., the sun rising every day), knowing about its occurrence would not be surprising to anyone, and therefore, does not provide any information. In contrast, if an event is highly unlikely, knowing about its occurrence represents a significant amount of information (Lombardi, 2016). For example, in English, the letter ‘q’ is always followed by ‘u’. Sending ‘u’ after ‘q’ would not add any information and would be wasteful coding (Davies, 2019). That is, the higher the probability and the less uncertainty, the less information, and vice-versa. This goes in line with Wiener’s cybernetics and his discussion of entropy as a measure of a system’s disorganisation and of information as a measure of a system’s organisation. As Wiener puts it, ‘ … the more probable the message, the less information it gives. Cliches, for example, are less illuminating than great poems’ (Wiener, 1988, p. 21).

Shannon assumed that uncertainty is intrinsic to communication systems. When a particular source sends a message, they are activating one possibility among many. If the receiver already knows what message the source would send, there would not be a need for communication. Sending one message, in such a case, reduces the intrinsic uncertainty of all the other messages that could have been sent but were not (Gregoire & Catherine, 2012). Information here is assumed to be 'the progressive unfolding of this relation between uncertainty and certainty' (Malaspina, 2018, p. 41). In an event of a message, information works dynamically within various (un)predictability levels.

In more practical terms, distortions in communication and information systems have been considered inevitable by various information theorists, due to the multiple layers of information processing and interpretation they involve. Computer systems too involve a large number of complex operations; and when subjected to any error, some loss of information inevitably takes place (Keyes, 1977). Such distortions may be the result of inconsistencies, noise, overload, imprecisions, etc. Hence, any representation of information at the receiving end of communications is better conceptualised as 'controlled distortions of the original information' (Ratzan, 2004). Importantly, information systems interact with thermodynamic subsystems in their operations, which propagates further uncertainty. For example, information transmits in communication devices in the form of energy, such as pulses of light or waves. In this process, any disturbances in the communication channel would result in inevitable energy distortions. So, even when information is successfully transmitted, it could never be identical to its original form. As argued by one study, 'The essence of the bit is the uncertainty inherent in it' (Kafri & Kafri, 2013, p. 135).

However, entropy as uncertainty or noise is not an accident or a negative function of communication. The theory Shannon introduced was built on the premise that information exists simultaneously with uncertainty and noise, and that the challenge of communication is reducing such noise rather than eliminating it. That is why Shannon introduced methods of 'noise tolerance', such as redundancy and error-correction (Fresco & Wolf, 2016). Even coding theories operate on the assumption of the existence of noise and accordingly, they encode information in such a way it could be retrievable despite such noise (Piccinini & Scarantino, 2016). In the same vein, the mathematician Warren Weaver argued that there are two different types of uncertainties: 'spurious uncertainty', representing undesirable noise in information communications, and 'desirable uncertainty', which results from the sender's freedom of choice in deciding which messages to send (Weaver, 1949). This means that even if noise and uncertainty are challenges in communication, as argued by Malaspina, ' … the creation of information can only occur on the basis of noise' (Malaspina, 2018, p. 75).

Hence, ontological uncertainties are essential to the operation of information and communication systems, and they are not just accepted, but also embraced. This is what Frederick P. Brooks, referred to when he discussed software engineering and the operation of computers being non-linear and complex. Brooks argued that such complexity is not accidental, but rather essential to the existence and operation of software. Although accidental complexities and uncertainties can be governed or managed, 'essential complexities' mostly cannot (Brooks, 1987). Given such ontological uncertainties, the outcomes of information systems are often 'emergent' rather than 'resultant' (Gregoire & Catherine, 2012), and the behaviour of information-processing systems is better described probabilistically (Keyes, 1977). Emergence and non-linearity are characteristics of self-organising and complex adaptive systems, in which outputs cannot be simply predicted based on inputs or studying individual parts of the system (Bousquet & Curtis, 2011).

