Dealing with uncertainty in cyberspace

Berg, B. van den

ScienceDirect

Computers & Security

Available online 5 June 2024, 103939

In Press, Journal Pre-proof What's this?

Dealing with uncertainty in cyberspace

Bibi van den Berg

Show more

Outline | Share Cite

https://doi.org/10.1016/j.cose.2024.103939

Get rights and content

Abstract

While cyberspace as a globally interconnected network offers economic, social and informational potential, at the same time this space also produces a wide variety of risks, for which no easy solutions exist. For the international community, for nation states, for organizations and even for individuals, *uncertainty* is a common thread for interaction, communication and the general use of (systems connected to) cyberspace. This research shows that there are five different common reactions to dealing with this uncertainty in cyberspace: (1) using risk management to control uncertainty; (2) recovering from uncertainty through resilience; (3) influencing uncertainty with laws and regulation; suspending uncertainty by engaging in trust; and (5) ignoring uncertainty through inaction. Some of these approaches are used more often than others. For instance, risk management is currently the dominant way of responding to uncertainty in cyberspace, with resilience gaining prominence. Other strategies, such as relying on trust or inaction, are less common. Oftentimes, using a mixture of strategies may be helpful, because some strategies may strengthen one another, for instance when a combination of risk management and resilience approaches is used. Each strategy has particular use for specific contexts, but since we lack an overview of which strategies are being used, we also cannot establish under which conditions which strategy is most beneficial. Solving this lack of knowledge can help us be more effective in dealing with uncertainties of a wide variety in cyberspace.

Keywords

Uncertainty; cyberspace; risk management; resilience; regulation; trust

1. Introduction

Cyberspace has been labelled as the most complex system mankind has ever made (Risk Nexus, 2014; Van den Berg and Kuipers, 2022). Its rapid development and massive adoption have led to a challenge: we have quickly become "*utterly dependent on a technological system that is both very disruptive and yet is poorly, if at all, understood*" (Naughton, 2016, p. 5). The global character of cyberspace, its vast number of users and interconnections and its rapid technological development contribute to a sense of uncertainty surrounding cyberspace. While nation states, organizations and end users all see the tremendous potential that a globally interconnected network offers, at the same time it has become clear that this space produces a wide variety of risks, for which no easy solutions exist (Giddens, 1999; Rasmussen, 1997).

In recent decades a sense of uncertainty has increased among nation states, in the private sector and among the public in light of three connected and mutually influencing trends: globalization, rising complexity in geopolitics and growing interconnectedness due to the use of digital network technologies. Globalization here refers to a set of social processes that lead to increased globality, which is a "*social condition characterized by the existence of global economic, political, cultural, and environmental interconnections and flows that make many of the currently existing borders and boundaries irrelevant*" (Robertson and White, 2007). Key elements of the notion of globalization that are mentioned in the literature are the disappearance of borders (Robinson, 2007; Steger, 2003), the fact that the capitalist economy has become the global norm (Antonio, 2007; Thompson, 1999) and increased cultural flows across the globe (Steger, 2003). While these developments have had great economic and political advantages, they are also seen to be an important source of uncertainty. A related development is that of increasing instability in geopolitics. Since the end of the Cold War, we have witnessed the demise of traditional blocks of power in international politics (Robertson and White, 2007), more opportunistic and short-lived partnerships between nation states and more rapid dynamism in the alliances that nations states make with other nation states. These developments lead to tension in the international arena. In the words of Robertson and White, "*the present international system is in a state of great and puzzling flux.*" (2007, p. 61). The rise of populism and increasing polarization in countries around the world in recent times fit with this phenomenon (Rohac, 2024). A final interrelated phenomenon is the rise of digital network technologies over the past few decades. Information and communication technologies have been tied into networks that now span the globe,

facilitating instantaneous information-sharing and means of communication. Collectively, these networks form an ecosystem of incredible complexity, called cyberspace. On the one hand, the rise of digital networked technologies has strengthened globalization (Demchak, 2012), on the other the global spread of cyberspace can also be considered an effect of globalization. Over the past decades, cyberspace has come to function as a critical backbone of economies around the globe (Demchak, 2012; Shull, 2019), and an essential part of the everyday activities of end users.

Combined, globalization, increased geopolitical instability and the rise of digital networked technologies lead to more uncertainty for the international community, for nation states, for organizations and even for individuals. It is not surprising, therefore, that these different actors seek to use means to 'tame' this uncertainty, to reduce risk, ambiguity and insecurity. This article discusses five common strategies that are used by different actors to reduce uncertainty in cyberspace. Understanding these strategies enables us to assess the merits and weaknesses of each strategy and develop an approach to choosing particular strategies for particular challenges in cyberspace. The following five broad strategies will be distinguished:

(1) seeking to reduce uncertainty through gaining more *control*, using risk management;

(2) increasing the *adaptability* of systems to withstand incidents through the notion of resilience;

(3) decreasing uncertainty by *steering* or *influencing* the behaviors of actors in cyberspace through regulation;

(4) *suspending* uncertainties by using trust; and

(5) *ignoring* uncertainties by choosing not to act on them.

In the next sections each strategy will be discussed in more detail.

2. Risk management: controlling uncertainty

Risk management is the dominant paradigm of dealing with risk in our modern times (Anton and Nucu, 2020; Power, 2004). Early forms of risk management emerged in the middle of the 20th century in response to questions of the insurability of risk (Dionne, 2013). It then became a solidified approach for controlling risks in different domains, for example in the financial sector and in public health. In recent decades, risk management has also become a key activity in organizations, which seek to reduce risks internally but also regarding the products or services they deliver to customers. Risk management is most well-known for its contributions to engineering, especially in relation to the

development of new systems and technologies, including digital, networked technologies (Power, 2004).

2.1. Five steps to managing risk

As a method, risk management consists of a number of different steps (cf. Anton and Nucu, 2020). The first of these involves the identification of risks: gaining an understanding of the sources and substance of risks that may lead to incidents in relation to a particular activity, system, process or technology (Berg, 2010). Next, individual risks are analyzed or assessed. This involves establishing the likelihood of the materialization of specific risks as well as determining the potential impact they may have once they materialize. Risk assessments can be conducted in a qualitative or a quantitative way, but risk management is most well-known for the latter: for its ability to express the size of risks through a formula, such as risk = probability x impact or a more complex version thereof (Amoroso and Amoroso, 2017; Lester, 2014). A third step involves the prioritization of risks. This entails that decision-makers prioritize which risks need to be addressed first and to which risk levels they need to be reduced. Making this call is based on the risk appetite (Dionne, 2013; Renault et al., 2016) of the entity that is managing the risks. The purpose is to reduce risks to acceptable risk levels (Berg, 2010; Heimann, 1997). In the fourth step the prioritized risks are treated: actions will be undertaken to reduce the likelihood and/or the impact of their instantiation. Treatment may take different forms, depending on the type of risk, the context and the entity's risk appetite. Four common forms of treatment are:

(1) accepting risks, i.e. not treating them (further) because the cost-benefit ratio is such that this would be considered a waste of resources, given the fact that their likelihood and/or impact is low;

(2) aborting activities in which the stakes are too high entirely because the impact of the materialization of a risk would be disastrous and/or the likelihood of that materialization is exceptionally high;

(3) transferring the risk to another party that is better equipped to carry the burden, for instance to an insurance company. This is mostly done in cases where the likelihood of incidents is low but the impact is severe; and

(4) mitigating the risk, i.e. seeking to implement preventative or restorative measures so that the likelihood and/or impact of a risk go down.

