WHAT HAPPENS WHEN THE MACHINES STOP? UNCOVERING THE RISK OF DIGITAL FRAGILITY AS THE ACHILLES' HEEL OF THE DIGITAL TRANSFORMATION OF SOCIETIES

Alexander Herwix, herwix@wiso.uni-koeln.de, Cologne Institute for Information Systems (CIIS), University of Cologne, Germany.

Ross Tieman, Alliance to Feed the Earth in Disasters (ALLFED), Fairbanks, USA

Morgan Rivers, Alliance to Feed the Earth in Disasters (ALLFED), Fairbanks, USA

Christoph Rosenkranz, Cologne Institute for Information Systems (CIIS), University of Cologne, Germany

David Denkenberger, Alliance to Feed the Earth in Disasters (ALLFED), Fairbanks, USA *and* University of Canterbury in Christchurch, New Zealand

ABSTRACT

The digital transformation of societies has been a core concern for the information systems (IS) research community since its emergence. While most of this work has had a positive outlook, recently a stronger focus on the unintended consequences and dark side of digitalization has come to the fore. This paper contributes to this emerging stream of research by zooming in on a heretofore unrecognized question with potentially catastrophic consequences: What happens to our increasingly digitalized societies when a prolonged blackout causes a large fraction of digital systems and services to stop working for an extended period of time? To answer this motivating question, we conducted two system dynamics-based simulation experiments to tease out how different degrees of digitalization in a society would affect the resilience of the food system in the face of two different, extreme but plausible prolonged blackout scenarios. We find that a high degree of digitalization has a strong significant negative impact on food system resilience in the investigated scenarios. In the discussion of our findings, we conceptualize "the risk of digital fragility" as the underlying driver of the observed results. Moving forward, we suggest seven mitigation strategies for the risk of digital fragility as fruitful avenues for future research.

Keywords: Digital transformation, digital agility, digital fragility, systemic catastrophic risk, blackout, system dynamics, simulation experiment

WHAT HAPPENS WHEN THE MACHINES STOP? UNCOVERING THE RISK OF DIGITAL FRAGILITY AS THE ACHILLES' HEEL OF THE DIGITAL TRANSFORMATION OF SOCIETIES

"The best way to keep something bad from happening is to see it ahead of time... and you can't see it if you refuse to face the possibility."

— William S. Burroughs

The study of the development, adoption, use and impact of digital systems and services through a socio-technical lens has been the defining feature of the IS research community at large (Sarker et al., 2019). While most of this work is motivated by and grounded in the *positive* expectation that digital systems and services can help to improve personal, organizational or societal agility and performance, our research community is also increasingly becoming aware that the pervasive use of digital systems and services may also have potential *negative* effects, often referred to as "unintended consequences" or "dark side" (e.g., D'Arcy et al., 2012; Giermindl et al., 2022; Mikalef et al., 2022; Tarafdar et al., 2013). This includes, for example, research on technostress (e.g., Tarafdar et al., 2019), the potential dark side of social media on democratic decision making (e.g., Seger et al., 2020), or the misuse of artificial intelligence (AI) technologies (e.g., Mikalef et al., 2022). Importantly, such research has helped us gain a deeper and more nuanced understanding of the costs and risks that ought to be considered as the digital transformation of our societies[1] continues. We aim to contribute to this valuable stream of research and argue that IS research so far has overlooked at least one fundamental question with potentially catastrophic consequences: What happens to our increasingly digitalized

[1] Throughout this paper we use the phrases *digital transformation of societies* and *digital transformation* interchangeably to refer to the overarching societal transformation induced by the rapid and ongoing digitalization of processes, digitization of data, and digital transformation of organizations (Hanelt et al., 2021; Vial, 2019; Wessel et al., 2021).

societies when a prolonged blackout causes a large fraction of digital systems and services to stop working for an extended period of time?

Digital systems and services are inherently dependent on electricity, which makes them generally strongly vulnerable to blackouts given the centralized design of most societies electricity infrastructures. Without access to the electricity grid, it is estimated that digital systems and services will start failing within minutes. Most digital systems and services would be reaching complete failure within just a few days (i.e., after backup power generators run out of fuel or start failing themselves; Petermann et al., 2011; Stockton and EIS Council, 2016, 2018). Thus, we argue that it is critical and prudent to consider the potential negative effects that pervasive use and dependency on digital systems and services may have in prolonged blackout scenarios.

In particular, what if the digital transformation of our societies is not only making our organizations more agile, productive, and resilient but also has the unintended dark side of making our societies more *fragile* and *vulnerable* in catastrophic scenarios involving blackouts? We deem this to be an important avenue to investigate as we continue to rapidly increase the dependencies of our societies on digital systems and services. In our view, as IS researchers, we have a moral responsibility as well as the necessary expertise to engage with such concerns and help our societies to consciously manage the tensions between the potential bright sides and dark sides of the digital transformation.

As a first step towards engaging with this line of thinking, we seek to rigorously validate and test our premises. For this, we employ a devil's advocate perspective and explore the impact of the digital transformation in extreme but plausible blackout scenarios in which a large fraction of digital systems and services would stop working. We refer to these

prolonged blackouts as catastrophic electricity loss (CEL) scenarios[2] that may be triggered by events such as a coordinated cyberattack or a series of high-altitude electromagnetic pulses (HEMPs) caused by the use of nuclear weapons. While it might be uncomfortable to consider such dark scenarios and tempting to dismiss them as highly unlikely, given their outsized potential impact[3] and the limited attention we tend to afford them, it is still considered to be of high expected value to engage with them (Dolan, 2018; Petermann et al., 2011; Stockton and EIS Council, 2016). We do this by using a system dynamics (SD)-based Monte Carlo simulation of the U.S. food supply chain to investigate the research question: *How do different degrees of digitalization in a society affect the resilience of the U.S. food system in catastrophic electricity loss scenarios?* This is an appropriate research approach to engage with our overarching concern as it allows us to rigorously explicate, quantify, and interrogate our assumptions regarding the potential negative impact of the digital transformation of societies in CEL scenarios in a domain of utmost societal relevance. In particular, the food system is generally designated as one of the critical infrastructures (CIs) of society that "provide goods and services that enable the maintenance and sustainment of public wellbeing including public safety, economic vitality, and security" (Katina and Keating, 2015: 317).