Information systems are connected to this idea of self-organisation, according to which the system chooses one among various possibilities of reaction, without relying on outside structural instructions. Here, emergence and non-linearity do not merely reflect particular practical challenges of not knowing, rather, they represent an ontological phenomenon (Fouad, 2022). Further, entropy as uncertainty, noise, or disorder increases complexity. The physicist Boltzmann argued that entropy is proportional to the number of microstates in a system (Kafri & Kafri, 2013). Complex systems are generally non-linear, resulting in randomness and emergence. Likewise, cybersecurity is as complex and non-linear. The inherent multiplicity of information and the large number of sub systems that are connected to one another engenders non-linearity and an entropic security environment.

The overarching conclusion here is that in information systems, entropy – defined as uncertainty, disorder, or noise – is a default state. A system without uncertainty is primarily a system without information. Additionally, noise is intrinsic to complex systems and to computer science. Communication channels are inevitably noisy, and the challenge is reducing or minimising such noise for information transmission to succeed. Even the process of reducing such uncertainty is marked by multiple indeterminacies per se (Cannizzaro, 2016). That is to say, information is ontologically linked to uncertainty and cannot exist without it. As one study put it, information is 'carved out' from an 'entropic space' (Wicken, 1987). Cybersecurity too is carved out from an entropic space, as will be shown next.

(3) **From security to failing better**If you really want to secure your computer, it is best to turn it off, disconnect it from the Internet, and if you really want to be secure, do not allow any person to get near it, open up the cover, pull out the hard drive, and hit it with a hammer until it no longer can be read. Philip Reitinger, Department of Homeland Security, the USA. (Protecting Cyberspace as a National Asset, 2010, p. 8)

There are multiple areas where ontological uncertainties are pervasive in cybersecurity. A prominent example is vulnerability analysis, through which bugs or errors in coding are investigated to determine which could be exploited by malicious actors. Most cyber incidents take place through the exploitation of certain vulnerabilities in software code. It is widely accepted in technical communities that bugs, that cause system failures, connectivity issues, irregular operations, or those that are security vulnerabilities, are unavoidable (Winkler & Gomes, 2016). Hence, Nissenbaum argued that the uncertainties created by bugs are 'endemic to programming' as the 'natural hazards' of information systems (Nissenbaum, 1997). What is more, it is often difficult to know how a piece of software will interact with different systems until it is released and installed (Ormes & Herr, 2016). Even when a patch (fix) is released to address a vulnerability, there is no guarantee that it will work unless it is applied, and sometimes, it may even cause additional vulnerabilities (Libicki et al., 2015). For example, the recent IT outage in July 2024 that affected millions of Windows systems around the world and disrupted airlines, airports, banks, hospitals, and several other industries, is thought to have been caused by bugs in a software update released by the security company CrowdStrike, that were only discovered when released to customers (Kerner, 2024).

Further, the dynamic nature of information and the constant changes in its operation make it challenging to maintain a static view of complex information systems. Anomalies, inherent to such systems (Lazarevic et al., 2005), can lead to cyber attacks being mistaken for overload signals or errors, and vice versa. This is becoming even more problematic with the rise of the Living Off the Land (LOTL) or fileless malware, which uses existing tools on the targeted system, instead of installing any codes or files (Lenaerts-Bergmans, 2023). Accordingly, uncertainties in cybersecurity as an infosphere are not solely limited to unknowns, but primarily also, a variety of *unknowables*.

Ontological uncertainties in information systems engender multiple policy challenges and enable and/or limit various cybersecurity practices and strategies. Firstly, all cybersecurity practices involve a high level of uncertainty, not only in relation to future cyber threats, but also to threats in the past and present (Scala et al., 2019). This challenges the conventional distinction between uncertainty and risk in many literatures, which posits that uncertainties are incalculable and unmeasurable, while risk provides the framework to calculate and measure them. In cybersecurity, however, risk management is still tied to numerous unknowns and unknowables. For example, although some risk literatures assume that precautionary measures implies the possibility of prevention in risk management (Aradau, 2016), the situation is different in relation to cyber intrusions. Because cyber threats are continuous, and intrusions happen in big numbers, prevention is only possible for a small number of incidents. Hence, prevention is practised differently in cybersecurity from other security fields in which a more absolute preventative security logic is more prominent, such as counter-terrorism. Prevention in cybersecurity is not necessarily about preventing one big disaster or incident, but rather about stopping as many incidents as possible, preventing them from spreading, and minimising their cascading damages.

