Vulnerabilities and cyberspace: a new kind of crisis

Berg, B. van den; Kuipers, S.L.

Vulnerabilities and Cyberspace: A New Kind of Crises

Bibi van den Berg, Institute of Security and Global Affairs, Leiden University and Sanneke Kuipers, Institute of Security and Global Affairs, Leiden University

https://doi.org/10.1093/acrefore/9780190228637.013.1604
Published online: 24 February 2022

Summary

While cyberspace has become central to all vital processes in the global economy and people's social lives, it also carries a wide variety of risks. Framing these risks is no easy feat: Some lead to harm in cyberspace itself, while others lead to harm in the offline world as well. Moreover, sometimes harm is brought about intentionally, while at other times it may be the result of accidents. The "cyber harm model" brings these challenges together and provides an opportunity to get a comprehensive overview of the different types of incidents related to cyberspace.

It also reveals where the biggest challenges for cyber crisis management lie, and it provides a typology of different types of cyber crises that may arise. Cyber-induced crises have characteristics that make them hard to grapple with, for instance the fact that they can be induced remotely and instantaneously at multiple locations. Moreover, cyber crises are not always easily traceable, and sometimes it is difficult to see that the cause of a particular crisis in the offline world is an act in cyberspace. Finally, the borderless nature of cyberspace leads to potential large-scale geographical spread for cyber crises.

Cyber crises also lead to a number of specific challenges for leadership, especially with respect to sense-making, meaning making, decision making, termination, and learning.

Keywords: cybersecurity, vulnerabilities, cyberspace, intentional harm, accidental harm, crisis management, harm in cyberspace, harm via cyberspace, cyber harm model, crisis analysis

Subjects: Policy, Administration, and Bureaucracy, Political Communication

The Centrality of Cyberspace

Cyberspace has become an indispensable ecosystem for businesses, organizations, citizens, and governments alike (Fransman, 2010). In a mere four decades, it developed from a brand new, virtual space populated by a technical and academic elite (Naughton, 2016; Severance, 2015) to a backbone for all vital processes in the global economy, as well as for people's social lives (Kuehl, 2009; Susskind, 2018). Cyberspace is without a doubt the largest and most complex system mankind has ever made, and its rapid development and massive adoption has led to an interesting challenge: Most of the global population has 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).

Defining cyberspace, or capturing its “core” in a short description, appears to be quite a challenge, although many authors have tried (see Deibert & Rohozinski, 2010a; Dunn Cavelty, 2013; Kuehl, 2009; Liaropoulos, 2011). Perhaps rather than coming up with a single, comprehensive definition, one ought to look at some of the key descriptors that collectively depict and delineate cyberspace as a phenomenon instead. The authors propose a total of six aspects, divided into two sets: descriptions of the *physical infrastructure* that make up cyberspace, or its *physicality*, and qualifications of the *use* one makes of cyberspace.[1]

While many people intuitively think of cyberspace as a virtual or intangible “space,” it is very much grounded in a hard, physical reality, without which it would not exist. Cyberspace depends on a physical, technical infrastructure consisting of many interconnected elements. Collectively, the physicality of cyberspace can be captured as follows: (a) Cyberspace is an *ecosystem*[2] (b) that it is made up of *digital technologies*, which are (c) *connected through networks*. Since cyberspace consists of and connects a wide range of different subsystems, it is often called a “system of systems” (cf. Fransman, 2010).

At the same time, what cyberspace is, as well as how it is viewed, is shaped to a significant extent by its use, that is, by the activities one engages in using this ecosystem and the purposes one has with those activities. Capturing the key aspects of the use one makes of cyberspace, it can be stated that (d) cyberspace is an ecosystem in which a variety of different types of *actors* engage in a wealth of different *behaviors* (discussed more later); (e) most importantly involving the *creation*, *storage*, *modification*, *sharing*, and *exploitation* of *information*; and (f) in their use of cyberspace these actors treat this ecosystem as an *operational* space, that is, a space in which strategic activities take place toward certain ends. Figure 1 summarizes these six characteristics, which collectively make up what cyberspace is and what it is for.

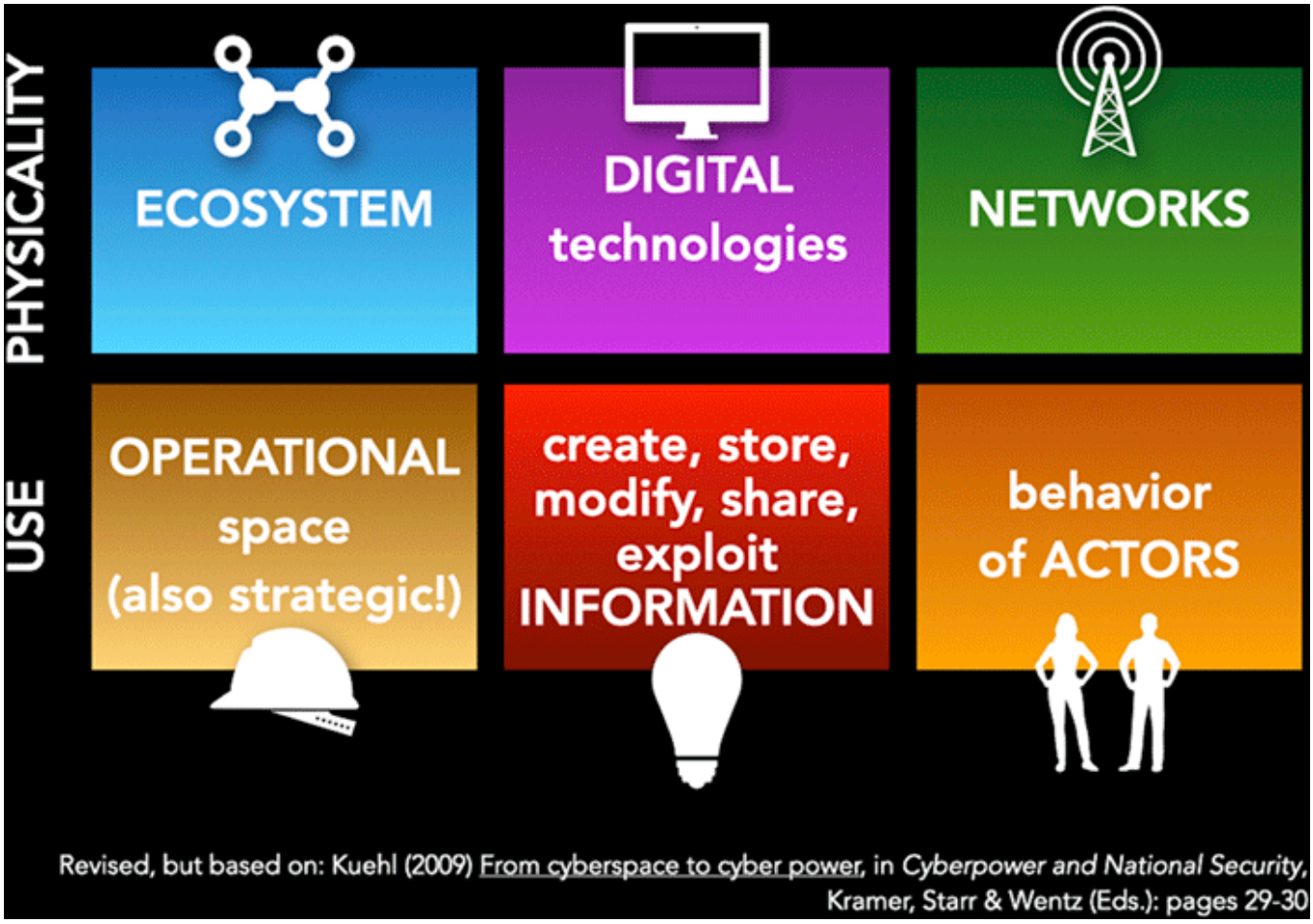

Figure 1. Six key characteristics of cyberspace.

As an ecosystem cyberspace is a highly complex environment, made up of countless subsystems, networks, and other infrastructural elements, which span the globe and interconnect in innumerable ways. Openness and flexibility were chosen as core design principles in the development of cyberspace to leave as much room as possible for innovation and facilitate maximum growth (cf. Leiner et al., 2009; Naughton, 2016). These enabling features have led to, and still lead to, the explosive expansion of the ecosystem, both in terms of the variety of uses it serves and the number of people populating this ecosystem.

Aside from the technical and infrastructural complexity of cyberspace's infrastructure, cyberspace's use is highly complex as well. For one, a wide variety of different actors populate cyberspace, ranging from individuals and consumers, to groups and collectives, to businesses and organizations, to nation-states and their proxies (Czosseck, 2013; Kuehl, 2009; Maurer, 2018a). Increasingly, nonhuman actors, such as bots, play a role in cyberspace, for instance in algorithmic and economic trading in the financial sector (cf. Kim, 2007) or in spreading marketing or political messages on social media such as Twitter (Howard & Kollanyi, 2016). Bots are also used for harmful purposes, most importantly to collectively flood specific website domains so that these go offline (cf. Lafrance, 2017).

Collectively, the actors in cyberspace engage in a wide variety of different activities in this ecosystem. Cyberspace is used to look up, share, or store information; to shop; to date or find friends; to pay; to connect or communicate; to read books or newspapers; to navigate; and so on and so forth. The list of activities that have gained the “cyber” prefix continues to grow. Think of cyber bullying (Bryce & Klang, 2009; Livingstone et al., 2011; Van der Hof et al., 2014), cyber terrorism (Brenner, 2007; Wade, 2003), cybercrime (Jewkes & Yar, 2010; Leukfeldt, 2017; Wall, 2015, 2017), cyber warfare (Ben-Israel & Tabansky, 2011; Demchak & Dombrowski, 2011; Rid, 2012; Singer & Friedman, 2013; Taddeo, 2012), and cyberespionage (Buchan, 2015; Contreras et al., 2013; Landau, 2013; Walsh & Miller, 2015; Ziolkowski, 2013). New possibilities to share, connect, collaborate, but also distort, manipulate, and attack in or via cyberspace arise almost daily. This leads to significant challenges for researchers seeking to understand human behavior in cyberspace. With the changes in the ecosystem, new and unexpected behaviors constantly emerge and behavioral norms change.