The final step in risk management processes is risk monitoring. In this last step, all previous steps are evaluated. Entities verify whether the treatment of risks has been effective and monitor whether new risks are on the horizon. With this step, the cycle of risk management is closed and loops back into step 1 of risk identification.

2.2. Criticisms of risk management

Risk management has been especially successful in the field of engineering, where it is used to build and deliver safer products and services, ranging from cars, airplanes and buildings to complex infrastructures and digital technologies. Because of its success risk management has spread to other societal domains and has become the dominant paradigm for dealing with risk for organizations and governments alike. However, in recent years several lines of criticism have been launched against the use of risk management outside its original habitat of engineering. These criticisms focus mostly on three issues:

(1) complexity,

(2) predictability, and

(3) modelling.

Criticists point out that while engineering challenges, such as increasing car or airplane safety, are challenging because cars and airplanes are complex machines, the level of complexity of these systems pales in contrast to that of, for instance, waging a war against another state, or making cyberspace more secure (van Asselt and Renn, 2011; also see Zio, 2018). Airplanes and cars are systems in which the number of variables that may lead to unsafety or insecurity is large but not unlimited. The number of variables that may lead to risk in cyberspace is infinitely greater and the same applies to all activities in which human agency and intentionality play a role, such as waging a war. Researchers point out that highly complex systems have emerging properties, i.e. properties and interactions between sub-components that no one could have foreseen (cf. Dahlberg, 2015). Cyberspace is considered to be one of these highly complex systems. Because of cyberspace's tremendous complexity, it is far more challenging to establish likelihoods and impacts with respect to risks in this domain (Aven and Zio, 2014). As a consequence, the level of uncertainty in calculations of risk increases to such a degree that it becomes questionable how useful such calculations are (Aven and Zio, 2021). It may therefore be unwise to apply linear predictive models, which are used in risk quantification, to get a handle on risks in principally unpredictable complex systems (Dahlberg, 2015; Dekker, 2011; Eling et al., 2021).

This problem is exacerbated by the fact that in cybersecurity there is a data problem that is absent in e.g. the airline industry. Since its inception in the early 20th century, the airline industry worldwide has collaborated to generate a single data set in which all near misses and accidents are reported.[1] This vast data set is used to ensure that the learnings from past incidents can contribute to preventing their reoccurrence. Because so much data is available, calculating the likelihood and impact of incidents is quite precise, which contributes to predictability. For cyberspace we do not have a data set like this (De

Bruijne and Van Eeten, 2007; Mulligan and Schneider, 2011; Pawlak and Wendling, 2013). Incidents in cyberspace are highly varied and complex, and new incidents of the category 'Black Swans' pop up on a regular basis (Makridakis et al., 2009; Paté-Cornell, 2012). There is also significant underreporting because organizations that are hit by attacks or outages often prefer to keep this information to themselves for fear of reputation damage. Moreover, there is currently no structure in place to report centrally in the first place. The incentive structure to report is also different from that of the aviation industry. And finally: cyberspace does not have a one-hundred-year history yet, so we are still learning what the vulnerabilities in cyberspace are. Since cyberspace is far more malleable than airplanes, and will continue to expand in new directions, it may take a long time before we understand the safety and security issues we may face in relation to cyberspace.

Finally, modelling is very difficult in relation to cyberspace. In aviation, new features in airplanes are tested under a variety of conditions in a modelled environment, and pilots learn to use airplanes in flight simulators. In virtual environments, incidents do not lead to real-world damage to people and systems. But how does one simulate a part of cyberspace in such a way that it truly mimics real-world conditions? Despite the fact that significant advances have been made in the field of simulation-based accident scenario exploration (Zio, 2018), it still remains difficult to create simulations that actually do justice to the complexity and connectivity in real-world cyberspace contexts.

Combined, these three criticisms – cyberspace's complexity, a lack of data, and a lack of possibilities to simulate – lead some critics to argue that the risk management has limited value for cybersecurity (Hall et al., 2015). At the same time, for public and private organizations it is often the go-to. In recent years several other approaches have gained popularity in response to dealing with risk in cyberspace, alongside risk management.

3. Resilience: recovering from uncertainty

The first of these is resilience. This term has gained prominence in policy documents, in crisis management strategies and more broadly in approaches to dealing with uncertainty in the safety and security realm (cf. Dahlberg, 2015; Demchak, 2012; Perelman, 2006; Suter, 2011; Woods, 2015). It has also become a prominently used approach in relation to uncertainties in cyberspace. The notion of resilience does not have a clear definition. Different views on what resilience is or how it could be accomplished have emerged. Three main interpretations of resilience can be distinguished:

(1) resilience as a form of protection;

(2) resilience as preparedness; and

(3) resilience as the ability to adapt.

4.1. Resilience is about protection

A first interpretation of resilience views it as a form of protection. Metaphorically, one could argue that proponents of this view see resilience protecting a treasure vault. Charting the ways in which robbers could break into this vault enables organizations to take measures to prevent a breach of the vault. The more preventative steps one undertakes to protect the vault, the better it will be protected, and the more resilient it is. This approach is similar to that of risk management. In this interpretation, resilience is the goal of a risk management process (Suter, 2011): it is the result that flows from the implementation of a proper and well-executed risk management framework.

4.2. Resilience is about preparedness

A second interpretation of resilience sees it as a means to prepare for potential incidents. This perspective overlaps partially with protection and prevention in the sense that here, too, the aim is to safeguard systems through increased defense. It differs from the first perspective in that it assumes that incidents will materialize, despite our best efforts to prevent them from occurring (Suter, 2011). Consequently, we should prepare for the moments when incidents materialize. This entails that in dealing with uncertainty in cyberspace two main organizational strategies should be followed:

(1) increasing the robustness of systems to withstand a maximum amount of stress and shocks, and

(2) ensuring that a wide variety of capabilities are in place so that, should systems fail or services become disrupted in or through an incident, the organization can recuperate or rebound as quickly as possible.

Preparing for incidents is geared towards restoring organizations to normal operations after incidents as swiftly and efficiently as possible. Organizations' ability to bounce back is often associated with the notion of Business Continuity (Cichonski et al., 2012; Suter, 2011; Zio, 2018) and to accomplish it organizations must ensure that they have so-called 'comprehensive recovery planning' in place (Bartock et al., 2016). Strategies for comprehensive recovery planning include incident and crisis exercises (Seker and Ozbenli, 2018), simulations and war games (Pfeifer, 2018). As Pfeifer explains, "[e]*xercises, simulations and war games are ways to gain insight into decision-making when under stress and confronted with novelty*" (2018, pp. 27–8). Especially when incidents are complex and involve cascading effects (Mouco et al., 2023), it is important that organizations practice how to resolve them internally and in collaboration with other organizations. This helps decision-makers learn about the interdependencies between systems and to anticipate various scenarios (Pfeifer, 2018). Moreover, it is important that incident playbooks are

prepared containing various scenarios including collaboration protocols between different groups.

Preparedness may also involve technical measures, such as building partial redundancies and diversity into systems, so that when one sub-system fails another one may take over, or systems may fail gracefully (Kisner et al., 2010). This increases robustness. Adding extra layers of protection around systems is another possible approach. The idea behind this is that, while individual barriers may have weaknesses, because there are different layers lined up one after the other, chances are that adverse events will not lead to severe harm. This has come to be known as the 'Swiss Cheese Model' (Reason, 1990), also sometimes referred to as 'defense-in-depth' (Ahmad et al., 2012; Amoroso and Amoroso, 2017; Krause et al., 2021), or an 'all hazards approach' (Perelman, 2006; Waugh, 2005). In relation to cybersecurity, increasing robustness involves measures such as adding redundancy to systems, increasing segmentation to networks and contained storage of classified or sensitive information (cf. Linkov et al., 2013).