This results in different temporalities of security that is not accurately defined as *the state* of being secure. Rather, security becomes a *process* of applying effective measures to deal with the continuous risk of cyber threats, not an end goal to eliminate threats altogether. Consequently, cybersecurity is sometimes referred to using normative adjectives, such as ‘good security’ or ‘bad security’, which semantically contradicts the positive notion of ‘security’. Here, cybersecurity does not subscribe to a binary logic that distinguishes between two states: secure and insecure. Therefore, even if cyber insecurity is perceived to be increasing, ontological uncertainties and the inevitability of insecurity make any small progress in any area look good in security evaluation. As argued by Chandler, failure is intrinsic to complex and non-linear systems, just like information systems (Chandler, 2014). Progress in cybersecurity is therefore often measured by the ability to ‘fail better’, or the relative future improvement to the conditions of the present and the past. This reflects the nature of information processes that cybersecurity aim to protect which, as argued by Malaspina, represents a ‘controlled way of falling’, ‘recuperated disorganizations’, or ‘repeated cycles of acquisition and loss of equilibrium’ (Malaspina, 2018, p. 73).

Acknowledging the informational essence of cybersecurity and the ontological nature of its uncertainties, as introduced by this article, produces two key insights: theoretical and empirical. First, theoretically, this informational approach challenges existing constructivist theoretical explorations of cybersecurity that assumes a high level of (human) actor control in constructing 'security' and 'threats'. A prominent paradigm – or meta-theory – in IR and critical security studies that has significantly shaped the study of security, including cybersecurity, is social constructivism. Social constructivism, which examines how social 'realities' and representations – such as states and identities – are produced, has been widely applied to conceptualising security as an 'intersubjective' process of construction (Vuori, 2010). For example, to date, one of the principal ways cybersecurity has been theorised in IR literature is through the Copenhagen School's securitisation theory (Buzan et al., 1998). As one of the most elaborate forms of social constructivism, the securitisation theory studies security as a *speech act* or a discourse in which a 'securitizing actor' presents a threat as existential to a particular referent object (i.e., object of protection) and thus requiring emergency measures to ensure the object's survival. The theory has been applied to studying the socio-political construction of cybersecurity in diverse contexts, including the USA (Dunn Cavelty, 2008; Hansen & Nissenbaum, 2009; S. T. Lawson, 2019); the European Union (EU) (Christou, 2020); Singapore (Aljunied, 2019); Japan (Kallender & Hughes, 2017); and Egypt (Hassib & Alnemr, 2021). Related to this is literature that adopt constructivist approaches and discursive methodologies to explore how cybersecurity threat representations are peculiar when compared to other security sectors (Betz & Stevens, 2013; S. Lawson, 2013; Jarvis et al., 2016).

Accounting for ontological uncertainties in information systems, which go beyond epistemic (non-)knowledge of human actors, challenges the anthropocentric assumptions of constructivism – specifically, its linkage of agency to human subjects and its presumption of high-level human control over security construction. If security construction takes place discursively, and if discourse is tied to human actors, then the ability to influence security ultimately resides in humans (Fouad, 2022). Prioritising human actors in security analysis overlooks how ontological uncertainties constrain human control and intentionality in cybersecurity environments. Accepting these uncertainties as ontological rather than merely epistemic, therefore, problematises the very capacity of human actors to construct security and the constructivist assumption that security is what actors make of it. Such limitations to human agency aligns with some physicists' arguments that information is the fundamental entity of existence, with matter and energy being mere reflections of the information they embody (Harshman, 2016). This argument is summarised by Tom Stonier in saying: '*Information exists*. It does not need to be *perceived* to exist. It does not need to be *understood* to exist. It requires no intelligence to interpret it. It does not have to have *meaning* to exist. It exists' (Stonier, 2012, p. 21).

Secondly, from an empirical standpoint, this information-theoretic approach problematises many cybersecurity practices that have been largely normalised and legitimised as forms of state 'defence', such as 'defend forward' or 'active cyber defence', in which non-disruptive practices aiming at intelligence gathering or 'hacking back' are conducted by governments, including the USA (US Department of Defense, 2023) and the UK (UK Government, 2022). Although these strategies are interpreted differently by different countries, they have generally been normalised in many policy and academic discussions as a form of 'defence', suggesting that the line between 'offence' and 'defence' has been blurred in cyberspace (Buchanan, 2016; Huntley, 2016). In critiquing such operations, many literatures resort to strategic considerations, such as loss of allied trust and disruption of allied intelligence operation (Smeets, 2020), or their negative implications on international cyber norms (Georgieva, 2020; Kello, 2021). An information-centric approach to cybersecurity problematises such practices from an ontological rather than a strategic or a legal standpoint.