From Cyberspace to Cybersecurity

Since cyberspace has become the single most important infrastructure in the world, both economically and socially, the security of this ecosystem has become a concern for governments, businesses, and citizens alike. After its inception, it soon turned out that while this massively interconnected, global system of systems had significant benefits, its use also led to the emergence of a wide variety of new risks. The software, hardware, and networks that collectively constitute cyberspace are full of *vulnerabilities*, that is, “errors in computer systems which can be exploited to breach security mechanisms” (Böhme, 2005, p. 1). When people exploit such vulnerabilities, this leads to so-called cyberattacks or cyber incidents. The latter are defined as “deliberate disruptions of routine and everyday cyber-security practices, designed to protect networks, computers, programs and data from attack, damage, or unauthorised access” (Balzacq & Dunn Cavelty, 2016, p. 180). When a vulnerability is exploited for the first time, it is called a “zero day”: “A cyber-attack exploiting a vulnerability that has not been disclosed publicly” (Bilge & Dumitras, 2012, p. 833). Because it is a previously unknown vulnerability, no protections exist against it yet. Since it takes time to create such protections and remedy the gap a vulnerability leaves, “zero day” refers to the day at which the exploit becomes known, and hence a process of defense or patching can be instigated.

Due to the complexity and interconnectedness of cyberspace, the number of vulnerabilities that may be exploited by perpetrators is almost limitless. This is why, in cybersecurity lingo, researchers tend to speak of the ever-increasing “attack surface” of systems and networks (cf. Onyeji et al., 2014; Soule et al., 2015). This term refers to the totality of all the possible ways attackers can exploit weaknesses of systems and networks (also see Meeuwisse, 2017, p. 181). By (inter)connecting ever more systems and networks, the attack surface will only increase in the upcoming years. Trends such as the rise of smart cities (Elmaghraby & Losavio, 2014) and the emergence of the internet of things (Schneier, 2018) are likely to exacerbate this hazard.

For researchers, governments, and businesses, when it comes to cybersecurity, three themes dominate the agenda at the beginning of the 2020s: cybercrime, cyberespionage, and the protection of critical infrastructures. This article discusses these three in turn to delve a little deeper into the particular vulnerabilities and issues at stake surrounding each theme.

Cybercrime

Cybercrime was among the first (sets of) risk that was identified after the emergence of cyberspace. Already in its early days, governments, law enforcement, and the academic community realized that individuals and groups were not just using cyberspace for benign purposes, they quickly discovered that many forms of offline crime now found penchants and guises in the online world and that cyberspace facilitated a variety of crime types hitherto unknown or nonexistent.

Cybercrime can be divided into three different categories (Wall, 2015, 2017). First, there is *computer-assisted* crime. This refers to criminal acts whereby digital technologies are used but are not essential to the activity, that is, these same activities could have occurred without the use of said technologies. Computer-assisted crime thus refers to all forms of "old" crime known before the advent of cyberspace, which are instead conducted in or via cyberspace. An example of computer-assisted crime is committing fraud or conducting money-laundering.

Second, there is the notion of *computer-enabled* crime. The emergence of digital networked technologies and cyberspace has facilitated a host of qualitatively different opportunities for already existing criminal activities. For instance, the rise of social media has facilitated novel forms of bullying or harassment. In contrast to old offline crime, these kinds of crime are different in their scale, reach, and impact. Using digital technologies, one can reach far more individuals, as well as harm them more frequently, anonymously and easily than in the days before cyberspace. Bullying and harassment, therefore, are not only facilitated by cyberspace but also transformed to some degree.

A third and final category is *computer-dependent* crime. In contrast to computer-assisted and computer-enabled crime, which both had offline forerunners, computer-dependent crime does not. It refers to all forms crime that depend on networked, digital technologies and cyberspace, that is, it could not be conducted without them. The most obvious example of computer-dependent crime is hacking; it is only because of the existence of digital networked technologies that hacking as an activity can exist.

Cyberespionage

A second set of security concerns relating to cyberspace has been the emergence of cyberespionage. Intelligence gathering has always been a part of statecraft (Chesterman, 2006), and in that sense, it is unsurprising that state actors employ cyberspace for purposes of espionage. Similarly, throughout history businesses have also sought to increase their competitive advantage by gathering intelligence on their competitors' practices and plans.

Here, too, therefore, a move to cyberspace was expected. The term *cyberespionage* may refer to both forms: It can denominate commercial and state espionage.[3] Often, the two forms of espionage can be intertwined. For instance, actors may seek to gain access to Boeing or Lockheed Martin, both commercial weapons manufacturers, because intelligence on their systems could give both rival companies and nation-states a competitive advantage.

Two points are key to understanding cyberespionage. First, the means and methods for gathering intelligence are qualitatively different in comparison to offline forms of espionage. The scale, reach, and impact of intelligence-gathering activities has changed fundamentally in light of the rise of networked, digital technologies. Actors may now gather data in bulk, for instance, that is, bring in immense volumes of (meta)data and use data analytics to sift through the data for relevant patterns.

Second, while espionage still sounds like the work of spies—controlled and handled by states to gather (specific) information on the activities of other states—in cyberspace a multitude of different actors, with or without relationships to the state, may conduct intelligence-gathering activities. News media and popular articles often tend to portray states as actors in cyberespionage, for instance when “China” stole personal information about 21 million American citizens working for the U.S. government by breaking into the database of the U.S. Office of Personnel Management (Nakashima, 2015), or when “Russia” meddled with the U.S. presidential elections in 2016 (Mueller, 2019), or when the “United States” gathered data on both friends and foes using the PRISM program, as revealed by the Edward Snowden leaks (Sottek, & Kopfstein, 2013).

In practice, nation-states do indeed sometimes actively instigate cyberespionage or run espionage programs in cyberspace themselves. Unit 61398, a Chinese cyber unit that is held responsible for large-scale espionage activities, is said to have been created by the Chinese government specifically and explicitly for this purpose (Buchan, 2015). The NSA’s activities, as revealed by Snowden in 2013, are also an example (Landau, 2013). But oftentimes, states also use other actors to engage in cyberespionage on their behalf. In the words of Tim Maurer, “To project cyber power . . . states rely on hackers that do not wear uniforms and are not part of the intelligence community—cyber mercenaries or, more broadly, cyber proxies” (Maurer, 2018b, p. 171). A “cyber proxy” can be any nonstate actor that operates in cyberspace on behalf of a nation-state, whether or not the state publicly acknowledges their actions (Czosseck, 2013, p. 2). When looking at the use of proxies for espionage or for offensive activity in cyberspace, three different relationships between states and their proxies can be distinguished (Maurer, 2018a, 2018b). First, states may *delegate* responsibility for espionage to proxies. This means that their activities are under close control of the state. Second, states may *orchestrate* proxies’ espionage or other offensive activities. This means that these proxies are on “a looser leash yet [act] in concert with a government’s objectives” (Maurer, 2018b, p. 174). Finally, states may *sanction* proxies’ espionage, which can mean a number of things, ranging from passive support to not interfering to end their activities. States may choose to use such proxies because they lack sufficient technical expertise themselves to engage in sophisticated attempts at intelligence gathering but also because it enables them to plausibly deny involvement should the attackers get caught (cf. Kello, 2013; Singer & Friedman, 2013).

One of the key challenges regarding both cyberespionage and cybercrime is the attribution problem. This problem “refers to the difficulty of identifying those initially responsible for a cyber-attack and their motivating factors” (Dunn Cavelty, 2013, p. 113). Because cyberspace connects systems and networks globally, each act in cyberspace crosses numerous networks and “hops” along the way. Tracing back these hops across borders (read: jurisdictions) is no easy feat. Anonymizing techniques and technologies may be used by criminals and spies, making it more difficult to find them (Clark & Landau, 2011), though some researchers point out it is not impossible to do so (Rid & Buchanan, 2015). Legally, proving beyond reasonable doubt which natural person “pushed the button” to engage in an attack and proving which intention this was done for (an act of war? A criminal act? A terrorist act?) is even trickier (Brenner, 2007). Proving that an actor could foresee (all) the potential outcome(s) of his or her actions is even harder in complex, networked ecosystems such as cyberspace. As time progresses, however, law enforcement is getting better at attributing cyberattacks and acts of espionage, and this has resulted in several indictments, especially in the United States (Maurer, 2018b). Such indictments can be read as a form of political signaling to other nation-states that espionage, or other forms of cyberattacks, do not go unnoticed and, more importantly, may help shape norms for state behavior in cyberspace (Keitner, 2019).

Critical Infrastructure Protection

A third topic that is high on the agenda of both researchers and politicians is the protection of critical infrastructures. Many states consider this to be one of the most important national security issues. The term *critical infrastructures* refers to “physical and information technology systems, networks, services, and assets which, if disrupted or destroyed, would have a devastating impact on the health, safety, security, or economic well-being of citizens or the active functioning of governments” (Onyeji et al., 2014, p. 54). Interestingly, infrastructures have only come to be labelled “critical” since the late 1990s, when, after the end of the Cold War, states realized that their infrastructures are both vital for societal and economic functioning and may be vulnerable to disruption or sabotage (Aradau, 2010). With the rise of cyberspace, in a sense, infrastructures have become even more “critical” because they are now part of a globally (inter)connected network. Operators of, for example, energy grids, utilities, and railroads have chosen to attach their operational technologies to cyberspace to increase efficiency and lower costs (Alcaraz & Zeadally, 2015; Gheorghe et al., 2007). When operators can manage the opening and closing of a range of flood controls remotely from a single central location, this is far more cost-efficient than when operators need to man a station or be close to the physical location of each individual dam. However, when operators can manage flood controls remotely, there is a real and urgent risk that others can too. This is why, in relation to critical infrastructures, the terms *cyber physical systems* and *cyber physical risks* are often used (cf. Cárdenas et al., 2009).

The term *cyber physical systems* refers to oftentimes large-scale, industrial systems that combine or integrate digital, networked technologies with operational technologies, or OT. The latter are technologies used to change physical states in the real world, for instance opening or closing a valve to control pressure in a pipeline, but also the state of traffic signs

or signaling over railways. Combining such operational technologies with digital, networked systems leads to two major challenges. First, as we have seen, by adding network technologies, these systems may be accessed via cyberspace not only by operators (the intended users) but also by outsiders, who may accidentally or willfully manipulate them. Since cyber physical systems have effects in the real world (e.g., opening or closing a valve or a dam), their manipulation may lead to (severe and large-scale) physical harm in the real world. The abuse of cyber physical systems through acts in cyberspace can ultimately lead to high numbers of deaths and damage in the offline world.

Second, operational technologies are oftentimes large-scale systems, collectively called industrial control systems (ICS). These are monitored by supervisory control and data acquisition (SCADA) systems. Since such systems are highly complex and purpose-made for individual facilities, replacing them is very expensive. Add to this the fact that many of the ICS and SCADA systems were developed in the decades before the rise of cyberspace and were, hence, never designed with (global) networking capabilities in mind (Onyeji et al., 2014). This means that there are serious concerns regarding the security of connecting these systems to cyberspace. To make matters worse, the technologies and systems used to connect such control systems to cyberspace oftentimes are off-the-shelf, box-standard information and communication technologies (ICTs), with all the on-board and built-in vulnerabilities these systems may have. Thus, critical infrastructures can be exploited with the same (types of) tools and mechanisms as any other networked, digital device.