4.3. Resilience is about adaptability

The third and final interpretation of the notion of resilience builds on the assumption that systems must be able to withstand sudden and substantial shocks that challenge their functioning and be able to overcome them by being able to adapt to shifting circumstances. Systems are sometimes exposed to grave incidents that cannot be prevented or avoided. Such changes may lead to productive change: systems that can adapt to changed circumstances may thrive and become stronger.

A metaphor to describe this interpretation of resilience is that of the body: sometimes a virus invades the body and makes it ill. In response to this, the body tries to fight off the virus by creating antibodies and strengthening its immune system. When successful, the body will emerge from this illness with a stronger immune system than it had before. When applying this metaphor to uncertainty and cyberspace, first and foremost there is a fundamental acceptance that risk and uncertainty cannot be eliminated from cyberspace. Incidents may be a productive part of cyberspace: they may teach us about vulnerabilities and about ways in which to overcome them. Strong cybersecurity means that an organization can withstand a great variety of different kinds of incidents, *and* when crippling incidents do materialize, that the organization is able to transform itself in their aftermath and to keep on functioning even if going back to the previous state is no longer possible. This differs from the second interpretation of resilience, viz. bouncing back to a previous state, in the sense that here, resilience is about a "…*system* [being able] *to cushion the effects of unforeseen disturbances by absorbing the shock and adapting to changing conditions, thus bouncing not back but forward to a more advanced level better suited for future hazards*" (Dahlberg, 2015, p. 553). What this entails in practice in terms

of increasing cybersecurity is for instance the use of self-healing capabilities and accelerated repair and recovery (Naqvi et al., 2021; Perelman, 2006).

Incident response is a crucial part of resilience in the form of adaptability. It refers to the reactions of organizations or individuals to cybersecurity incidents. Incident response usually consists of activities such as:
(1) detecting and analyzing the incident and its causes, including digital forensics;

(2) containing the incident and eradicating its causes;

(3) restoring systems and recovering data or information; and

(4) implementing measures to prevent a future reoccurrence of the same type of incident (cf. Schlette et al., 2021).

Resilience is still a relatively new term in relation to cyberspace, as evidenced by the fact that there are three parallel interpretations of the term. Especially the second and third interpretations of resilience often sit uncomfortably with organizational cultures, in which uncertainty is addressed along the lines of risk management. Using resilience as a starting point rather than risk entails a reconceptualization of organizational processes, of governance and key strategies in addressing the challenges that organizations face.

4. Regulation: influencing uncertainty

While risk management seeks to control uncertainty in cyberspace and resilience aims to improve the ways in which systems can recover from incidents, a third response to dealing with uncertainty in cyberspace is to regulate the behaviors of actors that make use of this space or contribute to its production. The essence of regulation is steering behavior in certain directions. This is also a way of taming uncertainty because the predictability of actors may be increased in specific contexts.

Regulation in relation to cyberspace takes various forms. In some cases, actors' behaviors are regulated through the architecture of the network. This has come to be known as techno-regulation (Benoliel, 2004; Brownsword and Yeung, 2008; Kerr, 2010; Koops, 2011; Leenes, 2011; Lessig, 2006; Nissenbaum, 2011) and nudging (Acquisti, 2009; Calo, 2013; Fogg, 2003; Johnson et al., 2012; Yeung, 2008). In other cases, social norms emerge between different stakeholders in cyberspace, which collectively shape what communities deem to be appropriate behavior in specific contexts (Farrell, 2015; Finnemore and Hollis, 2016; Lessig, 2006). Market forces may also regulate, steer and influence the behaviors of actors in cyberspace (Bradford, 2012). And finally, legal frameworks can regulate behavior in cyberspace. In principle, it is challenging to use laws to regulate behavior in cyberspace, because this space transcends national borders

and spans the globe. At the same time, in the past decades nation states and regional entities such as the European Union have sought to create legal frameworks for specific legal challenges in cyberspace, which are applicable to their territories. Three different kinds of regulation can be distinguished: 'inside-in regulation', 'inside-out regulation' and 'outside-out regulation'.

4.1. Inside-in regulation

The term 'inside-in regulation' refers to the idea that nation states or regions seek to influence the behavior of specific actors within their own territory. In practice, what this often entails is that nation states seek to erect borders in cyberspace to control particular types of behavior (Goldsmith and Wu, 2008). Despite the deterritoralized nature of cyberspace, nation states can aim regulatory interventions at parties within their jurisdiction, i.e. within the borders of their nation state (Wu, 2003, 1997). Examples of this kind of regulation abound. Think for instance of the regulation of local internet intermediaries, such as telecommunications and cable companies, who must comply with national legislation on aiding law enforcement in criminal investigations with respect to fraud, money laundering or child pornography. Or think of regulations aimed at search engines, focused on notice and takedown procedures and filtering and blocking content (Deibert et al., 2008). And finally, think of credit card companies and banks that are obliged by law in some states to check and block dubious financial transactions and provide aid in discovering fraud and money laundering practices (Wu, 1997). The main reason why nation states *can* regulate these parties, even in relation to a transboundary domain such as cyberspace, is because telecommunications companies and banks are by necessity local assets. A telecommunications company must have infrastructure (cables, wires, routers, switches etc.) in place in each state to be able to deliver a service to customers. Similarly, banks must have local offices to connect with their customers. Their territorial presence in a nation state enables the state to enforce its regulations on these parties.

4.2. Inside-out regulation

While inside-in regulation is aimed at influencing the behaviors of actors within the borders of a given nation state, inside-out regulation is regulation that aims to steer behavior within a state or region that has an (accidental, global) effect on actors outside that state or region. One of the most well-known examples of inside-out regulation is the so-called 'Brussels effect' that was first described by Anu Bradford (2012). With this term, Bradford refers to the fact that in the past decades the stringent regulatory standards that the European Union sets to protect EU citizens and to harmonize the EU internal market became regulatory standards worldwide. This has occurred in a variety of different fields, ranging from anti-trust law to environmental protection, and from food

safety and health to data protection. It was not the explicit intention of the European Union to create regulatory standards for the entire globe; this happened as a by-product. Its frameworks have an impact on for instance global companies from other parts of the world, since these companies must comply with EU regulations to be allowed to do business in the EU. Consequently, in the process of rolling out regulatory frameworks intended to keep EU citizens safe and harmonize its market, global players adopt these standards and apply them to all their customers worldwide, since this is economically more efficient. Thus, as Bradshaw points out, the European Union has unilaterally raised standards globally through the principles of harmonization and consumer protection. The global standard for data protection has increased, because companies such as Facebook and Google must now comply with this standard within the EU and choose to do so outside the EU as well.