Fundamentally, active cyber defence operations are not necessarily directed towards a particular enemy or an attack, they are rather primarily centred around *perceived* risks/threats and hypothetical scenarios of future attacks (Sexton, 2016). Further, such operations are primarily *informational* in nature, i.e., they require constant presence in adversaries' – or even allies' – networks to gather information that would enable the interception of attacks and provide warnings to improve defence systems (Healey, 2019). Multiple uncertainties can shape the threat perceptions upon which such operations are designed, one of which is the challenge of attribution – where identifying the source of an attack, the identity of the attacker, or their motivations becomes uncertain (Egloff & Smeets, 2021). Adding to this is the difficulty of gauging the full scale of damages from past cyber attacks, which further complicates forecasting the impact of potential future cyber incidents. Importantly, in many cyber operations, malware can spiral out of control, spreading to unintended systems and causing unintended consequences (Fouad, 2022). These include the possibility that the targeted system may prove resilient to exploitation attempts, or that vulnerabilities may be patched before they can be exploited (Valeriano et al., 2018). NotPetya and WannaCry ransomware attacks are two famous examples of autonomous cyber attacks or malware that self-propagated in ways that were unpredictable by their initiators (Buchanan, 2020). These are *ontological uncertainties* that are pervasive across the past, the present, and the future of information systems and cybersecurity.

Approaching cybersecurity as a disordered field analogous to entropy in the field of thermodynamics, in which ontological uncertainties go beyond human control, intentionality and rationality, and conceptualising defend forward, active cyber defence, or 'persistent engagement as informational operations can have important policy implications'. Primarily, this theorisation could shift the focus of cyber defence towards prioritising the production of secure-by-design codes over instrumentalising such codes in hacking operations for information gathering. This is not an argument against the relevance of gathering information that can reduce operational uncertainty, which may vary depending on the context. Rather, it is a call to question the underlying logics behind such practices, and the extent to which they can contribute to the security of information systems that are ontologically entropic.

Conclusion

This article introduced an information-theoretic analysis of cybersecurity and its complex uncertainties. Conceptualising cybersecurity as an infosphere is a theoretical move towards ontology and an analysis of information as the essence of the 'cyber'. Acknowledging the informational ontology of cybersecurity allows for utilising the rich and multi-disciplinary body of literature on the philosophy of information and information theory in studying the complexities of this field. The article focused specifically on ontological uncertainties as one such way to demonstrate the relevance of 'information' in understanding the materialities of cybersecurity.

Ontological uncertainties in cybersecurity cannot be reduced to operational or empirical challenges of 'not knowing'. They exist and persist in the operation of information systems and in cybersecurity defence strategies, regardless of human actors' perceptions and even when knowledge about cyber threats is available. Because of their ontological nature, such uncertainties are also not necessarily future-oriented; they span the past, the present, and the future. Operating in such an uncertain, noisy, or disordered space, i.e., entropic space, cybersecurity becomes a disordered field. Such disordered nature challenges some anthropocentric assumptions about the role of humans in constructing security and problematises practices framed as 'defensive' in which cyber operations are launched with the purpose of intelligence gathering. Failing better in the infosphere may, therefore, require an acknowledgment of its non-linearities and the limits of human control or rationality.