In sum, by equipping critical infrastructures with cyber connectivity, they have become easier and more efficient to manage. At the same time, they have been opened to a variety of severe and complex risks, which terrorists, state actors, competitors, and criminals could take advantage of. Due to the potential lethalness of these risks, critical infrastructure protection is justifiably high on the agenda for politicians, operators, and researchers. It should also be so for those interested in crisis management, yet the particular combination of cyber risk management and critical infrastructure protection gets relatively limited attention in the crisis literature (Kuipers & Welsh, 2017) and in the risk literature (Kuipers et al., 2018). While a predicted “cyber Pearl Harbor” (Hansen & Nissenbaum, 2009) has not materialized, if ever it will, then it is likely that it will stem from this particular category of vulnerabilities in cyberspace.

The Cyber Harm Model

After this discussion on the key topics in research and policymaking for cyberspace, the next questions to be answered include the following: What should those interested in crisis management take away from this discussion? What types of crises are most likely to occur, and/or will have the biggest impact, in relation to cyberspace and the risks we have encountered there? The range of potential problems caused by or encountered in cyberspace is quite extensive, and the particularities of the crises they may generate are wide-ranging and diverse. Cyberspace is a global, complex ecosystem, which contains risks on many levels, potentially affecting many different areas of life, both in cyberspace itself and outside. To

structure a discussion on the width and reach of potential issues, the authors developed the cyber harm model. This model starts from the question: Which harm does the exploitation of cyber vulnerabilities lead to, and where and how does this harm materialize? Focusing on the harm that is generated facilitates (a) clustering themes, topics, and issues in a relevant and clear manner, and, more importantly, (b) shedding light on the areas of gravest potential harm and thus inventories crisis-management implications. The cyber harm model is depicted in Figure 2.

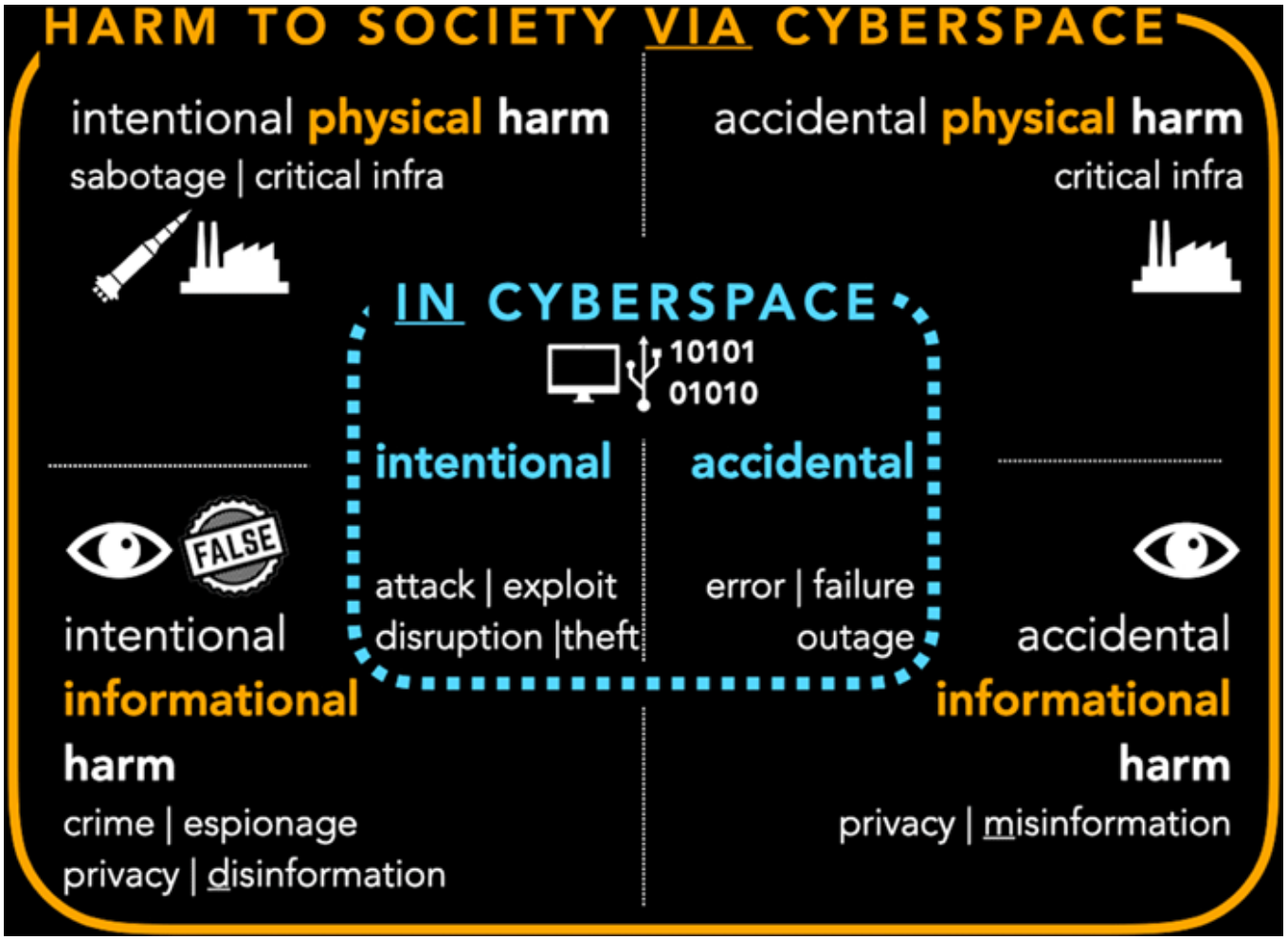

Figure 2. The cyber harm model.

The abuse of vulnerabilities in and of cyberspace may cause two different types of harm: (a) harm to systems, data, and networks, which we collectively label as *harm in cyberspace*; and (b) harm to human beings, institutions, values, or societies, which we collectively label as *harm via cyberspace*.

Cyber Incidents in Cyberspace: Harms to Systems, Data, and Networks

The middle of Figure 2 presents "harm *in* cyberspace": all forms of damage done to technical systems, to networks, software, hardware, and to data that is shared via, or stored in, cyberspace. Currently, much research on and debates about cybersecurity focus on this type of harm. Studies focus on the potential risk of losing data, opening communications to unintended audiences, and networks becoming unavailable. Systems and data that are attached to or available in cyberspace may be damaged, stolen, manipulated, broken, attacked, exploited, and so on. Because this may lead to loss of data, reputational damage, economic damage, and loss of trust, there is a real and realistic concern over such forms of harm.

In cybersecurity, therefore, much effort has been put into the "CIA Triad," that is, into protecting the confidentiality and the integrity of data, and the availability of networks and systems (cf. Meeuwisse, 2017; Schneier, 2018; Van den Berg & Keymolen, 2017). Confidentiality refers to the fact that data and communications must be kept secure while in transit and in storage. Integrity revolves around the idea that we must be able to rely on the fact that data has not been tampered with, for example, it has not been changed, manipulated, or moved. Availability means that networks and systems must be reliable: They must be resilient enough to remain accessible even under adverse conditions.

One important thing to note about the discussion on harm in cyberspace is that almost all current research and policymaking concentrates on intentional threats to maintaining the confidentiality and integrity of data and systems and the availability of networks and systems. Governments, businesses, and academics all seek to gain a better understanding of the risks of willful exploitation of vulnerabilities in cyberspace and to generate protections against such exploitation. However, while the threat of intentional attacks is real and widespread, systems, data, and networks may also be harmed as a result of unintentional or accidental causes. This type of harm receives far less attention from governments, businesses, and researchers. Unintentional harm in cyberspace may result from a natural disaster,[4] system error,[5] a configuration error,[6] or a human error.[7] Moreover, accidental or unintentional cybersecurity incidents may sometimes also be the result of mistakes or errors elsewhere. In this case, a cybersecurity incident can be labeled a cascading effect. The most common materialization of this cascading effect is when power systems go down, and as a consequence, networked, digital systems fail as well.[8] It is clear that for crisis-management purposes, it is not so relevant whether the source of cyber harm is intentional or accidental; in case of a cyber crisis, harm has exceeded a certain threshold and requires an urgent response. Whether or not this harm was generated willfully or, for instance, as a result of natural causes is less important in the moment of an escalating crisis; this is more relevant when the peak of the crisis has passed, and it is time to gain a deeper understanding of the causes to learn from that crisis. For crisis-management purposes, therefore, it would be worthwhile if cybersecurity research expanded its scope to include accidental cyber incidents because these can be, and are, a real source of concern alongside intentional threats.

A second important thing to note about harm in cyberspace is that it leads to what the authors call *indirect* harm to humans. As argued elsewhere:

> The terms “direct” and “indirect” refer to the *first* locus of the manifestation of a harm. Direct harms are harms that manifest themselves directly in or on a human being. Indirect harms, by contrast, are harms that first manifest themselves outside human beings, in their possessions, in other people, in the larger environment in which they operate, or in relation to core values and institutions that they hold dear, and that affect human beings through the damaging effects they have on those possessions, people, core values or on the environment.
>
> (Van den Berg et al., 2021, italics in original)

When systems, networks, or data are manipulated, attacked, exploited, damaged, plundered, or disrupted, this does not harm humans directly in the sense described earlier. Instead, it harms the things they value—financially, economically, socially, as well as in terms of efficiency. Of course, this does not make it any less serious. The damage that is done in cyberspace to systems and data can be significant.

Cyber Incidents via Cyberspace: Harm to Humans and Societies

One of the most troubling realizations in relation to the exploitation of vulnerabilities in, and of, cyberspace, is that these may also lead to harm outside cyberspace, that is, in the offline world. We call this category harm *via* cyberspace. In Figure 2 it is represented by the outer ring. Some of the harm that may be done via cyberspace came up already in the discussion of risks surrounding cyber physical systems and critical infrastructures. What characterizes harm via cyberspace is that activities conducted in cyberspace (hacking, sabotage, theft, disruption, as well as errors of a variety of different kinds) may have real-world effects, that is, they may lead to different types of harm in the physical world outside cyberspace.