We find that in all of our simulated scenarios, a higher degree of digitalization indeed leads to significant worse outcomes in terms of the peak amount of people affected by food shortages as well as the absolute number of days where people did not have access to food.

[2] With catastrophic electricity loss we mean blackouts covering a large geographic area with the size of multiple US states or EU countries, affecting at least 90% of the population and lasting for at least 30 days.
[3] One just has to look at the recent blackouts in Texas in February 2021 to get a glimpse of the potentially catastrophic consequences that large-scale and prolonged power outages can cause (Traywick et al., 2021).

Based on our scenario investigations and simulation results, we then go beyond the particularities of CEL scenarios and develop a novel theoretical framing that makes sense of the general dynamics we have observed. Specifically, we identify *the promise of digital agility* as a driving force and the potential bright side of the digital transformation of societies that is tempered by *the risk of digital fragility* as a potential dark side. As our results suggest, managing the interplay of these two sides will be a key challenge for our societies in general and IS research in particular. To kickstart engagement with this challenge, we aim to guide future research with a first set of tentative strategies that could help to manage it productively.

Our work contributes a fresh and critical look on a potential dark side of the digital transformation of societies that has largely been overlooked by IS research. Specifically, we illustrate the importance of considering CEL scenarios in the context of the ongoing digital transformation of our societies. Moreover, abstracting from the specifics of our work, we identify a set of general underlying dynamics inherent to the digital transformation of our societies that explain our results as a form of systemic catastrophic risk on the macro scale induced by competitive dynamics on the meso scale. Thus, we provide a simple but coherent explanation that resolves the mystery of how digital transformation with its promise of digital agility inadvertently ends up contributing to the risk of digital fragility. The usability and utility of our framing is demonstrated by a set of generic mitigation strategies for the risk of digital fragility that provide fruitful avenues for future research.

The rest of the paper is structured as follows. First, we clarify the key terms and concepts used in this study in the theoretical background section. Then, we describe and explain our research approach. Third, we present our scenario development and the results of two simulation experiments. Fourth, we discuss our findings and delineate implications for IS

research, IS practice, and policy making. Fifth, we conclude the paper with a call to action.

THEORETICAL BACKGROUND

The Digital Transformation of Societies and the Promise of Digital Agility

The digital transformation of our societies is quickly progressing as more and more aspects of our lives are becoming pervaded by digital systems (Haigh, 2022; Yoo, 2010). While this phenomenon may be examined from multiple viewpoints, in this paper, we are mostly concerned with a macro (i.e., societal) level perspective on the digital transformation of societies as a process of systemic and societal change that emerges from the interplay of competitive dynamics on the meso (i.e., organizational) level which, in turn, emerge from actions taken by individual actors on the micro level (Dopfer et al., 2004). Taking the macro level perspective, it has been suggested that much of the momentum behind the digital transformation of our societies is fueled by, what we call, *the promise of digital agility* (i.e., competitive advantage and resilience to be derived from the effective use of digital systems and services) on the meso level (Hanelt et al., 2021; Vial, 2019; Wessel et al., 2021). As illustrated in Figure 1, we view this promise of digital agility as being grounded in the realization that digital systems and services afford standardization and interconnectedness, which may be leveraged for competitive advantage and organizational resilience in competitive organizational environments.

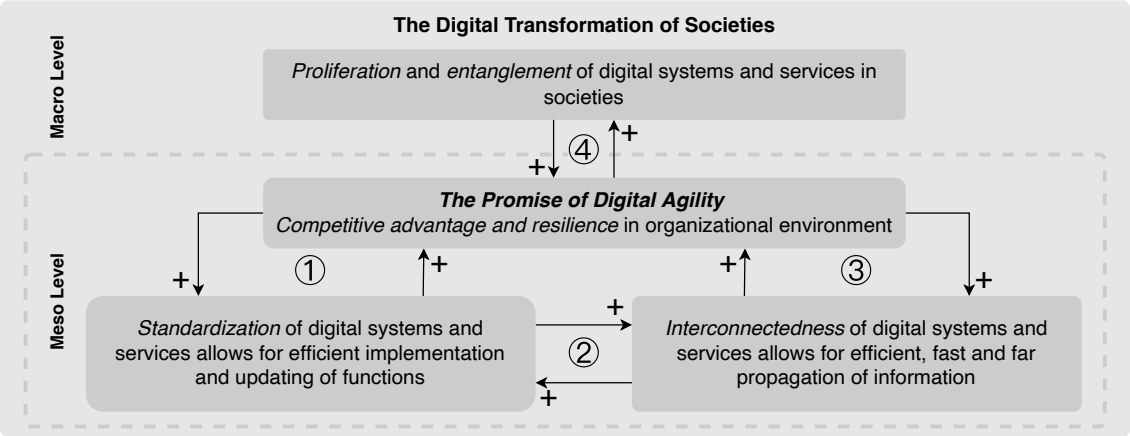

Figure 1. The promise of digital agility is grounded in the standardization and interconnectedness afforded by digital systems and services. Numbered relationships are explained in the text.

Referring to (1) in Figure 1, the *standardization* of modern digital systems and services generally follows a modular layered architecture (Yoo et al., 2010), which allows for the efficient implementation and continued updating of a wide variety of behaviors and functions. For instance, the same computer chip can be used for multiple different purposes, according to the software uploaded on it or a piece of software can be copied and installed on any number of machines. This organizing logic is so useful for business purposes that it is generally acknowledged that it confers competitive advantage to those who are able to leverage it most effectively (Yoo et al., 2010). This realization, in turn, has been sparking further investments into the development and standardization of a broad variety of digital systems and services (Haigh, 2022).