Acknowledgment

I am grateful to Matt Spencer for his invaluable feedback and suggestions, which greatly contributed to improving this article. I also extend my thanks to the anonymous reviewers for their constructive and helpful comments.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Noran Shafik Fouad is a Senior Lecturer in Digital Politics at Manchester Metropolitan University, UK. Her teaching and research explore the intersections of technology, security, and governance, with a particular focus on cybersecurity. Her areas of interest include critical approaches to cybersecurity in international relations, cybersecurity of the everyday, the global politics of cybersecurity, and the intersection between cybersecurity and global health. She is currently co-leading the Middle East and Africa stream within RUSI's Global Partnership for Responsible Cyber Behaviour. Previously, Noran worked as a Postdoctoral Research Associate at the Blavatnik School of Government, University of Oxford. There, she conducted public policy research on cybersecurity in the education sector and on risk-based approaches to cybersecurity in low – and middle-income countries. She also co-designed and co-taught executive education programmes, postgraduate courses, and online training for public policymakers on governing digital transformation and cybersecurity. Noran earned her PhD in International Relations from the University of Sussex, UK, funded by the University's Chancellor International Research Scholarship (CIRS), where she also worked as a Doctoral Tutor. She holds MSc and BSc degrees in Political Science from Cairo University, Egypt, where she was an Assistant Lecturer in Political Science. During this time, she conducted research on Middle East politics, focusing on internet governance and digital activism. She was also an Academic Assistant and Executive Editor for two academic journals published by the university. Email: n.fouad@mmu.ac.uk

ORCID

Noran Shafik Fouad http://orcid.org/0000-0001-9517-2267

References

Aalberts, T. E., & Werner, W. G. (2011). Mobilising uncertainty and the making of responsible sovereigns. *Review of International Studies*, *37*(05), 2183–2200. https://doi.org/10.1017/S0260210511000398

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

Aljunied, S. M. A. (2019). The securitization of cyberspace governance in Singapore. *Asian Security*, *6*(3), 1–20.

Aradau, C. (2016). Risk, (in)security and International Politics. In A. Burgess, J. O. Zinn, & A. Alemanno (Eds.), *Routledge handbook of risk studies* (pp. 290–298). Routledge, Taylor & Francis Group.

Aradau, C., Lobo-Guerrero, L., & Van Munster, R. (2008). Security, Technologies of risk, and the political: Guest editors' introduction. *Security Dialogue*, *39*(2–3), 147–154. https://doi.org/10.1177/0967010608089159

Aradau, C., & Van Munster, R. (2007). Governing terrorism through risk: Taking precautions,(un) knowing the future. *European Journal of International Relations*, *13*(1), 89–115. https://doi.org/10.1177/1354066107074290

Backman, S. (2023). Risk Vs. threat-based cybersecurity: The case of the EU. *European Security*, *32*(1), 85–103. https://doi.org/10.1080/09662839.2022.2069464

Backman, S., & Stevens, T. (2024). Cyber risk logics and their implications for cybersecurity. *International Affairs*, *100*(6), 2441–2460. https://doi.org/10.1093/ia/iiae236

Best, J. (2008). Ambiguity, uncertainty, and risk: Rethinking indeterminacy. *International Political Sociology*, *2*(4), 355–374. https://doi.org/10.1111/j.1749-5687.2008.00056.x

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, *44*(2), 147–164. https://doi.org/10.1177/0967010613478323

Booth, K., & Wheeler, N. J. (2023). Uncertainty. In P. D. Williams (Ed.), *Security studies: An introduction* (pp. 151–168). Routledge.

Bousquet, A., & Curtis, S. (2011). Beyond models and metaphors: Complexity theory, systems thinking and international relations. *Cambridge Review of International Affairs*, *24*(1), 43–62. https://doi.org/10.1080/09557571.2011.558054

Brantly, A. F. (2021). Risk and uncertainty can be analyzed in cyberspace. *Journal of Cybersecurity*, *7*(1), 1–12. https://doi.org/10.1093/cybsec/tyab001

Braun, B., Schindler, S., & Wille, T. (2018). Rethinking agency in international relations: Performativity, performances and actor-networks. *Journal of International Relations and Development*, *22*(4), 787–807. https://doi.org/10.1057/s41268-018-0147-z

Brooks, F. P. (1987). No silver bullet essence and accidents of software engineering. *Computer*, *20*(4), 10–19. https://doi.org/10.1109/MC.1987.1663532

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust and fear between nations*. C. Hurst & Co Publishers.

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Burgin, M. (2010). *Theory of information: Fundamentality, diversity and unification*. World Scientific.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cannizzaro, S. (2016). The philosophy of semiotic information. In L. Floridi (Ed.), *The Routledge handbook of philosophy of information* (pp. 290–303). Routledge.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Chandler, D. (2014). *Resilience: The governance of complexity*. Routledge.