4.3. Outside-out regulation

A third form of regulation that can be encountered in relation to uncertainty in cyberspace can be labelled as 'outside-out regulation'. Nation states or global companies sometimes also seek to regulate the behavior of (other) nation states. Currently, much of this takes the form debates on international behavioral norms for cyberspace (Finnemore and Sikkink, 1998). In the last decade and a half, nation states have engaged in international talks on norms for state behavior in cyberspace via the UN Group of Global Experts (UN-GGE, 2015, 2021) and the Open-Ended Working Group (OEWG) (Broeders, 2021; Levinson, 2021). But state actors are not the only party to engage in debates on cyber norms. International companies have joined ranks in e.g. the Tech Accord Consortium (led by Microsoft), the Charter of Trust (led by Siemens) and the Cyber Threat Alliance (led by Cisco) to make their voices heard with regards to norms for cyberspace, both for industry itself and for state actors (Katagiri, 2021; Maurer, 2019). Finally, there are multistakeholder norms processes, in which e.g. state actors, representatives from industry, NGOs and academia discuss and advise on norms, as is the case for instance in the Paris Call for Trust and Security in Cyberspace.

In all these processes, participants seek to formulate behavioral standards or 'rules of the road' that actors ought to adhere to in cyberspace to warrant the security of all in this ecosystem. A closely related debate is that on the development of International Law for cyberspace (Broeders and Van den Berg, 2020; Ziolkowski, 2013). Some authors argue that new laws should be developed for cyberspace internationally in the longer run, in addition to, or separate from, existing International Law. Others point towards difficulties in doing so, for example the "*quickly evolving nature of the technology* [, which challenges] *the longevity of a potential international treaty*" (Maurer, 2019, p. 268) but also the fact that the challenges of enforcement are multi-layered and highly complex: holding

parties legally accountable in cyberspace is difficult due issues of anonymity and attribution (Rid and Buchanan, 2015).

5. Trust: suspending uncertainty

A fourth strategy to deal with uncertainty is to accept that it exists, but to suspend it to be able to act under ambiguous conditions. This is exemplified by using trust as a response to uncertainty. In this case, one accepts that there is a fundamental uncertainty, that full control is principally unattainable and that it is unconstructive to seek such control. Instead, one embraces the idea that despite the fact that there is no full control, systems and people can be trusted, relied upon, to function in a predictable manner – at least to some extent and under certain conditions (Keymolen and Van der Hof, 2019; Van den Berg and Keymolen, 2017). Complexity is reduced through trust; it enables us to act against a backdrop of high ambiguity and variability (Luhmann, 2017, 2000). When we trust others or systems, we temporarily put complexities between brackets, and act *as if* the outcome of whatever it is we are engaging in is predictable and stable (Van den Berg and Keymolen, 2017).

Trust can act as a strategy with respect to uncertainty in cyberspace on several levels:

(1) Using cyberspace *requires* trust in systems, in code, in data, in the organizations and governments that facilitate this ecosystem's functioning, and in the organizations and individuals that we connect with via cyberspace (Henschke and Ford, 2016). Debates about cybersecurity rightfully focus on fostering and strengthening trust in cyberspace on a regular basis (Henschke and Ford, 2016).

(2) Trust acts as a key *mechanism* in relation to the adoption of processes, procedures and approaches to increase cybersecurity. Risk management has come to function as the dominant strategy for cybersecurity, but as of yet there is little scientific evidence of its effectiveness in this domain. The adoption of risk management for cybersecurity may therefore be viewed as an act of trust.

(3) Trust is also used as an explicit cybersecurity *strategy*: it is used to reduce uncertainty with respect to security in and of cyberspace (Van den Berg and Keymolen, 2017). This is the case whenever individuals or groups are mobilized to contribute to making parts of cyberspace more secure. Think of, for example, vulnerability disclosure programs in which end users bounty hunt for vulnerabilities in the systems of large internet companies or platforms. Vulnerability disclosure programs build on a mutual sense of trust: companies must trust individuals to scan their code and not take advantage of vulnerabilities they find. At the same time, the individuals participating in these vulnerability disclosure programs must trust the company to take seriously their work, to act on their discoveries and to credit their efforts.

6. Doing nothing: ignoring uncertainty

The previous four strategies all take an active stance towards uncertainty in cyberspace: they all aim to do something in the face of this uncertainty. A final strategy, however, of dealing with uncertainty in cyberspace, is to not only radically accept that it is a fundamental characteristic of this ecosystem, but also to do nothing in response to its manifestations. Currently this strategy is not practiced very often in the field of cybersecurity. Researchers and practitioners in the field sometimes express concern over the lack of response to encountered risks in cyberspace by business leaders or government representatives and plead for more active engagement with those risks (Blau, 2017; Epper Hoffman, 2018; Georg-Schaffner and Prinz, 2021). There is ample evidence of the frequency and impact of cybersecurity incidents and not acting on the most well-documented vulnerabilities and threats may therefore be considered a harmful strategy. Meeting so-called 'baseline cybersecurity' is essential for organizations' survival in an age of pervasive networked, digital technologies (Chaturvedi et al., 2021; Dezeure et al., 2024; Oladoyinbo et al., 2023). When 'doing nothing' equals 'ignoring cybersecurity risks', this seems unwise.

Many organizations today have cybersecurity high on their agendas (Georg-Schaffner and Prinz, 2021). At the same time, discussing cybersecurity challenges in the board room does not always lead to the right level of action yet, since boards often struggle to know what decisions to make with respect to cybersecurity (Epper Hoffman, 2018) and what level of investment is sufficient (Blau, 2017). In some cases, therefore, organizations do not act on cybersecurity risks because they are overwhelmed or undermotivated, or they lack capabilities, capacities or funds. While this may be an unwise strategy, it is also understandable considering the rapid development of new technologies and their associated risks, as well as the impenetrability of technical expertise required to understand them.

But there may also be other reasons to not act in relation to uncertainties in cyberspace and in some areas this could be considered a valid strategy. Doing nothing may entail a wait-and-see-approach. This strategy is particularly relevant in all instances where it is still unclear how significant or impactful a particular vulnerability or risk is. When solid data is lacking (De Bruijne and Van Eeten, 2007; Mulligan and Schneider, 2011; Pawlak and Wendling, 2013), it can be rational to accept uncertainty as a given and not act upon it (Trimintzios et al., 2014). Moreover, interventions involve costs and benefits. When the former outweigh the latter, it is reasonable to ignore risks and accept specific uncertainties.

Of course, embracing a tactic of inaction can only be adopted for some organizations, for some processes, systems and networks, and for some types of uncertainties. This applies to *all* the strategies discussed above: they work well under certain conditions and can be

used to address some specific uncertainties in cyberspace, but none ought to be used across the board. As a matter of fact, using a mixture of different strategies for different contexts and challenges would be best.

7. Different strategies for different problems. Or not?

As this article has shown, in the current cybersecurity landscape the dominant way of thinking about uncertainty in cyberspace is through the lens of risk management. In recent years, there is a noticeable shift towards resilience as a second strategy that complements the risk management paradigm. Risk management and resilience may be seen as complementary in the sense that the former focuses on the prevention of incidents, while the latter has a role to play once incidents have materialized. On a timeline, therefore, risk management focuses on what can be called 'left of bang' (Lester and Moore, 2020), while resilience focuses on being prepared for the bang and on what we could call 'right of bang' (Baskerville et al., 2014). Increasingly, researchers and practitioners also see potential for regulation as a strategy to deal with uncertainty in cyberspace. For a long time, regulation was considered a rather weak mechanism for cyberspace. Pointing to the global nature of cyberspace, and the power of private parties, who own and operate the vast majority of all architecture and services in cyberspace (Demchak, 2012; Goldsmith and Wu, 2008), the central assumption was that influencing actors' behavior in cyberspace through regulation would not be an effective strategy. Over time, this view has changed, in part because discussions have tended to focus more concretely on, for instance, standard-setting and certification (Amoroso and Amoroso, 2017; Shackelford et al., 2015), in part due to the fact that governments have taken a clearer regulatory stance vis-à-vis cyberspace and especially large internet companies (Naughton, 2016), and in part due to the noticeable effects of regulatory interventions, as shown in our discussion of the Brussels effect (Bradford, 2012; Schneier, 2018).