Related to (2) in Figure 1, the standardization of modern digital systems and services allows for and supports and unprecedented degree of *interconnectedness*, which, in turn, allows for the organization and standardization of even more complex and powerful digital systems and services (Sandberg et al., 2020). For instance, in the emerging Internet of Things (IoT) digital systems and services are now starting to be used to network entire cities together to allow for a greater control of processes, increased automation, and remote access (Zanella et al., 2014).

Regarding (3) in Figure 1, the increasing interconnectedness of digital systems and services also has important business value as it allows for a more efficient information transfer. Thus, the effective leveraging of interconnectedness promises competitive advantage, which, in turn, is sparking further investments to develop the interconnectedness of digital systems and services (Sandberg et al., 2020), for instance, as part of the emerging IoT (Zanella et al., 2014).

Considering (4) in Figure 1, all of these features and relationships fuel the promise of digital agility and, thus, contribute to a *proliferation* and *entanglement* of interconnected digital systems and services in society (Hillis, 2010). In a positive reinforcing feedback loop, this proliferation and entanglement, in turn, creates a competitive landscape that further grows the interest in the promise of digital agility as organizations increasingly fear to be left behind.

Importantly, these dynamics of the digital transformation contribute to an increasing set of complex interdependencies between different sectors of societies. For instance, digital systems and services rely on the electricity grid, which in turn depends more and more on digital systems and services for its functioning (Korkali et al., 2017; Parandehgheibi and Modiano, 2013; Siegel, 2018). Additionally, the electricity grid depends on power generation, which requires fossil fuel supply networks or renewable energy production systems, which in turn depend on digital supervisory control and data acquisition (SCADA) systems (Rinaldi, 2004).

As a result, the most critical sectors of our societies are increasingly viewed, modeled, and analyzed collectively as interdependent complex networks or *networks of networks* (Gao et al., 2012; Kenett et al., 2015) rather than mostly independent sectors that are only loosely coupled. This change in perspective is pivotal because it emphasizes the potential

for failures that can cascade across many different critical sectors of society, a fact which has already been observed in a variety of real life cases (Chang et al., 2007; Dobson et al., 2007; Haes Alhelou et al., 2019).

Given the potentially catastrophic outcomes of cascading failures (Petermann et al., 2011; Stockton and EIS Council, 2016), scholars have started to call for a more systematic engagement with the mechanisms and drivers in such scenarios. Explicitly called for are the development of useful models of interdependent critical infrastructures (Helbing, 2013) as well as guidelines for their design, regulation, and governance (Centeno et al., 2015; Hollick and Katzenbeisser, 2019). In particular, due to the nature of the challenge, more researcher attention from disciplines with experience in sociotechnical research perspectives is needed to prepare for or help prevent the most catastrophic scenarios that cascading failures across critical sectors of societies could entail (Centeno et al., 2015; Dolan, 2018; Helbing, 2013).

Cascading Failures and the Threat of Catastrophic Electricity Loss

Catastrophic electricity loss (CEL) is a phrase that we have coined for this paper. It refers to prolonged power outages of catastrophic proportions, sometimes also referred to as "black sky" events (e.g., Monken, 2015; Stockton and EIS Council, 2016). As a general rule of thumb, we start to speak of CEL when 90% of customers across a multistate (US-State) area lose electricity access for at least 30 days with long-term demand for emergency power (i.e., power provided by backup generators and alternative sources) and the potential for a slow recovery of grid capacity (sic., up to several months or years) to pre-event levels (NERC, 2012; Stockton and EIS Council, 2016). As such, it has to be observed that despite several large scale (and already devastating) power outages across different parts of the world (Haes Alhelou et al., 2019), an event that would qualify as

CEL has never happened up to now. Thus, CEL is, as of now, a truly rare and extreme event, which makes it hard to predict and easy to dismiss as unlikely or unrealistic (Goodwin and Wright, 2010; Wright and Goodwin, 2009). However, researchers highlight that CEL is certainly plausible (some say it is even inevitable; Dolan, 2018) and should be prepared for given its potentially catastrophic impact on societies (Hollick and Katzenbeisser, 2019; Petermann et al., 2011; Stockton and EIS Council, 2016).

Previous real world large-scale electricity loss such as during and after hurricane Katrina in 2005 (Reed et al., 2010) or during and after hurricane Maria in 2017 (Román et al., 2019) already illustrate the real harm and hardship that large-scale and long-term power outages can mean for people and societies. However, the impact of a CEL event would be much larger than these already devastating events. CEL could even occur on a global scale (e.g., in nuclear war or solar storm scenarios) and, thus, pose a profound challenge to humanity as a whole because significant shifts in global system dynamics (e.g., due to tipping points being crossed; Gladwell, 2000) would need to be expected. For instance, there are inherent and significant challenges to restarting entire electricity grids (Good, 2012; Siegel, 2018) or even multiple critical sectors of societies from complete shutdowns (Maher and Baum, 2013; Petermann et al., 2011).

Due to digital systems and services ultimate dependency on electric energy, we see the potential for such profound negative consequences as a critical incentive to engage with the threat of CEL scenarios. In particular, we chose to engage with CEL scenarios because they are generally highly neglected but tractable, which indicates a high cost effectiveness given their potential impact (Herwix and Haj-Bolouri, 2021). For instance, previous work has sketched out how food might be provided in the event of global CEL (Cole et al., 2016) and how other needs might be met (Abdelkhaliq et al., 2016). Further work ex-

plored scenarios of sun-obscuring catastrophes (e.g., asteroid or comet impact, supervolcanic eruption, and nuclear winter), which could cascade into near global CEL (Denkenberger et al., 2017). However, to the best of our knowledge no prior research has systematically considered the role of the digital transformation of societies in CEL scenarios.[4] This is an important gap given well-established concerns about the increasing interdependence between critical sectors of our societies (e.g., Buldyrev et al., 2010; Korkali et al., 2017; Rinaldi et al., 2001), which is only predicted to deepen as the digital transformation of our societies continues (e.g., Onyeji et al., 2014; Wang and Lu, 2013).