Christou, G. (2020). The collective securitisation of cyberspace in the European Union. In S. Lucarelli, J. Sperling, & M. Webber (Eds.), *Collective securitisation and security governance in the European Union* (pp. 52–75). Routledge.

Davies, P. (2019). *The demon in the machine: How hidden webs of information are finally solving the mystery of life*. Penguin UK.

Deacon, T. W. (2010). What is missing from theories of information? In P. Davies & N. H. Gregersen (Eds.), *Information and the nature of reality: From physics to metaphysics* (pp. 146–169). CUP.

Dekker, M., & Alevizos, L. (2024). A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy*, *7*(1), 1–18. https://doi.org/10.1002/spy2.333

Dunn, J. M. (2008). Information in computer science. In P. Adriaans & J. van Benthem (Eds.), *Philosophy of information* (pp. 581–608). Elsevier.

Dunn Cavelty, M. (2008). *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.

Dunn Cavelty, M., & Wenger, A. (2022). The ambiguity of cyber security politics in the context of multidimensional uncertainty. In M. Dunn Cavelty & A. Wenger (Eds.), *Cyber security politics: Socio-technological transformations and political fragmentation* (pp. 239–266). Routledge.

Durante, M. (2017). *Ethics, law and the politics of information: A guide to the philosophy of Luciano Floridi*. Springer.

Egloff, F. J., & Smeets, M. (2021). Publicly attributing cyber attacks: A framework. *Journal of Strategic Studies*, *46*(3), 502–533.

Fidler, M. (2016). Government acquisition and use of zero-day software vulnerabilities. In R. Harrison & T. Herr (Eds.), *Cyber insecurity: navigating the perils of the next information age* (pp. 3–18). Rowman & Littlefield Publishers.

Floridi, L. (2009). Philosophical conceptions of information. In G. Sommaruga (Ed.), *Formal theories of information: From Shannon to semantic information theory and general concepts of information* (pp. 13–53). Springer.

Floridi, L. (2010). *Information: A very short introduction*. OUP.

Floridi, L. (2013). *The philosophy of information*. Oxford University Press.

Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality*. OUP.

Floridi, L. (Ed.). (2016). *The Routledge handbook of philosophy of information*. Routledge.

Fouad, N. S. (2022). The non-anthropocentric informational agents: Codes, software, and the logic of emergence in cybersecurity. *Review of International Studies*, *48*(4), 766–785. https://doi.org/10.1017/S0260210521000681

Fouad, N. S. (2025). *Theorising cyber (in)security: Information, materiality, and entropic security*. Routledge.

Fresco, N., & Wolf, M. J. (2016). Information processing and instructional information. In L. Floridi (Ed.), *The Routledge handbook of philosophy of information* (pp. 77–89). Routledge.

Friis, K., & Ringsmose, J. (Eds.). (2016). *Conflict in cyber space: Theoretical, strategic and legal perspectives*. Routledge.

Futter, A. (2018). Cyber' semantics: Why we should retire the latest buzzword in security studies. *Journal of Cyber Policy*, *3*(2), 201–216. https://doi.org/10.1080/23738871.2018.1514417

Geers, K. (2011). *Strategic cyber security*. Kenneth Geers.

Georgieva, I. (2020). The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy*, *41*(1), 33–54. https://doi.org/10.1080/13523260.2019.1677389

Gregoire, N., & Catherine, N. (2012). *Foundations of complex systems: Emergence, information and prediction* (2nd ed.). World Scientific.

Hammerstad, A., & Boas, I. (2015). National security risks? Uncertainty, austerity and other logics of risk in the Uk Government's National Security strategy. *Cooperation and Conflict*, *50*(4), 475–491. https://doi.org/10.1177/0010836714558637

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

Harshman, N. L. (2016). Physics and information. In L. Floridi (Ed.), *The Routledge handbook of philosophy of information* (pp. 7–14). Routledge.

Hassib, B., & Alnemr, N. (2021). Securitizing cyberspace in Egypt: The dilemma of cybersecurity and democracy. In *Routledge companion to global cyber-security strategy* (pp. 521–533). Routledge.