The first thing to note is that the distinction between direct and indirect harm is also relevant when we speak of harm via cyberspace. For one, this type of harm may befall human beings, organizations, institutions, and societies directly: They may come to direct physical harm as a result of manipulations of systems or data in cyberspace. As the example on critical infrastructures illustrated, when a hacker opens a dam and floods an area, this may lead to large-scale physical harm, including potential deaths, in our physical reality. Direct harms via cyberspace can be found in the upper half of Figure 2.

But harm via cyberspace may also befall human beings, organizations, institutions, and societies indirectly: They can experience harm because their data is stolen (emotional/mental harm), or their money is stolen after their credit card data were leaked (financial harm), or they become a victim of disinformation (willful) or misinformation (by mistake). In this case, the harm is not done to their bodies or minds directly, but to the “things” (whatever those are) that they hold dear. This category of harms can be called *informational harms*, and they occupy the bottom half of Figure 2. Note that privacy harms and misinformation and disinformation are labeled as informational harms because these harms are generated using the content layer of cyberspace. These harms are the result of information that is willfully or

accidentally shared or manipulated. This is different from harm to data. “Data” here refers to the 1s and 0s of cyberspace, not the meaningful content that a combination of 1s and 0s may give rise to when interpreted by human beings. Of course, harms to data (in cyberspace) may give rise to mental or emotional harms (via cyberspace), for instance when data theft leads to privacy intrusions or financial harm for end users. But note that this need not be the case! When (personal) data gets stolen (harm in cyberspace), end users may not even know and may suffer no (noticeable) effects from this theft. In such a case, there is harm in cyberspace (data stolen), but no harm via cyberspace (privacy violation).

Second, as was the case with harms in cyberspace, Figure 2 shows that harms via cyberspace may not only be the result of the intentional actions of others but also the result of unintentional events. As before, here too, most efforts by governments, businesses, and academics are targeted at understanding, preventing, and mitigating the former while less attention is given to the latter, although governments are increasingly aware of the potentially disruptive consequences of accidental cyber incidents or crises (NCSC, 2021). There are grave concerns regarding the risks surrounding cyber physical systems, especially where these have the potential to generate severe economic, societal, and physical harm should they be exploited willfully by actors with bad intentions. It is wise that critical infrastructure protection receives this level of attention because incidents may have significant and large-scale impact. At the same time, it is unfortunate that less attention is paid to the direct and indirect effects of accidental and unintentional incidents via cyberspace because their physical impact may be no less harmful than that of intentionally caused ones. Ultimately, when a crisis emerges that is caused via cyberspace and leads to severe physical damage or even death, it does not matter much—especially immediately after the triggering event(s)—whether the crisis was caused by sabotage or by an outage. The impact may be as grave. Failures of modern-day technical systems have been an object of study for several decades now in safety science (cf. Aven, 2014; Hopkins, 2014) and for those interested in normal accidents (Perrow, 1984) and high-reliability organizations (Bundy et al., 2016; Weick et al., 2008). Unfortunately, that such failures can be caused in cyberspace and have effects in the physical world remains understudied. The risk thereof is grave and realistic. A critical infrastructure, such as a storm surge, may be opened or closed at will as a result of a hack, but this may equally occur as a result of a faulty software update, a human error, or a network error via cyberspace.

Blurred Lines

A final word on the cyber harm model: Please note that the distinction between harm *in* cyberspace and harm *via* cyberspace is not always or necessarily as binary as represented here. Incidents that start in cyberspace may have spill-over effects causing harm in the physical world—hence the dotted line surrounding the central ring in Figure 2. Similarly, incidents that are willfully instigated in cyberspace may have intentional effects inside and via cyberspace, yet they may also lead to unintentional, accidental (side-)effects. Alternatively, malicious actors may pick up accidents and errors seeking to exploit them (further), thus leading to intentional harm. This explains the dotted lines between the left and the right side

of said Figure 2. Finally, exploiting vulnerabilities in or via cyberspace may sometimes lead to both physical and informational harm. One case in which this happened was the 2012 cyberattack on Saudi Aramco, the Saudi Arabian oil and gas company (cf. Onyeji et al., 2014).[9] This company became the victim of a malware infection, which wiped 30,000 computers partially or overwrote their master boot records—the digital equivalent of destroying them physically. Luckily, the malware did not reach "industrial control system computers involved in drilling or refining operations" (Bronk & Tikk-Ringas, 2013, p. 86). Despite this fact, with respect to all its administrative processes, the company was instantly thrown back into the age of typewriters and faxes for a number of weeks. The only way to overcome this attack was to buy new equipment and throw out the old computers. This is an example of a cyberattack that was instigated in cyberspace but ultimately resulted in physical harm via cyberspace. However, that is not where this story ends. In the aftermath of the incident, it turned out to be difficult, at first, to establish who had initiated this attack. In an attempt at sowing confusion, two groups claimed responsibility. One was a group that called itself the Cutting Sword of Justice, the other was merely described as an "'anti-oppression' hacker group" (Bronk & Tikk-Ringas, 2013, p. 88). Security experts doubted their claims and pointed a finger at Iran, which had both the motive and the means to attack Saudi Arabia's oil and gas company. Iran's motive, experts argued (cf. Dehlawi & Abokhodair, 2013), was retaliation for the Stuxnet malware, which set back the country's nuclear enrichment program by several years through a cyberattack at its nuclear facility in Natanz (cf. Farwell & Rohozinski, 2011; Kello, 2013; Lachow, 2015; Zetter, 2014). Stuxnet is widely claimed to be a joint product of the United States and Israel, and in this light, it is not surprising that an oil company owned by one of their allies would be attacked by Iran. Moreover, Iran's oil sales suffered heavily from international sanctions against the country, while Saudi Arabia produced more oil because of them, thus strengthening the motive to attack further (Bronk & Tikk-Ringas, 2013). Iran also had the means: In response to Stuxnet, Iran had invested heavily in developing its own offensive cyber capabilities and even created an "official Cyber-warfare Division under the Islamic Revolution Guards Corps" (Dehlawi & Abokhodair, 2013, p. 74). Later on, leaked NSA documents confirmed Iran's alleged role in the Saudi Aramco cyberattack (cf. Alelyani & Kumar, 2018). The cover story generated by the two hacker groups that claimed responsibility can be considered a form of disinformation, a willful attempt at complicating attribution. Disinformation is a form of intentional informational harm via cyberspace. Taken as a whole, then, the Saudi Aramco cyberattack of 2012 is an example of harm via cyberspace of two kinds: It began with cyberattack that created physical harm to the companies' systems, and it was followed by informational harm through a disinformation campaign seeking to throw security experts off Iran's scent. This is why Figure 2 presents a dotted line between physical harm and informational harm.

Cybersecurity Crises: Key Characteristics

While cybersecurity incidents are often in the news, it is difficult to establish what constitutes a cybersecurity crisis. Boin et al. argue a crisis is "when a social system—a community, an organization, a policy sector, a country, or an entire region—experiences an urgent threat to its basic structures or fundamental values, which harbors many 'unknowns' and appears to

require a far-reaching response" (2005, p. 5; also see Rosenthal et al., 1997). But what kind of uncertainty is involved in cybersecurity crises? Why and under which conditions do they evoke a sense of urgency, and for whom? And which values are at stake when a cybersecurity incident may turn into a cybersecurity crisis?

Cybersecurity Crises Involve Uncertainty and Ambiguity

To begin with the first question: It is clear that cyber crises involve uncertainty and ambiguity in myriad ways. First, cybersecurity incidents can come from anywhere, and due to the makeup of digital action can sow immediate (near) real-time effects. Moreover, activities in cyberspace are almost always transboundary in their consequences (Ansell et al., 2010; Boin, 2009). Cyberspace connects the globe, and this means that incidents in and via cyberspace can be caused or instigated in one place but may have effects in very different places, without time delay. This makes cybersecurity crises fundamentally different from, let's say, an upcoming weather event or a kinetic attack with a long-range missile. In the latter cases, because the source and the trajectory of the impending doom are clear, it is possible to engage in activities to mitigate (at least some of) the potential consequences before its arrival. One can board up homes with storm shutters to prepare for a hurricane or launch anti-ballistic missiles to intercept an incoming projectile. Aside from knowing the source and trajectory of a threat, one other essential parameter here is time: There is a time delay between the buildup of a hurricane or the launch of a missile and its arrival at its destination. In cybersecurity crises these factors are usually absent. Those potentially effected generally lack the knowledge that a large-scale incident is unfolding, lack the knowledge where the incident is coming from, and lack the time to mitigate or prepare because there is no delay between the instigation of a cybersecurity threat or accident and its impact. Combined, these characteristics of cybersecurity crises lead to two uncertainties: Once a cybersecurity crisis materializes, it is often incredibly difficult to establish what is going on, and who or what caused this crisis. Without knowing the answer to both questions, it is difficult to respond. Finding answers to these questions, moreover, is technically challenging and time-consuming (Golandsky, 2016). Due to the interconnectedness of systems and the global character of cyberspace, it may take weeks or months to unravel what caused a crisis and how it unfolded or even to return to (some semblance of) normality. Finding the actual source of a crisis and pointing a finger at a specific actor who is responsible for it, that is, attributing it, are even more difficult.

Yet another aspect that causes uncertainty in cybersecurity crises is that such crises can morph over time. Vulnerabilities may not be detected, sometimes for a very long time. The same goes for incidents themselves: Both accidents and incidental attacks may remain undetected as they lead to incidents, and they only become noticeable once they escalate to the point of a crisis. This leads to a high degree of uncertainty for decision makers: It means they can be confronted with a large-scale crisis in an instant.

And finally, it is not always clear when or whether a cybersecurity crisis is resolved. While organizations and sectors may be able to bounce back from incidents and resume their normal operations, as long as the root cause lives on and vulnerabilities are not (adequately) remedied, symptoms may have been addressed, but the next crisis may be just around the corner.

Cybersecurity Crises Lead to a Sense of Urgency

In the description of Boin et al. (2005), crises are also events characterized by a high degree of urgency. Does this also apply to cybersecurity crises? This question can be answered using the cyber harm model. In this model two types of incidents are distinguished: those that lead to harm *in* cyberspace, and those that start in cyberspace but then lead to harm *outside* cyberspace in the offline world. The latter were labeled cyber physical incidents. Both types of harm can lead to severe crises, but of different kinds. An example of a crisis in cyberspace was the 2016 SWIFT hack, also known as the Bangladesh Bank Robbery. SWIFT is a trust service: It enables financial institutions to share information about bank transfers and requests in a secure environment; when banks are asked to transfer large sums of money, they use SWIFT to ensure that the requests are trustworthy. In 2015 and 2016 the SWIFT system was hacked; attackers obtained legitimate SWIFT credentials and could thus order large sums of money to be sent to different bank accounts, without anyone noticing until US$101 million had already been stolen (Zetter, 2016). Only US$18 million of that money has been recovered.