RESEARCH APPROACH

The research leading up to this paper can best be described as a combination of *scenario planning* in the *intuitive logic* school (Amer et al., 2013; Wilkinson et al., 2013) with a *system dynamics* modeling and simulation exercise (Fang et al., 2018). This is an appropriate research approach to answer our research question because scenario planning allows us to work with rare and difficult to predict events (Derbyshire and Wright, 2014; Goodwin and Wright, 2010; Wright and Goodwin, 2009) whereas SD modelling provides us with a rigorous way to open up our reasoning to critical scrutiny and academic discussion as well as play out the consequences of our assumptions (Fang et al., 2018; Rahmandad and Sterman, 2012).

Specifically, we use scenario planning in the intuitive logic school to identify and explore plausible scenarios of CEL—"a set of hypothetical events set in the future constructed to clarify a possible chain of causal events as well as their decision points" (Kahn and Wiener, 1967: 6)—with the goal of better understanding how a hypothetical situation might come about and be influenced rather than making quantitative assessments of their likelihood (Amer et al., 2013; Kahn and Wiener, 1967). This is reasonable because while

[4] See Appendix A for the results of a systematic review of IS research on this topic.

CEL scenarios are inherently complex, rare and uncertain events and, thus, difficult to predict with a well-calibrated probability distribution[5], this does not mean that their occurrence is unlikely (Goodwin and Wright, 2010). Even events which have been rare in the past, can still occur with a very high probability in the near future.[6]

Thus, we view our scenarios not as predictions of the future but rather as fictions and stories that can be deployed to question assumptions, start discussions, and work toward shared interpretative frames (Goodwin and Wright, 2010; Wilkinson et al., 2013; Wright, 2005). They should be understood as reframing devices rather than forecasting tools and not be judged in terms of their predictive accuracy but by their utility for action (Wilkinson et al., 2013). In our case, we used the developed scenarios as inputs for the adaptation of a SD-based simulation model of the U.S. food supply chain[7] to assess its resilience in the face of CEL scenarios. By doing so, we are able to combine the flexibility of the scenario planning approach with the rigorousness, extensibility, and auditability of simulation-based research (Dong, 2022).

Process-wise, our research was realized through a multi-step approach visualized in Figure 2. We started with the identification of plausible scenarios that fit our definition of CEL. Here, we followed prior suggestions to employ a *devil's advocate* perspective to consider rare but influential events that could have potentially disastrous effects (Goodwin and Wright, 2010; Wright and Goodwin, 2009). This can help to challenge

[5] A probability distribution is called calibrated if the chance that we assign to an event is accurate. For instance, it snows on 5% of days when we estimated the probability of snow is 5%. If it snows on more, or less, than 5% of those days then the probability assessment is mis-calibrated (Goodwin and Wright, 2010).
[6] For instance, taking the seminal example of the black swan (Taleb, 2010), there were hundreds of years where Europeans had a very low probability of encountering a black swan, simply because they had never visited large parts of the world. But once expeditions to Australia where getting more common, the first black swan encounter was simply a matter of time. However, given the data available at the time, the increasing chance of a black swan encounter would have been almost impossible to predict.
[7] We have adapted a peer-reviewed system dynamics based model of the U.S. food supply chain that was developed to assess the resilience of the U.S. food system in severe pandemics (Huff et al., 2015).

preexisting assumptions about likely futures, which has been argued to improve decision making by opening up horizons, challenging group think and combatting frame blindness (Goodwin and Wright, 2010; Wright and Goodwin, 2009). For this we have, in line with best practice recommendations (Wright and Goodwin, 2009), developed a scenario framework that establishes a systematic understanding of the progression of catastrophic risks and helps us in developing the broad outlines of scenarios which could cause CEL. In a next step, we then selected two potential scenarios for deeper investigation. Our choice of scenarios can be characterized as a convenience sample influenced by fit with our research question, expertise available, and length restrictions for this paper.