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, *5*(1), 1–15. https://doi.org/10.1093/cybsec/tyz008

Huntley, W. L.. (2016). Strategic implications of offense and defense in cyberwar. In *The 49th Hawaii international conference on system sciences (HICSS)* (pp. 5588–5595). IEEE.

Jarvis, L., Macdonald, S., & Whiting, A. (2016). Analogy and authority in cyberterrorism discourse: An analysis of global news media coverage. *Global Society*, *30*(4), 605–623. https://doi.org/10.1080/13600826.2016.1158699

Kafri, O., & Kafri, H. (2013). *Entropy: God's dice game*. Createspace Independent Pub.

Kallender, P., & Hughes, C. W. (2017). Japan's emerging trajectory as a 'cyber power': From securitization to militarization of cyberspace. *Journal of Strategic Studies*, *40*(1–2), 118–145. https://doi.org/10.1080/01402390.2016.1233493

Kaminska, M. (2021). Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. *Journal of Cybersecurity*, *7*(1), 1–15. https://doi.org/10.1093/cybsec/tyab008

Kello, L. (2021). Cyber legalism: Why it fails and what to do about it. *Journal of Cybersecurity*, *7*(1), 1–15. https://doi.org/10.1093/cybsec/tyab014

Kerner, S. M. (2024, July 26). *CrowdStrike outage explained: What caused it and what's next*. TechTarget. https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next.

Kessler, O., & Daase, C. (2008). From insecurity to uncertainty: Risk and the paradox of security politics. *Alternatives*, *33*(2), 211–232. https://doi.org/10.1177/030437540803300206

Keyes, R. W. (1977). Physical uncertainty and information. *IEEE Transactions on Computers*, *C–26*(10), 1017–1025. https://doi.org/10.1109/TC.1977.1674737

Krahmann, E. (2011). Beck and beyond: Selling security in the world risk society. *Review of International Studies*, *37*(01), 349–372. https://doi.org/10.1017/S0260210510000264

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, *10*(1), 86–103. https://doi.org/10.1080/19331681.2012.759059

Lawson, S. T. (2019). *Cybersecurity discourse in the United States: Cyber-doom rhetoric and beyond*. Routledge.

Lazarevic, A., Kumar, V., & Srivastava, J. (2005). Intrusion Detection: A Survey. In V. Kumar, J. Srivastava, & A. Lazarevic (Eds.), *Managing cyber threats: issues, approaches, and challenges* (pp. 19–78). Springer US.

Lenaerts-Bergmans, B. (2023, February 22). *What are living off the land (LOTL) attacks?* CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/living-off-the-land-attacks-lotl/

Lewallen, J. (2021). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance*, *15*(4), 1035–1052. https://doi.org/10.1111/rego.12341

Libicki, M. C., Ablon, L., & Webb, T. (2015). *The defender's dilemma: Charting a course toward cybersecurity*. Rand Corporation.

Lombardi, O. (2016). Mathematical theory of information (Shannon). In L. Floridi (Ed.), *The Routledge handbook of philosophy of information* (pp. 30–36). Routledge.

Malaspina, C. (2018). *An epistemology of noise*. Bloomsbury Publishing.

McDonald, M., & Mitchell, A. (2017). Introduction: Posthuman international relations. In C. Eroukhmanoff & M. Harker (Eds.), *Reflections on the Posthuman in international relations: The Anthropocene, security and ecology* (pp. 1–9). E-International Relations.

Miller, D. (Ed.). (2005). *Materiality*. Duke University Press.

Mitchell, A. (2014). Only human? A worldly approach to security. *Security Dialogue*, *45*(1), 5–21. https://doi.org/10.1177/0967010613515015

Moynihan, H. (2021). The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy*, *6*(3), 394–410. https://doi.org/10.1080/23738871.2020.1832550

Nakayama, B. J. (2022). Information Vs the cyberspace domain. *Journal of Cyber Policy*, *7*(2), 213–229. https://doi.org/10.1080/23738871.2022.2083976

Nissenbaum, H. (1997). Accountability in a computarized society. In B. Friedman (Ed.), *Human values and the design of computer technology* (pp. 41–64). Cambridge University Press.