Using trust or doing nothing (in the sense of delaying a response) are currently not considered as common strategies on any significant scale. Both have their merits under certain conditions. As Keymolen points out, it is obviously unwise to address the security challenges of a nuclear power plant through trust mechanisms (Van den Berg and Keymolen, 2017) but trust might be a useful strategy in all those instances where ordinary citizens or end users could be mobilized to help make cyberspace more secure. The same goes for doing nothing. In a reality in which not only the vulnerabilities but also all the solutions that are provided for them are shrouded in urgency and mystery, it is sometimes wise to take a little more time to understand the size, the likelihood and the potential impact of incidents, before adding yet another issue to the decision makers' cognitive load. This is especially the case for all issues and solutions for which substantial data are lacking or the costs of interventions are high.

8. Dealing with uncertainty in cyberspace: Using all tools in toolbox

This article shows that there is a wide variety of uncertainties in cyberspace due to its complex makeup, and that there is also an assortment of possible responses to these uncertainties. As a matter of fact, oftentimes vulnerabilities, threats and risks are best addressed using a mixture of different strategies. They complement and strengthen each other. Regulation works best in a reality in which shared norms already exist, while shared norms and regulation foster and are fed by trust. Similarly, resilience thrives when basic risks have been managed properly, while risk management is most conducive in environments that also focus on preparedness for eventual incidents.

Each of the individual responses to uncertainty that have been discussed in this article have their merits and weaknesses. Risk management works best for all so-called 'subway uncertainties' (Makridakis et al., 2009): uncertainties that appear with relative regularity, so that they can be predicted using probabilistic mathematics. This kind of uncertainties follows a Bell curve pattern and materialize with such constancy that their occurrence can be quantified. When the impact of the materialization of this kind of risk is also fairly well-known, risk management can come to its maximum potential: it can help quantify and prioritize risks of the highest urgency. A clear example of a type of uncertainty that can be addressed well using risk management is combatting DDoS attacks. Due to the regularity and volume of such attacks, over the past years organizations have learnt to understand anomalies in network traffic to such a degree that they may now see DDoS attacks coming early on and have risk management interventions in place to prevent the debilitating effects of such attacks.

Resilience can be used be to prepare for so-called 'coconut uncertainties' (Makridakis et al., 2009): for very rare known unknowns or for unknown unknowns (also known as Black Swans) (van Asselt and Renn, 2011; Taleb, 2010; Zio, 2018). To do justice to the complexity of cyberspace, and to the potential of cascading effects (Cedergren and Johansson, 2017; Luiijf et al., 2008), butterfly effects (Dekker, 2011), and the effects of tight coupling (De Bruijne and Van Eeten, 2007; Demchak, 2012; Perrow, 1984), incident planning and investment in recovery efforts is necessary. The current trend of ransomware is one of these areas where a resilience approach works best. Defense-in-depth and a Swiss Cheese model approach enable organizations to create defensive layers to face this challenge as well as they possibly can, while also allocating time, effort and means for crisis management should the defenses fail. The same holds for highly advanced attacks by APTs: a combined focus on multiple layers of defense combined with preparedness for incidents is currently the most viable strategy to face this threat.

Regulation has potential for two problem areas: addressing uncertainties caused by weak design and thwarting the deliberate exploitation of vulnerabilities by malicious actors. Weak design leads to vulnerabilities in code, configurations, processes and

communications. Regulation can help remedy this issue by setting standards for technology design and service delivery, and it can help foster trust through, e.g., certification, standardization and oversight. Malicious actors of a wide variety may willfully exploit vulnerabilities in cyberspace and are, therefore, one of the biggest sources of uncertainty in this ecosystem. Regulation may have a deterrent effect on such abuse and may lead to prosecution and punishment in case of actual transgressions.

Trust can be used as a viable strategy to deal with uncertainties when implicit normative frameworks already exist, in contexts in which interpersonal connections are essential, and in which harm is limited in cases of transgression. One area where this is fruitful is information sharing with respect to threats or zero days or vulnerabilities. In different countries around the globe, public-private collaborations have emerged, in which parties share information on these topics (Weiss and Jankauskas, 2018). Some of these collaborations take the form of informal networks, whereas others are more formally organized. It is especially in the former category that trust is one of the key drivers (Henschke and Ford, 2016).

Finally, doing nothing is suitable for uncertainties where data on likelihoods is lacking but there is sufficient evidence that no severe harm will be done in the case of incidents. When new threats emerge on the horizon, it oftentimes remains difficult for quite some time to get a sense of the likelihood with which they will materialize, and the conditions under which they will do so. Reliable data on incidents relating to this kind of threat are not easy to come by. If, on top of this, the impact of an incident would be limited, then it is safe to take a wait-and-see-response. An example of this kind of uncertainty in cyberspace is the discovery of vulnerabilities that do not lead to serious system risks and are labelled ‘low/low’ by (inter)national organizations that label emerging threats.

Collectively, risk management, resilience, regulation, trust and doing nothing can be seen as different tools in a toolbox. For some challenges, a hammer works best, and for others a saw or a set of pliers. The same goes for responding to different uncertainties in cyberspace. Choosing the right tool for the right problem would strengthen cybersecurity efforts across the board and decrease uncertainty in cyberspace to a considerable degree.

Uncited References

Oladoyindo, 2023

CRediT authorship contribution statement

Bibi van den Berg: Conceptualization, Formal analysis, Investigation, Methodology, Resources, Writing – original draft, Writing – review & editing.

Declaration of competing interest

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

Recommended articles

Data availability

No data was used for the research described in the article.

References

Acquisti, 2009 A. Acquisti

Nudging Privacy: The Behavioral Economics of Personal Information

Security & Privacy Economics (2009), pp. 72-75

Google Scholar ↗

Ahmad et al., 2012 A Ahmad, SB Maynard, S. Park

Information security strategies: towards an organizational multi-strategy perspective

J Intell Manuf, 25 (2012), pp. 357-370, 10.1007/s10845-012-0683-0 ↗

Google Scholar ↗

Amoroso and Amoroso, 2017 Amoroso E, Amoroso M. From CIA to APT: An introduction to cybersecurity. Columbia, SC (USA): Independently published; 2017.

Google Scholar ↗

Anton and Nucu, 2020 SG Anton, AEA. Nucu

Enterprise Risk Management: A Literature Review and Agenda for Future Research

Journal of Risk and Financial Management, 13 (2020), p. 281, 10.3390/jrfm13110281 ↗

View in Scopus ↗ Google Scholar ↗

Antonio and Ritzer, 2007 RJ. Antonio, G Ritzer

The cultural construction of neoliberal globalization

editor

The Blackwell companion to globalization, Blackwell Publishing Ltd., Malden, MA; Oxford, UK (2007), pp. 67-84

CrossRef ↗ Google Scholar ↗

van Asselt and Renn, 2011 MBA van Asselt, O. Renn

Risk governance

J Risk Res, 14 (2011), pp. 431-449, 10.1080/13669877.2011.553730 ↗

View in Scopus ↗ Google Scholar ↗

Aven and Zio, 2021 T Aven, E. Zio

Globalization and global risk: How risk analysis needs to be enhanced to be effective in confronting current threats

Reliab Eng Syst Saf, 205 (2021), pp. 1-8, 10.1016/j.ress.2020.107270 ↗

Google Scholar ↗

Aven and Zio, 2014 T Aven, E. Zio

Foundational Issues in Risk Assessment and Risk Management

Risk Anal, 34 (2014), pp. 1164-1172, 10.1111/risa.12132 ↗

View in Scopus ↗ Google Scholar ↗

Bartock et al., 2016 Bartock M, Cichonski J, Souppaya M, Smith M, Witte G, Scarfone K. Guide for cybersecurity event recovery (NIST Special Publication 800-184). NIST (National Institute of Standards and Technology); 2016. https://doi.org/10.6028/nist.Sp.800-184 ↗.