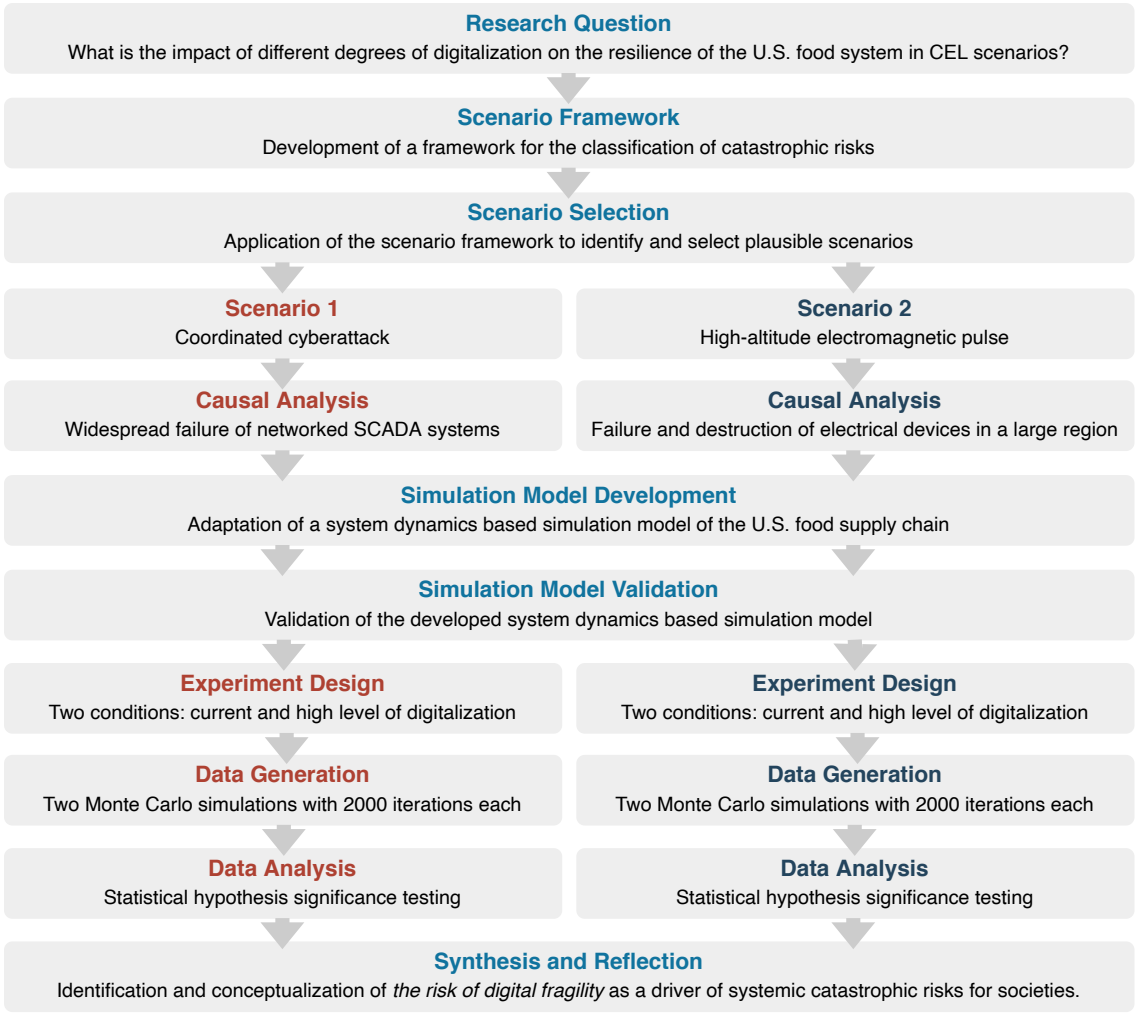

Figure 2. Summary of the research process.

We then engaged in desk research as well as a series of informal workshop sessions to investigate and develop the causal logic within each of the two scenarios. This step was informed and guided by broad but extensive literature searches on the topics as well as prior work of the authors that already engaged with the subject matter (e.g., doing impact analyses of HEMPs and other catastrophes – sources redacted for review). We used a comprehensive network diagram as well as specific causal diagrams as collaborative objects (Barley et al., 2012) to integrate our understanding. After several rounds of discussions within the author team as well as consultations with two outside experts with multiple years of professional experience in relevant domains[8], the authors reached consensual agreement regarding the causal logic within the scenarios and decided on a set of key parameter ranges (sic., severity of disruption and minimum recovery time for key affected sectors of society) that would provide plausible boundaries for the two selected CEL scenarios.

Next, we focused on the adaptation of an existing, peer-reviewed SD-based model of the U.S. food supply chain (Huff et al., 2015) to simulate how different degrees of digitalization would affect the outcome of CEL scenarios in a critical sector of society. This phase was highly iterative with simulation model development and validation going hand in hand. We used the recommended model validation guidelines from Fang et al. (2018) to ensure the validity and usefulness of our simulation model as summarized in Appendix B. In particular, we constructed two baseline blackout scenarios that more closely resemble already observed (i.e., less extreme) blackouts so that we could broadly compare the outputs of the model against available data. The details of these behavior tests are summarized in the online appendix.

[8] We consulted an academic expert in cybersecurity as well as an professional working at an electric utility in a relevant capacity.

Once all the validation tests passed and we were confident in the usefulness of our simulation model, we designed two experiments that would help us answer our research question. For each selected scenario we estimated a set of parameter ranges that would allow us to simulate their outcomes for two conditions: (1) Our current estimated level of digitalization, and (2) a higher level of digitalization that could plausibly come to be realized within the next decade. Thus, in line with general practice in simulation research, we decided on a simple experimental design with one control and one treatment condition that we could test with statistical hypothesis significance testing.

For the data generation we used the sensitivity simulation facility in the modelling and simulation software VENSIM PLE+[9] to run two reproducible Monte Carlo simulations with 2000 iterations per experiment. Using Monte Carlo simulations with thousands of iterations enabled us to sample a large fraction of the plausible scenario space as it allows for the use of probability distributions over specified ranges to estimate the interplay between uncertain parameters rather than having to settle for less informative point estimates for all simulation parameters. Thus, Monte Carlo simulation is a particularly appropriate method to investigate inherently uncertain phenomena such as CEL scenarios.

For the data analysis, the data generated by VENSIM PLE+ was exported to Microsoft Excel to calculate descriptive statistics as well as to conduct the statistical hypothesis significance testing. In particular, we used the built-in Excel functions for F-tests and two-tailed t-tests to calculate the p-values necessary for the testing of our hypotheses. All of the necessary data to reproduce our analyses including the simulation model, a documentation of the simulation model, a justification for our parameter choices, configuration files for running our experiments, the Monte Carlo simulation results, and the Excel

[9] https://vensim.com/

spreadsheet used for data analysis are made accessible as an online appendix to this publication.[10]

In a final step of synthesis, we then reflected on the results of our experiments and scenario investigations and identified underlying dynamics in the considered CEL scenarios. We conceptualized these dynamics as contributing to "the risk of digital fragility" which drives and is driven by systemic catastrophic risks for our societies. Tentative mitigation strategies for digital fragility were derived based on this framing as well as related work.