O'Malley, P. (2012). *Risk, uncertainty and government*. Routledge-Cavendish.

Ormes, E., & Herr, T. (2016). Understanding information assurance. In R. Harrison & T. Herr (Eds.), *Cyber insecurity: Navigating the perils of the next information age* (pp. 3–18). Rowman & Littlefield Publishers.

Perrow, C. (1999). *Normal accidents: Living with high risk technologies*. Princeton University Press.

Piccinini, G., & Scarantino, A. (2016). Computation and information. In L. Floridi (Ed.), *The Routledge handbook of philosophy of information* (pp. 23–29). Routledge.

Primiero, G. (2016). Information in the philosophy of computer science. In L. Floridi (Ed.), *The Routledge handbook of philosophy of information* (pp. 90–106). Routledge.

Rasmussen, M. V. (2004). It sounds like a riddle': Security studies, the war on terror and risk. *Millennium-Journal of International Studies*, *33*(2), 381–395. https://doi.org/10.1177/03058298040330020601

Ratzan, L. (2004). *Understanding information systems: What they do and why we need them*. American Library Association.

Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the unbearability of uncertainty. In *2016 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 137–143).

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39*(10), 2119–2126. https://doi.org/10.1111/risa.13309

Schulzke, M. (2018). The politics of attributing blame for cyberattacks and the costs of uncertainty. *Perspectives on Politics*, *16*(4), 954–968. https://doi.org/10.1017/S153759271800110X

Sexton, M. (2016). U.K. cybersecurity strategy and active cyber defence – Issues and risks. *Journal of Cyber Policy*, *1*(2), 222–242. https://doi.org/10.1080/23738871.2016.1243140

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, *27*(3), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

Slayton, R. (2021). Governing uncertainty or uncertain governance? Information security and the challenge of cutting ties. *Science, Technology, & Human Values*, *46*(1), 81–111. https://doi.org/10.1177/0162243919901159

Smeets, M. (2020). U.S. cyber strategy of persistent engagement & defend forward: Implications for the alliance and intelligence collection. *Intelligence and National Security*, *35*(3), 444–453. https://doi.org/10.1080/02684527.2020.1729316

Soni, J., & Goodman, R. (2017). *A mind at play: How Claude Shannon invented the information age*. Simon and Schuster.

Stevens, T. (2015). *Cyber security and the politics of time* (1st ed.). Cambridge University Press.

Stevens, T. (2023). *What Is cybersecurity for?* Policy Press.

Stockdale, L. P. D. (2013). Imagined futures and exceptional presents: A conceptual critique of 'pre-emptive security'. *Global Change, Peace & Security*, *25*(2), 141–157. https://doi.org/10.1080/14781158.2013.774342

Stonier, T. (2012). *Information and the internal structure of the universe: An exploration into information physics*. Springer Science & Business Media.

UK Government. (2022). *Government cyber security strategy 2022-2030*. https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf.

US Department of Defense. (2023). *Cyber strategy of the department of defense*. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.

Vuori, J. A. (2010). A timely prophet? The Doomsday clock as a visualization of securitization moves with a global referent object. *Security Dialogue*, *41*(3), 255–277. https://doi.org/10.1177/0967010610370225

Weaver, W. (1949). The mathematics of communication. *Scientific American*, *181*(1), 11–15. https://doi.org/10.1038/scientificamerican0749-11

Weinstein, D. (2014). Snowden and U.S. Cyber Power. *Georgetown Journal of International Affairs*, *15*(1), 4–11.

Wicken, J. S. (1987). Entropy and information: Suggestions for common language. *Philosophy of Science*, *54*(2), 176–193. https://doi.org/10.1086/289369

Wiener, N. (1948). *Cybernetics: Or, control and communication in the animal and the machine*. Wiley & Sons.

Wiener, N. (1988). *The human use of human beings: Cybernetics and society*. Hachette UK.

Williams, M. J. (2008). (In)Security studies, reflexive modernization and the risk society. *Cooperation and Conflict*, *43*(1), 57–79. https://doi.org/10.1177/0010836707086737

Winkler, I., & Gomes, A. T. (2016). *Advanced persistent security: A cyberwarfare approach to implementing adaptive enterprise protection, detection, and reaction strategies*. Syngress.