Google Scholar ↗

Baskerville et al., 2014 R Baskerville, P Spagnoletti, J. Kim

Incident-centered information security: Managing a strategic balance between prevention and response

Information & Management, 51 (2014), pp. 138-151, 10.1016/j.im.2013.11.004 ↗

View PDF View article View in Scopus ↗ Google Scholar ↗

Benoliel, 2004 D. Benoliel

Technological standards, Inc.: Rethinking cyberspace regulatory epistemology

Calif Law Rev, 92 (2004), pp. 1069-1117

CrossRef ↗ Google Scholar ↗

Berg, 2010 H-P. Berg

Risk management: procedures, methods and experiences

Reliability: Theory & Application, 1 (2010), pp. 79-95

Google Scholar ↗

Blau, 2017 A. Blau

The behavioral economics of why executives underinvest in cybersecurity

Harv Bus Rev (2017)

Google Scholar ↗

Bradford, 2012 A. Bradford

The Brussels effect

Northwest Univ Law Rev, 107 (2012), pp. 1-68

View in Scopus ↗ Google Scholar ↗

Broeders, 2021 D. Broeders

The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment

Journal of Cyber Policy (2021), pp. 1-21, 10.1080/23738871.2021.1916976 ↗

Google Scholar ↗

Broeders and Van den Berg, 2020 D Broeders, B. Van den Berg

Governing cyberspace: Behavior, power, and diplomacy

D Broeders, B Van den Berg (Eds.), Governing cyberspace: Behavior, power, and diplomacy, Rowman & Littlefield, Lanham (2020), pp. 1-17

View in Scopus ↗ Google Scholar ↗

Brownsword et al., 2008 R Brownsword, K. Yeung, R Brownsword, Yeung Karin

Regulating technologies: Tools, targets and thematics

Hart, Oxford (2008), pp. 3-23

CrossRef ↗ Google Scholar ↗

Calo, 2013 R. Calo

Code, nudge, or notice?

Iowa Law Rev, 99 (2013), pp. 773-802

Google Scholar ↗

Cedergren and Johansson, 2017 A Cedergren, J. Johansson

Cascading effects: What are they, and how do they affect society?

University of Lund (2017)

Google Scholar ↗

Chaturvedi et al., 2021 M Chaturvedi, S Sharma, G. Ahmed

Study of baseline cyber security for various application domains

IOP Conf Ser Mater Sci Eng, 1099 (2021), Article 012051, 10.1088/1757-899x/1099/1/012051 ↗

Google Scholar ↗

Cichonski et al., 2012 P Cichonski, T Millar, T Grance, K. Scarfone

Computer security incident handling guide (NIST Special Publication 800-61)

NIST (National Institute of Standards and Technology (2012), 10.6028/NIST.SP.800-61r2 ↗

Google Scholar ↗

Dahlberg, 2015 R. Dahlberg

Resilience and Complexity

Journal of Current Cultural Research, 7 (2015), pp. 541-557, 10.3384/cu.2000.1525.1573 ↗

View in Scopus ↗ Google Scholar ↗

De Bruijne and Van Eeten, 2007 M De Bruijne, M. Van Eeten

Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment

Journal of Contingencies and Crisis Management, 15 (2007), pp. 18-29

CrossRef ↗ View in Scopus ↗ Google Scholar ↗

Deibert et al., 2008 R Deibert, J Palfrey, R Rohozinski, J Zittrain

Access denied: The practice and policy of global internet filtering

MIT Press, Cambridge, Mass (2008)

Google Scholar ↗

Dekker, 2011 S. Dekker

Drift into failure

CRC Press/Taylor & Francis Group, Boca Raton (FL), USA (2011)

Google Scholar ↗

Demchak, 2012 CC. Demchak

Resilience and cyberspace: Recognizing the challenges of a global socio-cyber infrastructure (GSCI)

J Comp Pol Anal: Res Pract, 14 (2012), pp. 254-269, 10.1080/13876988.2012.687619 ↗

View in Scopus ↗ Google Scholar ↗

Dezeure et al., February 16, 2024 F Dezeure, L Moerel, G. Webster

Improving the World's Cyber Resilience, at Scale. Implementing Baseline Security by Default

Implementing Baseline Security by Default (February 16, 2024), p. 2024

Google Scholar ↗

Dionne, 2013 G. Dionne

Risk management: History, definition, and critique

Risk Management and Insurance Review, 16 (2013), pp. 147-166, 10.1111/rmir.12016 ↗

View in Scopus ↗ Google Scholar ↗

Eling et al., 2021 M Eling, M McShane, T. Nguyen

Cyber risk management: History and future research directions

Risk Manag Insur Rev, 24 (2021), pp. 93-125, 10.1111/rmir.12169 ↗

Google Scholar ↗

Epper Hoffman, 2018 K. Epper Hoffman

How to get the board on board with cybersecurity

Independent Banker, 68 (2018), pp. 46-51

Google Scholar ↗

Farrell, 2015 Farrell H. Promoting norms for cyberspace. 2015.

Google Scholar ↗

Finnemore and Hollis, 2016 M Finnemore, DB. Hollis

Constructing norms for global cybersecurity

Am J Int Law, 110 (2016), pp. 425-479

View in Scopus ↗ Google Scholar ↗

Finnemore and Sikkink, 1998 M Finnemore, K. Sikkink

International Norm Dynamics and Political Change

Int Organ, 52 (1998), pp. 887-917

View in Scopus ↗ Google Scholar ↗

Fogg, 2003 BJ. Fogg

Persuasive technology: Using computers to change what we think and do

Morgan Kaufmann Publishers, Amsterdam; Boston (2003)

Google Scholar ↗

Georg-Schaffner and Prinz, 2021 L Georg-Schaffner, E. Prinz

Corporate management boards' information security orientation: an analysis of cybersecurity incidents in DAX 30 companies

Journal of Management and Governance (2021), 10.1007/s10997-021-09588-4 ↗

Google Scholar ↗

Giddens, 1999 A. Giddens

Risk and responsibility

Mod Law Rev, 62 (1999), pp. 1-10

CrossRef ↗ Google Scholar ↗

Goldsmith and Wu, 2008 JL Goldsmith, T. Wu

Who controls the Internet?