An example of a crisis via cyberspace is the NotPetya attack in 2017. On June 27 of that year, Russia engaged in a cyberattack seeking to wipe the systems of a large number of different elements in Ukraine’s critical infrastructure, including banks, airports, and gas and electricity companies; ministries; Ukraine’s National Bank; and one of its nuclear power plants. Russia has been using cyber-offensive capabilities for years to enhance the impact of its ongoing offline conflict with Ukraine. What set this attack apart, however, was that the malware used did not stay in Ukraine. It spread around the globe like wildfire, and it affected entire companies in a matter of minutes. It had a severe impact on parties that had nothing to do with the Russian-Ukrainian conflict. Once it left Ukraine, its path of destruction seemed completely random. The malware even bounced back and affected the Russian state oil company Rosneft. Considered the most devastating cybersecurity incident of all times, it caused approximately US$10 billion in damage worldwide (Greenberg, 2018). Large international companies, such as the international shipping company Maersk and the European affiliate of FedEx, TNT Express, were affected. Maersk saw 17 of its 76 terminals worldwide go offline entirely and could no longer do business for more than a week after its systems were wiped and networks went offline. It took the company many months to recover completely.

The sense of urgency in both examples is obvious. In the example of the SWIFT hack a large sum of money simply evaporated. But more importantly, trust was undermined in a banking service that was used by millions of banks around the globe—one that was designed and used to facilitate trust. In the example of NotPetya, the sense of urgency stemmed from the fact that the spread of malware in cyberspace could have worldwide, severe consequences in the

offline world for global companies, whose entire operations ground to a halt. It took time to understand that this was the result of a conflict in a faraway place to which these companies were no party at all. The sense of urgency in crises like these, then, is about the realization that modern-day companies are entirely dependent on ICT networks and technologies for their functioning, and that in an interconnected world this dependency can lead to crises that are crippling, difficult to solve, and affect an entire company or even an entire sector.

In a Cybersecurity Crisis High and Conflicting Values Are at Stake

A final characteristic of crises, according to Boin et al. (2005), is that in crises there are high and conflicting values at stake. They argue that "crises occur when core values or life-sustaining systems of a community come under threat. Think of widely shared values such as safety and security, welfare and health, integrity and fairness, which become shaky or even meaningless as a result of (looming) violence, destruction, damage, or other forms of adversity" (Boin et al., 2005, pp. 2–3). While researchers point out that a large-scale "digital Pearl Harbor" has not materialized yet in the early 2020s despite severe warnings (Brito & Watkins, 2011; Deibert & Rohozinski, 2010b; Dunn Cavelty, 2008), at the same time it is clear that in a world where interconnectedness and reliance on digital, networked technology is only increasing, it is likely that severe cybersecurity crises will materialize at some point in the future. When they do, core values such as safety and security may come under pressure, especially when crises instigated or caused in cyberspace lead to severe harm, even death and destruction, outside cyberspace, as may be the case in cyber-physical events. But cybersecurity crises may not just be about physical harm, as the cyber harm model shows. They may also generate what the authors call informational harms, which, in some cases, may affect core values of society. One clear example is disinformation campaigns aimed at influencing election outcomes (Schneier, 2018). The 2016 US presidential elections raised awareness around the globe that cyberspace can be used to influence people's voting behaviors by sending them fake news via social media, among others ways. Since then, scientists and policymakers alike have pointed out that meddling with elections has a fundamental impact on the foundations of democratic states and that it is urgent to find a response to this threat (Maurer, 2018a). A cybersecurity crisis such as election interference affects fundamental values such as freedom, integrity, and fairness.

Unfortunately, one of the tricky aspects of cybersecurity crises is that while they undermine certain important values, at the same time, often to (re)solve or prevent the crises, competing values of equal importance appear to have to be sacrificed. One obvious example is the tension between security and privacy: For the collective to be secure online or for security in cyberspace to be restored, the privacy of individuals must be sacrificed, or so the reasoning goes (Chandler, 2009; Taipale, 2004). This involves granting special privileges to law enforcement and allowing (or at least not curbing) surveillance of internet traffic and behavior. While privacy, in a sense, is about the security of and for the individual, in times of crisis this sense of security is often sacrificed for the greater good, thus generating a tension between two core values in Western societies.

Managing Cybersecurity Crises

What are the implications of the characteristics of cybersecurity crises for the management of such crises? From the previous sections one may deduce that managing cybersecurity crises is difficult. For one, the essence of the threat in relationship to cyberspace is not straightforward: The cyber harm model shows that harms generated in or via cyberspace may manifest themselves in a variety of ways, and they may be directed at different parties or targets. The source of incidents, their scope, and their consequences are often (partly) invisible and ill-understood. Because cybersecurity crises are transboundary, they often affect multiple jurisdictions. Moreover, they require public-private cooperation, they may undermine the functioning of policy sectors, and they may escalate in unforeseen directions (Kuipers & Boin, 2015, p. 193). Multiple stakeholders in multiple functional domains at different levels of government may become involved in managing crises caused in or via cyberspace, leading to challenges for communication and collaboration, but also with respect to mandates and responsibilities.

An extra complicating factor is the fact that cyberspace as an ecosystem is not a public space. Instead, the vast majority of all the infrastructural elements that make up cyberspace, be they networks, systems, platforms, or software, are privately owned (Deibert & Rohozinski, 2010a; Schneier, 2018). At the same time, governments have responsibilities to keep cyberspace safe and secure. Risks to cybersecurity can constitute threats to national security (Brito & Watkins, 2011; Chandler, 2009; Dunn Cavelty, 2013) because cyber incidents may lead to loss of life when critical infrastructures are exploited (Alcaraz & Zeadally, 2015; Aradau, 2010; De Bruijne & Van Eeten, 2007; Gheorghe et al., 2007) or because the societal and economic value of cyberspace, itself a key infrastructure in many societies, is too great (Broeders, 2015, 2017; Deibert & Rohozinski, 2010b).

To fulfill the obligation to provide for a safe and secure cyberspace, governments and other public parties must collaborate closely with a wide variety of private parties, who they depend on not only for technical skills and expertise but also for data on the “state of affairs” in relation to (the security of) the systems, platforms, and networks these private parties manage, own, operate, or oversee. This is true under conditions of normalcy, yet all the more so in times of crisis. Public-private partnerships are generally considered the only feasible route for the adequate protection of security in and via cyberspace (Czosseck, 2013; Luiijf & Besseling, 2013), although some have reservations over potential clashes between public and private interests (Dunn Cavelty & Suter, 2009), which, notably, may materialize most clearly in times of crisis.

Typical for cybersecurity incidents is the interdependency among actors involved. As the causes of the incident may fall outside a country’s domain, crisis managers may seek to collaborate with the state or organization from which the incident originated, for example to stop it, to mitigate further incidents, or to engage in prosecution of perpetrators. Moreover, preventative or recuperative mechanisms (both in the form of expertise and technical tools) may be available in other jurisdictions and may help states bounce back after a crisis. Framed

in Thompson's tripartite of interdependencies one could argue that with respect to cyberspace, jurisdictions largely have reciprocal interdependence (discussed in Ansell et al., 2010, p. 197; Thompson, 1967).

Due to the networked character of cyberspace, actors responsible for cybersecurity need one another to stay safe and to respond adequately and effectively to cyber-induced crises. Collaboration between states, for example information exchange, is therefore essential. However, this is easier said than done. Where complex crises always suffer from difficulties in coordination, once they become transboundary and cross-border, the complexity of coordination and collaboration increases manifold. To paraphrase Ansell et al., under these conditions responsibilities become murky and ever-larger numbers of actors need to be coordinated—after all, "the number of interaction relations rises exponentially" (Ansell et al., 2010, p. 199). Ownership in times of crisis will most certainly be a particular challenge for cyber-related crises because the transboundary crisis response will involve a network of actors in which allocation of responsibility and accountability is highly unclear (Boin, 2009, p. 373).

Examining the core tasks of leadership in crises, here defined as sense-making, decision making, and meaning making (Boin et al., 2016), cybersecurity incidents have specific implications for crisis managers. Sense-making is developing a shared understanding based on recognition from vague, ambivalent, and contradictory signals that a crisis is unfolding and how it is evolving. Decision making pertains to detecting the key strategic decisions and to address these at the appropriate level of authority and competence, meanwhile coordinating with other stakeholders. Meaning making implies that crisis leaders reduce uncertainty by communicating and providing an authoritative account of what is going on, why it is happening, and what legitimizes the proposed response (Boin et al., 2016).

Sense-Making

Sense-making on security crises in cyberspace, that is, with respect to harm done to systems, data, and networks, is impeded by the complexity of the infrastructure, both the hardware and the software of systems. This infrastructure is layered and multifaceted, and so many different systems are used at the same time—each with their own vulnerabilities and distributed over locations, devices, and platforms—that it is difficult to monitor adequately whether anything is amiss, and if so, where or what exactly. Moreover, incidents may take place surreptitiously, which makes it difficult to detect that anything is amiss. Data theft or unwanted disclosure of data, for instance, often go undetected, sometimes for months on end, because perpetrators have unobtrusively gained access. In the offline world, the theft of property means that the owner no longer has the physical object. In cyberspace, data are stolen by making a copy of them. The offender now has the data, but so does the owner.[10] Hence, it is far harder to detect that theft has taken place.

What this means is that, in the case of harm to systems/data, an incident may be underway for a long time and developed into something very large (in terms of impact or scale or both) before anyone realizes something is amiss. An example is the 2017 Marriott data leak. In this leak, the data included names, telephone numbers, addresses, gender, date of birth, passport numbers, and credit card numbers of more than 500 million customers and were stolen from one of the reservation systems of the hotel chain. By the time the Marriott hotel chain discovered the data leak, it had been going on for 4 years.

Sense-making is also particularly difficult with respect to those crises where incidents manifest themselves via cyberspace. Such incidents have their origins in cyberspace but cause effects in the offline world. In terms of sense-making, it means that the connection needs to be made between harmful effects generated in the real world and their digital root causes. Hence, a crisis may be misjudged as originating in some place or being caused by a certain system or person, when it was caused somewhere entirely different and by one or more other actors. In addition, deliberate efforts to create confusion by disinformation further obfuscate causes and origins of the problem. The Saudi Aramco cyberattack of 2012 discussed previously illustrates that a cyber crisis can have both informational and physical security dimensions and that it can originate in a complex geopolitical conflict.