SCENARIO DEVELOPMENT

Our scenario development was guided by a comprehensive scenario framework, which we present in depth in Appendix C. In short, the framework opened up a potential space of 63 unique broad catastrophic risk scenarios along the three key dimensions of *risk origin* (how does the risk begin?), *risk scaling* (how does the risk reach catastrophic scale?), and *risk impact* (how does the risk impact a focal system?).[11] Given these key scenario dimensions, we were able to systematically develop the broad outlines of a variety of plausible CEL scenarios by considering combinations of characteristics. In particular, we developed several broad classes of plausible CEL scenarios,[12] but decided to focus on two scenario classes that exhibited strong ties to the digital transformation of our societies and, thus, were particularly relevant to our investigation (see Table 1):

- *Coordinated cyberattacks* intentionally caused by a small number or a large number of humans (i.e., a malicious risk or a conflict risk) as a scenario that is deemed

[10] https://osf.io/k3c9g/

[11] In particular, the risk origin dimension highlights seven potential starting points for a CEL scenario. The risk scaling dimension highlights three potential ways a CEL scenario could reach a catastrophic scale. The risk impact dimension highlights three potential ways a focal system could be catastrophically impacted.

[12] We considered amongst others: a severe pandemic caused without human involvement (i.e., a natural risk) or caused by humans, whether intentionally (i.e., a malicious risk) or unintentionally (i.e., an accident risk); a hurricane as a naturally occurring phenomenon (i.e., a natural risk) that could be intensified or even caused by human involvement in the climate and weather system due to massive greenhouse gas emissions (i.e., a commons risk), a geomagnetic storm as a naturally occurring phenomenon (i.e., a natural risk).

to become more likely as cyberwarfare is proliferating (e.g., King and Gallagher, 2020),

- *High-altitude Electro-Magnetic Pulse,* either, intentionally caused by humans, whether small in numbers (i.e., a malicious risk) or large in numbers (i.e., a conflict risk), or unintentionally caused by them (i.e., an accident risk) as a scenario where digital systems may be rapidly destroyed on a catastrophic scale (e.g., Wilson, 2008).

Table 1. An overview of the investigated scenarios with a classification of their associated risk types with the electricity grid as the focal system.

Scenario Name	Risk Origin	Risk Scaling	Risk Impact
Coordinated Cyberattacks	Malicious Risk, Conflict Risk	Cascading Risk	Functioning Risk, Infrastructure Risk
High-altitude Electro-Magnetic Pulse	Malicious Risk, Conflict Risk, Accident Risk	Leverage Risk	Functioning Risk, Infrastructure Risk

Coordinated Cyberattacks

For our simulation experiment, we consider a coordinated cyberattack on the electrical grid that was intentionally caused by a small number of humans (e.g., an elite cyberwarfare team of an adversarial state) as this seems to be the most plausible way in which a cyberattack could cause CEL.[13] The U.S. Electric Infrastructure Security (EIS) council notes that with the rise of terrorism and the sophistication of cyberwarfare measures, it is prudent to assume that eventually a large scale cyberattack will cause a wide-scale power outage (Stockton and EIS Council, 2016). In particular, a coordinated

[13] However, the recent shutdown of the Colonial Pipeline (a pipeline network which transports a large fraction of the oil on the East Coast of the US) illustrates that a cyberattack could potentially even unintentionally cause CEL (i.e., be an accident risk). In this specific case, low confidence in the cybersecurity measures of the company led to the shutdown of the entire pipeline network after the cybercrime group DarkSide attacked the business network of the company with ransomware (Sanger and Perlroth, 2021).

attack to disable the supervisory control and data acquisition (SCADA) systems (i.e., systems that control the operation of machinery) of power plants or in other electrical grid components should be treated as a plausible scenario given that it could be perpetrated not only by nation states but also cyber terrorist groups. Attacks by cyber terrorist groups are very difficult to deter because retaliation is hampered by a lack of international treaties and enforcement mechanisms against such groups (Tehrani et al., 2013). Importantly, such attacks need not necessarily be limited to a given country or region as SCADA systems are increasingly interconnected through proprietary networks (Korkali et al., 2017) and sometimes even reachable via the Internet (Pliatsios et al., 2020). In our hypothetical scenario a 'Stuxnet' like worm (King, 2012; Nicolas et al., 2011) infiltrates a large fraction of SCADA systems involved in the electricity grid and then triggers a simultaneous disruption that almost instantaneously takes down around 90% of the entire U.S. electricity grid. Attempts to recover the electricity grid start immediately but the sheer size of the outage and failures in backup power generators at some facilities lead to severe challenges in communication, coordination and recovery (Siegel, 2018). This is troublesome because recovery from complete shutdown of the electricity grid is a complex process that requires intensive communication to sync up different sections of the electricity grid (Good, 2012; Siegel, 2018). Considering these challenges, the recovery is remarkably quick as the entire U.S. energy sectors pulls together to restore the operational capacity of the electricity grid just 14 to 45 days after the incident. A more comprehensive analysis of the plausibility of such a scenario is provided in Appendix D.

High-altitude Electromagnetic Pulse

A HEMP could be caused in a variety of ways. For instance, it could be intentionally caused by a small terrorist group that is supported by a nuclear power state such as North Korea (i.e., a malicious risk). It could also intentionally be used by nation states in a

conflict situation (i.e., a conflict risk). Finally, it could also be caused unintentionally, for example, in a military accident (i.e., an accident risk).