Illusions of a borderless world, Oxford University Press, New York (2008)

Google Scholar ↗

Hall et al., 2015 P Hall, C Heath, L. Coles-Kemp

Critical visualization: A case for rethinking how we visualize risk and security

Journal of Cybersecurity (2015), 10.1093/cybsec/tyv004 ↗

Google Scholar ↗

Heimann, 1997 CFL. Heimann

Acceptable risks: Politics, policy, and risky technologies

University of Michigan Press, Ann Arbor (1997)

Google Scholar ↗

Henschke and Ford, 2016 A Henschke, SB. Ford

Cybersecurity, trustworthiness and resilient systems: guiding values for policy

Journal of Cyber Policy, 2 (2016), pp. 82-95, 10.1080/23738871.2016.1243721 ↗

Google Scholar ↗

Johnson et al., 2012 EJ Johnson, SB Shu, BGC Dellaert, C Fox, DG Goldstein, G HÃ¤ubl, *et al.*

Beyond nudges: Tools of a choice architecture

Mark Lett, 23 (2012), pp. 487-504

CrossRef ↗ View in Scopus ↗ Google Scholar ↗

Katagiri, 2021 N. Katagiri

Why international law and norms do little in preventing non-state cyber attacks

Journal of Cybersecurity, 7 (2021), 10.1093/cybsec/tyab009 ↗

Google Scholar ↗

Kerr, 2010 IR. Kerr

Digital locks and the automation of virtue (2010), pp. 247-303

Google Scholar ↗

Keymolen and Van der Hof, 2019 E Keymolen, S. Van der Hof

Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust

Journal of Cyber Policy, 4 (2019), pp. 143-159, 10.1080/23738871.2019.1586970 ↗

View in Scopus ↗ Google Scholar ↗

Kisner, 2010 RA Kisner, WW Manges, LP MacIntyre, JJ Nutaro, JK Munro, PD Ewing, *et al.*

Cybersecurity through real-time distributed control systems

Oak Ridge National Laboratory (2010)

Technical Report ORNL/TM-2010/30

Google Scholar ↗

Koops, 2011 B-J. Koops

The (in)flexibility of technoregulation and the case of purposebinding

Legisprudence, 5 (2011), pp. 171-194

CrossRef ↗ Google Scholar ↗

Krause et al., 2021 T Krause, R Ernst, B Klaer, I Hacker, M. Henze

Cybersecurity in Power Grids: Challenges and Opportunities

Sensors, 21 (2021), 10.3390/s21186225 ↗

Google Scholar ↗

Leenes, 2011 R. Leenes

Framing techno-regulation: An exploration of state and non-state regulation by technology

Legisprudence, 5 (2011), pp. 143-169, 10.5235/175214611797885675 ↗

Google Scholar ↗

Lessig, 2006 L. Lessig

Code: Version 2.0

(2nd ed.), Basic Books, New York (2006)

Google Scholar ↗

Lester, 2014 A. Lester

Risk management

(6th ed.), Butterworth-Heinemann, Oxford (2014), pp. 71-82,

10.1016/B978-0-08-098324-0.00012-3 ↗

Google Scholar ↗

Lester and Moore, 2020 P Lester, S. Moore

Responding to the Cyber Threat: A UK Military Perspective

Connections: The Quarterly Journal, 19 (2020), pp. 39-44, 10.11610/Connections.19.1.04 ↗

Google Scholar ↗

Levinson, 2021 NS. Levinson

Idea entrepreneurs: The United Nations Open-Ended Working Group & cybersecurity

Telecomm Policy, 45 (2021), 10.1016/j.telpol.2021.102142 ↗

Google Scholar ↗

Linkov et al., 2013 I Linkov, DA Eisenberg, K Plourde, TP Seager, J Allen, A. Kott

Resilience metrics for cyber systems

Environment Systems and Decisions, 33 (2013), pp. 471-476, 10.1007/s10669-013-9485-y ↗

View in Scopus ↗ Google Scholar ↗

Luhmann, 2017 N. Luhmann

Trust and power

(English edition), Polity, Malden, MA (2017)

Google Scholar ↗

Luhmann, 2000 Luhmann N. Familiarity, Confidence, Trust: Problems and Alternatives. In: Gambetta D, editor., 2000, p. 94–107.

Google Scholar ↗

Luiijf et al., 2008 Luiijf E, Nieuwenhuis A, Klaver M, Van Eeten M, Cruz E. Empirical findings on critical infrastructure dependencies in Europe. In: Setola R, Geretshuber S, editors. Critical Information Infrastructure Security. CRITIS 2008: Lecture Notes in Computer Science, vol 5508, Berlin, Heidelberg: Springer; 2008, p. 302–10. https://doi.org/10.1007/978-3-642-03552-4_28 ↗.

Google Scholar ↗

Makridakis et al., 2009 S Makridakis, RM Hogarth, A. Gaba

Forecasting and uncertainty in the economic and business world

Int J Forecast, 25 (2009), pp. 794-812, 10.1016/j.ijforecast.2009.05.012 ↗

View PDF View article View in Scopus ↗ Google Scholar ↗

Maurer, 2019 T. Maurer

A Dose of Realism: The Contestation and Politics of Cyber Norms

Hague Journal on the Rule of Law, 12 (2019), pp. 283-305, 10.1007/s40803-019-00129-8 ↗

Google Scholar ↗

Mouco et al., 2023 Mouco A, Ruddell BL, Ginsburg S. Resilience to High Consequence Cascading Failures of Critical Infrastructure Networks. The Sam Houston State University Institute for Homeland Security; 2023. https://doi.org/10.17605/OSF.IO/5R2H6 ↗.

Google Scholar ↗

Mulligan and Schneider, 2011 DK Mulligan, FB. Schneider

Doctrine for cybersecurity

Daedalus, 140 (2011), pp. 70-92

View in Scopus ↗ Google Scholar ↗

Naqvi et al., 2021 MA Naqvi, M Astekin, S Malik, L. Moonen

Adaptive Immunity for Software: Towards Autonomous Self-healing Systems

2021 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), IEEE (2021), pp. 521-525, 10.1109/SANER50967.2021.00058 ↗

Google Scholar ↗

Naughton, 2016 J. Naughton

The evolution of the Internet: From military experiment to general purpose technology

Journal of Cyber Policy, 1 (2016), pp. 5-28, 10.1080/23738871.2016.1157619 ↗

View in Scopus ↗ Google Scholar ↗

Nissenbaum, 2011 H. Nissenbaum

From preemption to circumvention: If technology regulates, why do we need regulation (and vice versa)

Berkeley Tech LJ, 26 (2011), pp. 1367-1386

Google Scholar ↗

Oladoyindo, 2023 Oladoyinbo TO, Adebiyi OO, Ugonnia JC, Olaniyi OO, Okunleye OJ. Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An Enterprise Risk Management Approach 2023. https://doi.org/10.2139/ssrn.4612909 ↗.

Google Scholar ↗

Paté-Cornell, 2012 E. Paté-Cornell

On “Black Swans” and “Perfect Storms”: Risk Analysis and Management When Statistics Are Not Enough

Risk Anal, 32 (2012), pp. 1823-1833, 10.1111/j.1539-6924.2011.01787.x ↗

View in Scopus ↗ Google Scholar ↗

Pawlak and Wendling, 2013 P Pawlak, C. Wendling

Trends in cyberspace: can governments keep up?

Environment Systems and Decisions, 33 (2013), pp. 536-543, 10.1007/s10669-013-9470-5 ↗

View in Scopus ↗ Google Scholar ↗

Perelman, 2006 Perelman LJ. Shifting security paradigms: Toward resilience 2006. https://doi.org/10.13140/2.1.2751.8086 ↗.