Crisis managers need to adapt their sense-making toolbox to deal effectively with the specific characteristics of cyber crises. Several cases illustrate the importance of incorporating awareness and ability to identify intentional disinformation on the source, motivation, and agent behind a cyber threat or crisis. Structural disconnects between cause and effect in terms of timing, geographic location, and functional domain seem to be the new normal. Yet sense-making and the creation of a common operational picture by crisis and disaster responders usually takes place within a geographically defined network of actors, with a specialized professional background (medical, military, law enforcement, engineering), that does not include cyber expertise or awareness and already is in dire need of more reflexivity (Wolbers & Boersma, 2013).

Decision Making and Crisis Response

Decision making and ownership of a cyber crisis is also particularly challenging due to the networked nature of cyberspace. Containment of crises is a challenge as those suffering the consequences are rarely the ones holding the key to its solution. Because systems are massively interconnected, software is shared globally, and networks connect geographical locations worldwide, once a cyber incident occurs it may spread far and wide. The NotPetya incident is an example. In terms of crisis decision making, this means that the level of authority and competence for the response has truly gone global and decentralized at the same time. Consequently, existing security networks—usually based on geographic regions and historical ties between centralized public authorities in specific countries—are of limited help. Parties need to share both information and capabilities to collectively increase preparedness for cyber incidents. In this light, private and public sector organizations around the globe have started to collaborate in cyber emergency response teams (CERTs). Such

collaborations are challenging in several respects. First, bridging cultures and ways of working among public and private parties in CERTs is not always straightforward. Political executives and administrative chiefs need to find a way to deal with the autonomy of (technical) cyber experts that do their work “legal-ish” and cooperate beyond established institutional frameworks (LaPorte, 2018, p. 270). Moreover, finding a common language and understanding the widely differing interests that drive technical experts and government officials is a challenge to be overcome. A high degree of professional expertise combined with decentralized authority and mandates to cooperate in transboundary crises are required to nip cybersecurity emergencies in the bud and forge a real-time response. The European Commission, among others, has invested heavily in detection and sense-making capacity related to cybersecurity, which contrasts remarkably with a much less developed decision making and coordination structure in this policy area (Backman & Rhinard, 2018).

A second challenge that requires further development is the creation and implementation of regulation. On the regional and national levels, there is the emergence of regulations to address particular sets of cybersecurity risks, but regulatory frameworks need to be expanded, both in scope and in range. While regulation tends to lag behind technological developments, at the same time it is essential to curb the spread of insecure technologies and, hence, to prevent potential future crises. At the international level, for now the focus is on debating norms for state behavior (Finnemore & Hollis, 2016; Nye, 2014), which may contribute to reducing the risk of, for example, attacks on critical infrastructures, and further down the line maybe even reduce espionage.

Within single organizations, cyber crises can blind decision makers when the information necessary to support decision making or to overcome the crisis has become unavailable. The operational response to the consequences of cyber incidents is impeded by the fact that hardcopy or nondigital alternatives are no longer available and the means of communication are often affected by the very same ICT-problem. For instance, when computer systems go down in hospitals, this may threaten patient safety when surgeries or treatments have to be cancelled because the electronic patient records that provide doctors and nurses with the necessary information are no longer accessible or because medical equipment—potentially even life-support systems—may no longer work.[11] Meanwhile, other hospitals cannot take over because they need the same electronic records to provide appropriate and safe care to transferred patients, or they may be suffering from the same cyber incident. Offline backups and decoupled systems are then key to regain insight in crucial medical information and provide appropriate care. The approach to downscaling operations and prioritizing work (a form of “triage”) with reduced capacity is similar to business continuity in other types of crises.

Meaning Making

The crisis leadership task most complicated by cybersecurity problems is perhaps meaning making. Providing an authoritative account is almost impossible given the multiple stakeholders and jurisdictions (without hierarchical relation to each other) involved. Reducing

uncertainty and helping people understand what is going on and why are extremely difficult when the origin of the crisis is invisible, its consequences are unpredictable and perhaps ongoing, and culpability is obfuscated. In other types of crises, an extreme event exposes security breaches or safety problems that can be visibly addressed—an airport can be guarded, a levee or seawall can be constructed, a vaccination can be provided. Moreover, extreme events are opportunities for policy exploitation: Reform-oriented actors can mobilize support for new policy directions (Birkland, 2006; Boin et al., 2009). The reform rhetoric can go hand in hand with an attempt to channel emotions and turn a dreadful incident into positive steps for the future. New Zealand's Prime Minister Jacinda Ardern's strong and successful plea for gun control after the Christchurch attack in 2019 illustrates this. Terrorist attacks also usually lead to political calls for solidarity and embracing the values of freedom and justice for all. Leaders from neighboring states or communities can join the choir and stand by each other. The traits of cyber crises highly complicate all of this. Particularly security incidents in cyberspace that do not lead to direct harm outside cyberspace for people and what they value are often hard to understand for a lay audience, including political executives and policymakers. The sense of urgency and the threat awareness may differ significantly between experts and amateurs. For cyber incidents via cyberspace, the harm is more obvious, but the causes are so difficult to understand that providing assurance is nearly an impossible task.

When leaders are grasping for simplifications to provide a narrative on cyber-induced crises that people actually understand, they tend to unjustly employ metaphors from physical crises and tangible threats. "Cyber Pearl Harbor," "cyberterrorism," and "cyber meltdown" are just a few illustrations that seldom do justice to a much more complex reality. Meanwhile, a strong divide emerges between those cyber experts who warn a cyber apocalypse is looming because of the sheer characteristics of interconnectedness and complex interaction and those who point to the resilience of cyberspace and the fact there is little to no evidence for complete system breakdowns. Their debate resembles the opposite positions in the organizational crisis literature on "normal accidents" (Perrow, 1984, 1994) on the one hand and "high reliability" on the other hand (LaPorte, 1994, 1996). A positive consequence might be that the younger field of cybersecurity governance can benefit from insights that resulted from the high-reliability debate and ways to resolve it (Rijpma, 1997; Sagan, 1994). For meaning making, resolving the debate on cyber threats and high reliability may offer crisis managers a better vocabulary and metaphors that do justice to the real nature of the cyber incidents and threats, which help provide people with assurance, understanding, and actionable advice.

Lessons on Cyber Crisis Management

This article has revealed that cyber-related incidents may lead to crises of a wide variety, with harm that may sometimes be contained to cyberspace (harm done to data, systems, and networks) but sometimes also to humans, institutions, physical (infra)structures, and so on outside cyberspace. While both types of incidents may lead to crises, they are crises of a very different kind. For crisis managers, the challenges of cyber-induced crises are significant and wide-ranging. Currently, scholarship and practice lag behind an understanding of and

capabilities for (dealing with) cybersecurity incidents. In the upcoming years, public and private parties will have to invest time and effort to get ahead of the curve for these types of incidents. Cyberspace is changing rapidly and becoming an ever-more essential backbone for our modern-day world. This not only brings great benefits but also requires society to get a better handle on the most complex system humankind has ever created.

Acknowledgments

The authors thank Christine Boelema Robertus for gathering and processing the data provided in notes 9–12.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Whitfield, D., Gilmore, J, Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M. A., & Weitzner, D. J. (2015). *Key under doormats: Mandating insecurity by requiring government access to all data and communications*.

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53–66.

Alelyani, S., & Kumar, H. G. R. (2018). Overview of cyberattack on Saudi organizations. *Journal of Information Security and Cybercrimes Research*, *1*(1), 42–51.

Anderson, M. (2019, 14 March 2019). Facebook says outages due to 'server configuration change' *<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fapnews.com%2Farticle%2F5b0605282cf041cabdfa6727e76be0b6&data=04%7C01%7Cs.l.kuipers%40fgga.leidenuniv.nl%7Ca08e89b012d4454bc88608d9c64e9f12%7Cca2a7f76dbd74ec091086b3d524fb7c8%7C0%7C0%7C637758863255368645%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=ntnHzOKFzC5b15%2B9Bnj2raUy%2ByI5aZNmXEox1ZNRocA%3D&reserved=0>*. *AP News*.

Ansell, C., Boin, A., & Keller, A. C. (2010). Managing transboundary crises: Identifying the building blocks of an effective response system *<http://dx.doi.org/10.1111/j.1468-5973.2010.00620.x>*. *Journal of Contingencies and Crisis Management*, *18*(4), 195–207.

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, *41*(5), 491–514.

Aven, T. (2014). What is safety science? *<https://doi.org/10.1016/j.ssci.2013.07.026>* *Safety Science*, *67*(0925), 15–20.

Backman, S., & Rhinard, M. (2018). The European Union’s capacities for managing crises. *Journal of Contingencies and Crisis Management*, *26*(2), 261–271.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cybersecurity <https://doi.org/10.1017/eis.2016.8>. *European Journal of International Security*, *1*(2), 176–198.

Ben-Israel, I., & Tabansky, L. (2011). An interdisciplinary look at security challenges in the information age. *Military and Strategic Affairs*, *3*(3), 21–37.

Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world <https://doi.org/10.1145/2382196.2382284>. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security—CCS'12* (pp. 833–844). ACM.

Birkland, T. (2006). *Lessons of disaster: Policy change after catastrophic events*. Georgetown University Press.

Böhme, R. (2005, December 27–30). Vulnerability markets: What is the economic value of a zero-day exploit? [Paper presentation]. In *Proceedings of 22C3*, Berlin, Germany.

Boin, A. (2009). The new world of crises and crisis management: Implications for policymaking and research. *Review of Policy Research*, *26*(4), 367–378.

Boin, A., 't Hart, P., & McConnell, A. (2009). Crisis exploitation: Political and policy impacts of framing contests. *Journal of European Public Policy*, *16*(1), 81–106.

Boin, A., 't Hart, P., Stern, E., & Sundelius, B. (2005). Crisis management in political systems: Five leadership challenges. In A. Boin, P. 't Hart, E. Stern, & B. Sundelius (Eds.), *The politics of crisis management: Public leadership under pressure* (pp. 1–17). Cambridge University Press.

Boin, A., Stern, E., & Sundelius, B. (2016). *The politics of crisis management: Public leadership under pressure*. Cambridge University Press.

Brenner, S. W. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law and Criminology*, *97*(2), 379–476.

Brito, J., & Watkins, T. (2011). Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. *Harvard National Security Journal*, *3*(1), 39–84.

Broeders, D. (2015). *The public core of the internet: An international agenda for internet governance*. WRR.

Broeders, D. (2017). Defining the protection of "the public core of the internet" as a national interest. *ORF Issue Brief*, *190*, 1–8.

Broeken, A. (2018, December 18). Elektronisch patiëntendossier Beatrixziekenhuis gaat plat: afspraken afgezegd <https://www.ad.nl/rivierenland/elektronisch-patientendossier-beatrixziekenhuis-gaat-plat-afspraken-afgezegd~a7ea574d>. *AD*.

Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco <https://doi.org/10.1080/00396338.2013.784468>. *Survival*, *55*(2), 81–96.

Bryce, J., & Klang, M. (2009). Young people, disclosure of personal information and online privacy: Control, choice and consequences. *Information Security Technical Report*, *14*(3), 160–166.

Buchan, R. (2015). Cyber espionage and international law. In N. Tsagourias & R. Buchan (Eds.), *Research handbook on international law and cyberspace* (pp. 168–189). Edward Elgar.

Bundy, J., Pfarrer, M., Short, C. E., & Coombs, T. W. (2016). Crises and crisis management: Integration, interpretation, and research development. *Journal of Management*, *43*(6), 1661–1692.

Cárdenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009, 23 July). *Challenges for securing cyber physical systems* [Paper presentation]. Workshop on Future Directions in Cyber-physical Systems Security, Department of Homeland Security.

Chandler, J. (2009). Privacy versus national security: Clarifying the trade-off. In I. R. Kerr, C. Lucock, & V. Steeves (Eds.), *Lessons from the identity trail* (pp. 121–138). Oxford University Press.

Chesterman, S. (2006). The spy who came in from the Cold War: Intelligence and international law. *Michigan Journal of International Law*, *27*, 1071–1131.

Clark, D. D., & Landau, S. (2011). Untangling attribution. *Harvard National Security Journal*, *2011*, 25–40.

Contreras, J. L., DeNardis, L., & Teplinsky, M. (2013). Mapping today's cybersecurity landscape. *American University Law Review*, *62*, 1113–1131.

Czosseck, C. (2013). State actors and their proxies in cyberspace. In K. Ziolkowski (Ed.), *Peacetime regime for state activities in cyberspace* (pp. 1–29). NATO CCD COE.

De Bruijne, M., & Van Eeten, M. (2007). Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management*, *15*(1), 18–29.

Dehlawi, Z., & Abokhodair, N. (2013, June 4–7). *Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident* [Paper presentation]. IEEE International Conference on Intelligence and Security Informatics.

Deibert, R. J. (2011). Towards a cyber security strategy for global civil society? *Global Information Society Watch*, 23–26.

Deibert, R. J., & Rohozinski, R. (2010a). Liberation vs. control: The future of cyberspace <https://doi.org/10.1353/jod.2010.0010>. *Journal of Democracy*, *21*(4), 43–57.

Deibert, R. J., & Rohozinski, R. (2010b). Risking security: Policies and paradoxes of cyberspace security <https://doi.org/10.1111/j.1749-5687.2009.00088.x>. *International Political Sociology*, *4*(1), 15–32.

Demchak, C. C., & Dombrowski, P. (2011). Rise of a cybered Westphalian age. *Strategic Studies Quarterly*, *5*(1), 32–61.

Dunn Cavelty, M. (2008). Cyber-terror: Looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*, *4*(1), 19–36.

Dunn Cavelty, M. (2019). Cyber-security. In A. Collins (Ed.), *Contemporary security studies* (4th ed., pp. 410–427). Oxford University Press.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*, 105–122.

Dunn Cavelty, M., & Suter, M. (2009). Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *4*(2), 179–187.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy *<https://doi.org/10.1016/j.jare.2014.02.006>*. *Journal of Advanced Research*, *5*(4), 491–497.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war *<https://doi.org/10.1080/00396338.2011.555586>*. *Survival: Global Politics and Strategy*, *53*(1), 23–40.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *The American Journal of International Law*, *110*(3), 425–479.

Fransman, M. (2010). *The new ICT ecosystem: Implications for policy and regulation*. Cambridge University Press.

Gheorghe, A. V., Masera, M., De Vries, L., Weijnen, M., & Kröger, W. (2007). Critical infrastructures: The need for international risk governance *<http://dx.doi.org/10.1504/IJCIS.2007.011543>*. *International Journal Critical Infrastructures*, *3*(1–2), 3–19.

Golandsky, Y. (2016). *Cyber crisis management, survival or extinction?* [Paper presentation]. International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, UK.

Greenberg, A. (2018, August 22, 2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Security Studies Quarterly*, *53*(4), 1155–1175.

Hopkins, A. (2014). Issues in safety science *<https://doi.org/10.1016/j.ssci.2013.01.007>*. *Safety Science*, *67*, 6–14.

Howard, P. N., & Kollanyi, B. (2016). Bots, #Strongerin, and #Brexit: Computational propaganda during the UK-EU referendum *<http://doi.org/10.2139/ssrn.2798311>*.

Jewkes, Y., & Yar, M. (2010). Handbook of internet crime. Willan.

Keitner, C. (2019). *Attribution by indictment* <http://doi.org/10.2139/ssrn.3322943> (Paper No. 316). UC Hastings Research Paper.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft <https://doi.org/10.1162/ISEC_a_00138>. *International Security*, *38*(2), 7–40.

Kim, K. (2007). Overview of electronic and algorithmic trading. In K. Kim (Ed.), *Electronic and algorithmic trading technology: The complete guide* (pp. 15–27). Academic Press.

Kovacs, A., & Hawtin, D. (2013). *Cyber security, cyber surveillance and online human rights*. Stockholm Internet Forum on Internet Freedom for Global Development.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining a problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (p. 664). University of Nebraska Press.

Kuipers, S. L., & Boin, R. A. (2015). Exploring the EU's role as transboundary crisis manager: The facilitation of sense-making during the Ash-crisis. In R. Bossong & H. Hegemann (Eds.), *European civil security governance: Diversity and cooperation in crisis and disaster management* (pp. 191–210). Macmillan.

Kuipers, S., Van Grieken, B. J., & Van Asselt, M. B. A. (2018). Risk, hazards, and crises in research: What risks get researched, where, and how? <https://doi.org/10.1002/rhc3.12160> *Risk, Hazards & Crisis in Public Policy*, *9*(4), 384–396.

Kuipers, S., & Welsh, N. H. (2017). Taxonomy of the crisis and disaster literature: Themes and types in 34 years of research <https://doi.org/10.1002/rhc3.12123>. *Risk, Hazards & Crisis in Public Policy*, *8*(4), 272–283.

Lachow, I. (2015). The Stuxnet enigma: Implications for the future of cybersecurity. *Journal of International Affairs*, *1*, 118–127.

Lafrance, A. (2017, January 31). The internet is mostly bots <https://www.theatlantic.com/technology/archive/2017/01/bots-bots-bots/515043/>. *The Atlantic*.

Landau, S. (2013). Making sense from Snowden: What's significant in the NSA surveillance revelations. *IEEE Security & Privacy*, *11*(4), 54–63.

LaPorte, T. R. (1994). A strawman speaks up: Comments on the limits of safety. *Journal of Contingencies and Crisis Management*, *2*(4), 207–211.

LaPorte, T. R. (1996). High reliability organizations: Unlikely, demanding and at risk. *Journal of Contingencies and Crisis Management*, *4*(2), 60–71.

LaPorte, T. R. (2018). Preparing for anomalies, revealing the invisible: Public organization puzzles, in risk. *Hazards and Crisis in Public Policy*, *9*(3), 258–277.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2009). A brief history of the internet *<https://doi.org/10.1145/1629607.1629613>*. *SIGCOMM Computing Community. Review*, *39*(5), 22–31.

Leukfeldt, R. (Ed.). (2017). *Research agenda: The human factor in cybercrime and cybersecurity*. Eleven International.

Liaropoulos, A. (2011). Power and security in cyberspace: Implications for the Westphalian state system. In M. Majer, R. Ondrejcsak, V. Tarasovic, & T. Valasek (Eds.), *Panorama of global security environment* (pp. 541–548). Centre for European and North American Affairs.

Livingstone, S., Haddon, L., Gãrzig, A., & Ãlafsson, K. (2011). *Risks and safety on the internet: The perspective of European children*. *Full findings*.

Luiijf, E., & Besseling, K. (2013). Nineteen national cyber security strategies. *International Journal Critical Infrastructures*, *9*(1–2), 3–31.

Maurer, T. (2018a). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.

Maurer, T. (2018b). Cyber proxies and their implications for liberal democracies *<https://doi.org/10.1080/0163660X.2018.1485332>*. *The Washington Quarterly*, *41*(2), 171–188.

Meeuwisse, R. (2017). *Cybersecurity for beginners*. Cyber Simplicity.

Mueller, R. S. I. (2019). Report on the investigation into Russian interference in the 2016 Presidential Election, Volume I and II *<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.documentcloud.org%2Fdocuments%2F5955118-The-Mueller-Report.html&data=04%7C01%7Cs.l.kuipers%40fgga.leidenuniv.nl%7Ca08e89b012d4454bc88608d9c64e9f12%7Cca2a7f76dbd74ec091086b3d524fb7c8%7C0%7C0%7C637758863255368645%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=CtJegkD3c3jaG3%2BCLyhZvV12M6OHNHaTqn3MKTji4K0%3D&reserved=0>*. Washington, DC.

Nakashima, E. (2015, July 9). Hacks of OPM databases compromised 22.1 million people, federal authorities say *<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.washingtonpost.com%2Fnews%2Ffederal-eye%2Fwp%2F2015%2F07%2F09%2Fhack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say%2F&data=04%7C01%7Cs.l.kuipers%40fgga.leidenuniv.nl%7Ca08e89b012d4454bc88608d9c64e9f12%7Cca2a7f76dbd74ec091086b3d524fb7c8%7C0%7C0%7C637758863255368645%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=sxea7lOiRSh8lGS6byuh9MjMKPUKjlf0YwMV3KyiNDQ%3D&reserved=0>*. *The Washington Post*.

Naughton, J. (2016). The evolution of the internet: From military experiment to general purpose technology *<https://doi.org/10.1080/23738871.2016.1157619>*. *Journal of Cyber Policy*, *1*(1), 5–28.

NCSC. (2021). Cybersecurity Assessment Netherlands 2021 <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fenglish.nctv.nl%2Fbinaries%2Fnctv-en%2Fdocuments%2Fpublications%2F2021%2F08%2F05%2Fcyber-security-assessment-netherlands-2021%2FCSBN2021_EN_02.pdf&data=04%7C01%7Cs.l.kuipers%40fgga.leidenuniv.nl%7Ca08e89b012d4454bc88608d9c64e9f12%7Cca2a7f76dbd74ec091086b3d524fb7c8%7C0%7C0%7C637758863255368645%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=wjqU%2BBh8uCEHixKkgNo84h5ZvbjIXYAUpbUzNbGkK9Y%3D&reserved=0>. *The Hague*.