No matter the cause, researchers have identified increasing vulnerabilities to HEMP and other electromagnetic pulse (EMP) attacks as digital systems and services proliferate in CIs (Savage et al., 2010). As integrated circuits shrink and a wider variety of technologies become reliant on digital microelectronics, the scope of destruction from HEMP attacks has dramatically broadened from a few technologies in the 1980s to the ubiquitous digital systems and services of today. The early time, high frequency component of a (H)EMP known as the E1 pulse component is especially concerning. The minimum electric field of the E1 pulse required to upset the operation of common desktop computers fell by a factor of seven from 1980 to 2001 (Camp and Garbe, 2006). The control center components of SCADA systems are physically similar in design to desktop computers, and are among the most vulnerable technologies to (H)EMP E1 effects. A comprehensive test of several SCADA systems found 100% of the control systems were affected, in many cases observing permanent damage to the system components (Foster et al., 2008). Many SCADA systems communicate using long surface level ethernet cables that can have strong currents induced by an E1 pulse, increasing their vulnerability. In addition, most critical infrastructures, at least in the US, are not shielded against the effects of HEMP with the military branch being the only exception (The Threat: The State of Preparedness Against the Threat of an Electromagnetic Pulse (EMP) Event, 2015).

For our simulation experiment, we consider a devastating but plausible scenario were an unknown adversarial nation state detonates two HEMP weapons 160 km above the population heavy centers of the West Coast and the East Coast of the U.S. destroying a significant fraction of digital systems such as SCADA systems in the entire country within

seconds (Wilson, 2008).[14] As a result of this attack, the electricity grid and multiple other critical infrastructures (e.g., the energy sector at large, information and communications technology sector, etc.) are severely disrupted and only function at about 40% capacity. Due to the large amounts of equipment that need to be replaced on a national scale and potentially extremely long lead times for the replacement of some critical electricity grid components such as high voltage transformers (i.e., several months; U.S. Department of Energy, 2014), we estimate a broad range of recovery times from 60 to 525 days (i.e., 2 month to 1.5 years). A more comprehensive analysis of the plausibility of such a HEMP scenario is provided in Appendix E.

SIMULATION OVERVIEW

To investigate the effects of different degrees of digitalization in a society in the aforementioned scenarios, we simulate how the scenarios play out in the context of the U.S. food supply chain. This is a useful choice as the food system is a critical sector of society that has a strong correlation with human well-being. If for whatever reason people start to lose access to food, this directly translates into losses of well-being and, after some time, enhanced probabilities of illness and even death. Thus, loss of access to food can act as reasonable proxy variable to assess the overall severity of a CEL scenario.

Our simulation of the U.S. food supply chain is built on the prior work of Huff et al. (2015). In their work, they have investigated the resilience of the U.S. food system against severe pandemics. For this, they had developed a SD-based simulation focused on modeling the impacts of worker absenteeism on the scale of the entire U.S. on the different stages in the food supply chain, namely, *farms*, *food processing*, *food distribution*, and

[14] While we do not consider this, such a scenario could quickly turn into an all-out HEMP exchange with other nuclear power states such as China or Russia (Pry, 2020, 2021) if they are presumed to be responsible for this attack.

food retail. We built on this work by removing some of the parts focused on modeling the effects of worker absenteeism and replacing them with models of key sectors of society affected by CEL and how they would impact the food supply chain at each stage. The main logic of the resulting model is visualized in Figure 3.[15]

Starting at the top left and moving to the bottom right of Figure 3, the demand flow is moving from the total U.S. population through each stage of the food supply chain down to the farm sector. At each stage the expected demand is stored and used to regulate the production and transportation of food products up to the next stage in the supply chain. Importantly, for each of the major production and transportation steps in the supply chain, the maximum carrying capacity is constrained by the disruption of the key infrastructures the step is dependent on. In particular, we have modeled the constraints in such a way that disruptions to the key infrastructures can interact in a variety of different ways to limit the capacity at each step. Specifically, as part of the modelling, we have taken a socio-technical perspective and distinguished between three broad sources of disruption effects: the *human factors*, the *non-digital technical factors*, and the *digital technical factors* involved in a step. This separation allows us to model the impact of CEL disruptions on a granular level for each step[16] as well as enables us to investigate the impact that different degrees of digitalization have in the case of disruption scenarios.

[15] Here, we only present the main logic of the model due to the large size and complexity of the complete model. However, the complete model can be retrieved from the online appendix and should be reasonably accessible once the main model logic is understood. The complete model can be run and experimented with using the free VENSIM model reader (https://vensim.com/free-download/).

[16] Altogether, we have estimated 56 parameters to model the impact that infrastructure disruptions have on the food supply chain. See the online appendix for a detailed documentation.