Google Scholar ↗

Perrow, 1984 C. Perrow

Normal accidents: Living with high-risk technologies

Basic Books, New York (1984)

Google Scholar ↗

Pfeifer, 2018 JW. Pfeifer

Preparing for Cyber Incidents with Physical Effects

The Cyber Defense Review, 3 (2018), pp. 27-34

Google Scholar ↗

Power, 2004 M. Power

The risk management of everything: Rethinking the politics of uncertainty

London: Demos; (2004)

Google Scholar ↗

Rasmussen, 1997 J. Rasmussen

Risk management in a dynamic society: A modelling problem

Saf Sci, 27 (1997), pp. 183-213

View PDF View article View in Scopus ↗ Google Scholar ↗

Reason, 1990 J. Reason

Human error

Cambridge University Press, CambridgeNY (1990), pp. 1-302

New York (NY)

Google Scholar ↗

Renault and Agumba, 2016 BY Renault, JN Agumba

Ansary N

An assessment of enterprise risk management process in construction firms (2016), pp. 66-79

Google Scholar ↗

Rid and Buchanan, 2015 T Rid, B. Buchanan

Attributing Cyber Attacks

The Journal of Strategic Studies, 38 (2015), pp. 3-37, 10.1080/01402390.2014.977382 ↗

Google Scholar ↗

Nexus, 2014 Risk Nexus

Beyond data breaches: Global interconnections of cyber risk

Atlantic Council (2014)

Google Scholar ↗

Robertson and White, 2007 R Robertson, KE. White

What is globalization?

editor

G Ritzer (Ed.), The Blackwell Companion to Globalization, Blackwell Publishing Ltd., Malden, MA; Oxford, UK (2007), pp. 29-55

CrossRef ↗ Google Scholar ↗

Robinson, 2007 WI. Robinson

Theories of Globalization

editor

G Ritzer (Ed.), The Blackwell Companion to Globalization, Blackwell Publishing Ltd., Malden, MA; Oxford UK (2007), pp. 125-144

CrossRef ↗ Google Scholar ↗

Rohac, 2024 D. Rohac

Populism, Globalization, and Geopolitics

editor

Cope Z (Ed.), The Palgrave Handbook of Contemporary Geopolitics, Springer Nature Switzerland, Cham (2024), pp. 1-20, 10.1007/978-3-031-25399-7_8-1 ↗

Google Scholar ↗

Schlette et al., 2021 D Schlette, M Caselli, G. Pernul

A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective

IEEE Communications Surveys & Tutorials, 23 (2021), pp. 2525-2556,

10.1109/COMST.2021.3117338 ↗

View in Scopus ↗ Google Scholar ↗

Schneier, 2018 Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W. W. Norton; 2018.

Google Scholar ↗

Seker and Ozbenli, 2018 E Seker, HH. Ozbenli

The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation

2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE (2018), pp. 1-9, 10.1109/CyberSecPODS.2018.8560673 ↗

Google Scholar ↗

Shackelford et al., 2015 SJ Shackelford, AA Proia, B Martell, AN. Craig

Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST Cybersecurity Framework on shaping reasonable national and international cybersecurity practices

Tex Int Law J, 50 (2015), pp. 305-356

Google Scholar ↗

Shull, 2019 Shull A. Governing cyberspace during a crisis in trust. Centre for International Governance; 2019.

Google Scholar ↗

Steger, 2003 MB. Steger

Globalization: A very short introduction

Oxford University Press, Oxford (2003)

Google Scholar ↗

Suter, 2011 M. Suter

Resilience and Risk Management in Critical Infrastructure Protection Policy: Exploring the Relationship and Comparing its Use

Center for Security Studies (CSS), Zurich, Switserland (2011)

ETH Zurich

Google Scholar ↗

Taleb, 2010 NN. Taleb

The black swan: the impact of the highly improbable

(2nd ed.), Random House Trade Paperbacks, New York (2010)

Google Scholar ↗

Thompson, 1999 G. Thompson

Introduction: Situating globalization

Int Soc Sci J, 160 (1999), pp. 139-153

CrossRef ↗ Google Scholar ↗

Trimintzios et al., 2014 P Trimintzios, R Holfeldt, M Koraeus, RG Uckan, G Makrodimitris

Enisa. Report on cyber-crisis cooperation and management

ENISA (2014), 10.2824/34669 ↗

Google Scholar ↗

UN-GGE 2021 UN-GGE

Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final substantive report

United Nations Group of Global Experts (2021)

Google Scholar ↗

UN-GGE 2015 UN-GGE

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

(2015)

A/70/174

Google Scholar ↗

Van den Berg and Keymolen, 2017 B Van den Berg, E. Keymolen

Regulating security on the Internet: control versus trust

International Review of Law, Computers and Technology, 31 (2017),

10.1080/13600869.2017.1298504 ↗

Google Scholar ↗

Van den Berg and Kuipers, 2022 B Van den Berg, S. Kuipers

Vulnerabilities and cyberspace: A new kind of crises

Oxford Research Encyclopedia of Crisis Analysis (2022),

10.1093/acrefore/9780190228637.013.1604 ↗

Google Scholar ↗

Waugh, 2005 WL. Waugh

Terrorism and the all-hazards approach

Journal of Emergency Management, 3 (2005), pp. 8-11

Google Scholar ↗

Weiss and Jankauskas, 2018 M Weiss, V. Jankauskas

Securing cyberspace: How states design governance arrangements

Governance, 32 (2018), pp. 259-275, 10.1111/gove.12368 ↗

Google Scholar ↗

Woods, 2015 DD. Woods

Four concepts for resilience and the implications for the future of resilience engineering

Reliab Eng Syst Saf, 141 (2015), pp. 5-9, 10.1016/j.ress.2015.03.018 ↗

View PDF View article View in Scopus ↗ Google Scholar ↗

Wu, 2003 T. Wu

When code isn't law

Va Law Rev, 89 (2003), pp. 679-751

View in Scopus ↗ Google Scholar ↗

Wu, 1997 T. Wu

Cyberspace sovereignty: The Internet and the international system

Harv J Law Technol, 10 (1997), pp. 647-667

View in Scopus ↗ Google Scholar ↗

Yeung et al., 2008 K. Yeung, R Brownsword, Yeung Karin

Towards an understanding of design-based instruments

Hart, Oxford (2008), pp. 79-109

View in Scopus ↗ Google Scholar ↗

Zio, 2018 E. Zio

The future of risk assessment

Reliab Eng Syst Saf, 177 (2018), pp. 176-190

View PDF View article View in Scopus ↗ Google Scholar ↗

Ziolkowski, 2013 K. Ziolkowski

Peacetime Regime for State Activities in Cyberspace

(2013), pp. 1-782

Google Scholar ↗

Cited by (0)

Prof.dr. Bibi van den Berg (1975) is full professor of Cybersecurity Governance at Leiden University, and the head of the Cybersecurity Governance research group at the Institute of Security and Global Affairs of this university. Van den Berg has an MA and PhD in philosophy, both from Erasmus University in Rotterdam. Her research and teaching focus on several themes: (1) cybersecurity governance, (2) governance of security and safety and (3) regulating human behavior through the use of technologies (techno-regulation and nudging).

Van den Berg is the chair of ACCSS, the Academic Cyber Security Society in the Netherlands. She is also a member of the Dutch Cyber Security Council (a Council that advises the Dutch cabinet on how to improve cybersecurity in the Netherlands). Aside from this, Van den Berg is a member of

the ICT Advisory Board of the Central Bureau of Statistics in the Netherlands, the chair of the Advisory Board of IDEMIA, a member of the Advisory Board of ANVS, a member of the Committee Knowledge and Research of the Police Research Board, and a member of the Board of dcypher, the Dutch platform for cybersecurity knowledge and innovation.

1 See https://aviation-safety.net/database/↗ (last accessed on 19 March 2024).