Nye, J. S., Jr. (2014). *The regime complex for managing global cyber activities* (pp. 1–32). Global Commission on Internet Governance, Harvard University, Belfer Center for Science and International Affairs.

Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cyber security and critical energy infrastructure <https://doi.org/10.1016/j.tej.2014.01.011>. *The Electricity Journal*, *27*(2), 52–60.

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books.

Perrow, C. (1994). The limits of safety: The enhancement of a theory of accidents. *Journal of Contingencies and Crisis Management*, *2*(4), 212–220.

Rid, T. (2012). Cyber war will not take place <https://doi.org/10.1080/01402390.2011.608939>. *Journal of Strategic Studies*, *35*(1), 5–32.

Ridler, K. (2018, December 29). US investigating CenturyLink internet outage, 911 failures <https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fapnews.com%2Farticle%2Fus-news-mo-state-wire-ajit-pai-wa-state-wire-id-state-wire-1454add5707d41118930e49ae5752f11&data=04%7C01%7Cs.l.kuipers%40fgga.leidenuniv.nl%7Ca08e89b012d4454bc88608d9c64e9f12%7Cca2a7f76dbd74ec091086b3d524fb7c8%7C0%7C0%7C637758863255368645%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=c%2FeOLhk77QoDMSeX2SlM0yzjhN2eyP4lArYsoa49Ymk%3D&reserved=0>. *AP News*.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks <https://doi.org/10.1080/01402390.2014.977382>. *The Journal of Strategic Studies*, *38*(1–2), 3–37.

Rijpma, J. (1997). Complexity, tight-coupling and reliability: Connecting normal accidents theory and high reliability theory. *Journal of Contingencies and Crisis Management*, *5*(1), 15–23.

Rosenthal, U., & Kouzmin, A. (1997). Crises and crisis management: Toward comphensive government decision making. *Journal of Public Administration Research and Theory*, *7*, 277–304.

Sagan, S. (1994). Towards a political theory of organizational high reliability. *Journal of Contingencies and Crisis Management*, *2*(4), 228–240.

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. W. W. Norton.

Severance, C. R. (2015). *Introduction to networking: How the internet works*. CreateSpace.

Singer, P. W., & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Sottek, T. C., & Kopfstein, J. (2013, July 17). Everything you need to know about PRISM: A cheat sheet for the NSA's unprecedented surveillance programs *<https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>*. *The Verge*.

Soule, N., Simidchieva, B., Yaman, F., Watro, R., Loyall, J., Atighetchi, M., Carvalho, M., Last, D., Myers, D., & Bridget Flatley, C. (2015, August 18–20). *Quantifying & minimizing attack surfaces containing moving target defenses* [Paper presentation]. 3rd International Symposium on Resilient Cyber Systems (ISRCS), Philadelphia, PA.

Speed, R. (2019, January 24). Office 365 enjoys good old-fashioned Thursday wobble as email teeters over in Europe *<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.theregister.com%2F2019%2F01%2F24%2Foffice_365_down%2F&data=04%7C01%7Cs.l.kuipers%40fgga.leidenuniv.nl%7Ca08e89b012d4454bc88608d9c64e9f12%7Cca2a7f76dbd74ec091086b3d524fb7c8%7C0%7C0%7C637758863255368645%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=WMAoVZTmxn5ImDCWgWURuXjRri%2B%2FFMI2Rk3RGiYcw1A%3D&reserved=0>*. *The Register*.

Susskind, J. (2018). *Future politics: Living together in a world transformed by tech*. Oxford University Press.

Taddeo, M. (2012). Information warfare: A philosophical perspective. *Philosophy & Technology*, *25*(1), 105–120.

Taipale, K. A. (2004). Technology, security and privacy: The fear of Frankenstein, the mythology of privacy and the lessons of King Ludd. *Yale Journal of Law & Technology*, *7*(1), 125–221.

The Associated Press. (2019, April 14). Facebook, Instagram, WhatsApp back up after massive outage *<https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fapnews.com%2F806c4f4851294cf59c868c87ed107f56&data=04%7C01%7Cs.l.kuipers%40fgga.leidenuniv.nl%7Ca08e89b012d4454bc88608d9c64e9f12%7Cca2a7f76dbd74ec091086b3d524fb7c8%7C0%7C0%7C637758863255368645%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=VcOZxbyVMVcghKvpoD7WyeWOWVpqX08omEWrodkf5Ik%3D&reserved=0>*.*AP News*.

Thompson, J. D. (1967). *Organizations in action*. McGraw-Hill.

Van den Berg, B., & Keymolen, E. (2017). Regulating security on the internet: Control vs. trust <https://doi.org/10.1080/13600869.2017.1298504>. *The International Review of Law, Computers & Technology*, *3*, 188–205.

Van den Berg, B., Prins, R., & Kuipers, S. (2021). Assessing contemporary crises: Aligning safety science and security studies <https://doi.org/10.1093/acrefore/9780190228637.013.1733>. Oxford University Press.

Van der Hof, S., Van den Berg, B., & Schermer, B. (2014). *Minding minors wandering the web: Regulating online child safety*. TCM Asser Press.

Wade, L. (2003). Terrorism and the internet: Resistance in the Information Age. *Knowledge, Technology, & Policy*, *16*(1), 104–127.

Wall, D. S. (2015). The internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 77–98). SAGE.

Wall, D. S. (2017). Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing. In R. Brownsword, E. Scotford, & K. Yeung (Eds.), *The Oxford handbook on the law and regulation of technology*. Oxford University Press.

Walsh, P. F., & Miller, S. (2015). Rethinking "Five Eyes" security intelligence collection policies and practice post Snowden <https://doi.org/10.1080/02684527.2014.998436>. *Intelligence and National Security*, *31*(3), 345–368.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Process of collective mindfulness. In A. Boin (Ed.), *Crisis management* (pp. 31–66). SAGE.

Wolbers, J. J., & Boersma, F. K. (2013). The common operational picture as collective sensemaking. *Journal of Contingencies and Crisis Management*, *21*(4), 186–199.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown.

Zetter, K. (2016). That insane $81M Bangladesh bank heist? Here's what we know. *Wired*.

Ziolkowski, K. (2013). Peacetime cyber espionage: New tendencies in public international law. In K. Ziolkowski (Ed.), *Peacetime regime for state activities in cyberspace* (pp. 425–465). NATO CCD COE.

Zittrain, J., & Palfrey, J. (2008). Internet filtering: The politics and mechanisms of control. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global internet filtering* (pp. 29–57). MIT Press.

Notes

1. This conceptualization is an expansion and revision of Kuehl (2009, pp. 29–30).

2. While the term *ecosystem* may resonate with biological, living organisms in readers' minds, it is also commonly used to describe cyberspace (see Abelson et al., 2015; Deibert, 2011; Dunn Cavelty, 2019; Kovacs & Hawtin, 2013; Nye, 2014; Zittrain & Palfrey, 2008). The reason is that there are clear similarities between biological ecosystems and the technical realm of cyberspace. Both consist of interdependent yet dynamically developing elements that strengthen, weaken, stabilize, or otherwise rely on one another. Both are influenced by outside and inside factors. While cyberspace is a man-made ecosystem, and other ecosystems are commonly not, due to the complexity and interconnectedness of the former, it is still valid to label it an ecosystem.

3. To accommodate for this duality in potential goals, many definitions of cyberespionage do not stipulate the purposes beyond the fact that it is about "intelligence gathering." See, e.g., the 2012 US Cyber Operations Policy, which defines cyberespionage as "*operations and related programs or activities conducted … in or through cyberspace, for the primary purpose of collecting intelligence …from, computers, information or communication systems, or networks with the intent to remain undetected* " (Buchan, 2015, p. 170).

4. For instance, in 2012 a fire destroyed a network exchange owned and operated by Vodafone in the Netherlands, which led to an outage of telephone communications for approximately 5 million subscribers in that country. See Vodafone Dutch service disrupted by fire *<https://www.reuters.com/article/vodafone-netherlands/vodafone-dutch-service-disrupted-by-fire-idUSL6E8F4BPW20120404>* and Integrated report Vodafone Netherlands *<https://www.vodafone.nl/_assets/downloads/algemeen/vodafone_netherlands_integrated_report2012%20_2013.pdf>*.

5. Between December and May of 2019 alone, the authors registered 21 large-scale, high-impact platform and internet outages globally due to system errors alone (the total number of large-scale, high-impact unintentional or accidental incidents registered in the same time period was 107). These ranged from platforms such as Facebook, Instagram, and WhatsApp going offline to entire network disruptions. See Anderson (2019) on a global outage at Facebook and Instagram that occurred in March 2019. Note that a month later, Facebook, Instagram, and WhatsApp all three went offline due to another system error (The Associated Press, 2019). Microsoft also had several platform outages. For instance, in January 2019, Outlook went offline due to a system error in all of Europe (Speed, 2019). Finally, an example of a large-scale, severe network outage due to a system error occurred on December 27, 2018, when the network of the internet provider CenturyLink in the United States was no longer available to customers across the nation. It even took 911 services offline in parts of the country (Ridler, 2018).

6. For instance, due to poorly configured settings, the user profiles and shopping details of millions of Chinese shoppers at Gearbest *<https://techcrunch.com/2019/03/14/gearbest-orders-exposed/?guccounter=1>* were accidentally exposed in 2019.

7. For instance, Australian bank employees sent the data of 10,000 customers to the wrong email address, not just once, but more than 600 times before the mistake was detected *<https://gizmodo.com/australian-bank-sends-10-000-customers-data-to-wrong-em-1826482530>*.

8. One example of this was a power outage at Heathrow Airport in June 2017, which caused massive flight delays and was caused by an IT worker accidentally switching off the power supply *<https://www.independent.co.uk/news/business/news/british-airways-system-outage-it-worker-power-supply-switch-off-accident-flights-delayed-cancelled-a7768581.html>*.

9. Saudi Aramco is the most profitable company in the world and is the second-largest oil producer (measured in barrels per day) in the world *<https://en.wikipedia.org/wiki/Saudi_Aramco>*.

10. One notable exception is the use of ransomware, when end users are locked out of their own systems or devices until they pay a fee to criminals who have accessed their systems. This is comparable with stealing one's possessions in the offline world: The owner immediately realizes something is amiss, and they no longer have access to their own content.

11. In the Netherlands alone, the authors registered two cases in which this scenario materialized between December 2018 and January 2019. One of these involved a group of hospitals that all used the same systems and networks, thus exacerbating the impact (Broeken, 2018).

Related Articles

Information and Communication Technology in Crisis and Disaster Management

Cyber-Interference in the 2016 U.S. Presidential Election: A Crisis Analysis Case Study

Assessing Contemporary Crises: Aligning Safety Science and Security Studies