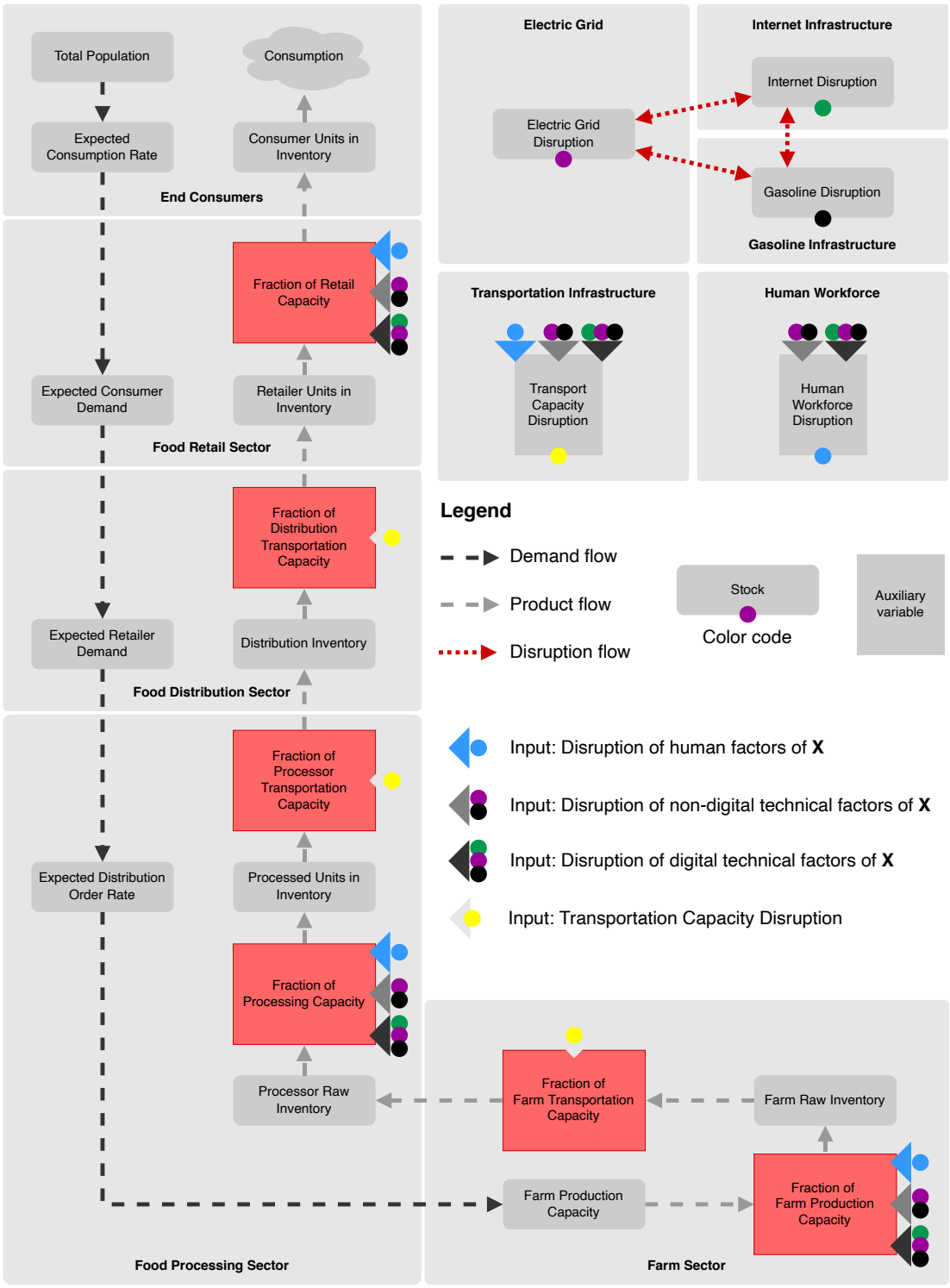

Figure 3. Overview of the main logic of the SD-based simulation model.

In terms of the key sources of disruption, we have identified the electricity grid, the Internet, the gasoline infrastructure, the transportation infrastructure and the human workforce as major dependencies of the food system.[17] We explicitly modeled the electricity grid, the Internet, the gasoline infrastructure, and their interdependencies as base infrastructures. The transportation infrastructure and the human workforce are modeled as extending infrastructure that depend on the base infrastructures but do not constrain them in turn.

SIMULATION EXPERIMENTS

Our goal with this paper is to investigate the effect that different degrees of digitalization in a society would have on the resilience of the food supply chain in the case of CEL scenarios. As a first step toward answering this question, we decided to use our SD-based simulation model to conduct two simulation experiments in two different CEL scenarios. We vary the degree of digitalization in the U.S. food supply chain between one control condition (i.e., current level of digitalization) and one treatment condition (i.e., plausible future higher level of digitalization). For this, we identified 6 parameters in our model that would significantly vary between these two conditions and assigned them plausible value ranges for both conditions as summarized in Table 2.

We use the final values of two food system disruption related variables as dependent variables for our experiments: 1) *Peak number of people without access to food,* and 2) *Cumulative number of person days without access to food*. Here, person days without access to food are defined in terms of the difference in the actual rate of consumption and the

[17] We acknowledge that the water system is another major dependency. However, due to the strong correlation between the water system and the electricity grid (e.g., Petermann et al., 2011) and in favor of limiting the complexity of the model, we decided against modeling the water system explicitly and instead subsumed its disruption effects within the disruption effects of the electricity grid.

desired rate of consumption by the population.[18] Both variables together provide a useful summary of how the CEL scenarios and the different degrees of digitalization in societies affect the food supply chain. Whereas the peak number of people without access to food scopes the maximum *intensity* of the disruption, the cumulative number of person days without access to food also reflects the duration of the disruption and, thus, more closely approximates the overall *size* of a disruption.[19]

The two hypotheses to be tested in the simulation experiments are:

H_1: In the case of CEL scenarios, a high degree of digitalization in a society leads to more intense disruptions in the food supply chain.

H_2: In the case of CEL scenarios, a high degree of digitalization in a society leads to altogether larger disruptions in the food supply chain.

The testing of these hypotheses was conducted in two simulation experiments that made ease use of two Monte Carlo simulation with 2000 iterations to sample a broad spectrum of the parameter space for the control as well as treatment condition. In particular, all parameter ranges were sampled using a uniform probability distribution reflecting our high uncertainty regarding the real probability distribution of the variables.

Table 2. An overview of the model parameters varied between the treatment and control condition of the simulation experiments. See the online appendix for a justification of the assigned parameter values.

Location	Description	Control	Treatment

[18] In our calculations of peak numbers of people affected, we naively assume that people either have full or no access to food. While this might not be an entirely realistic assumption, it is reasonable for our simulation experiments as we are not interest in accurate predictions of the number of people affected in CEL but the impact of different degrees of digitalization in societies.

[19] For instance, a high peak number of people without access to food but a comparatively low cumulative number of person days without access to food would indicate an intense but short disruption of the food supply chain, whereas a low peak number of people without access to food but a comparatively high cumulative number of person days without access to food would indicate a less intense but prolonged disruption.

Farm	Overall factor of digital technical factors on total disruption	30% - 50%	50% - 90%
Transport	Overall factor of digital technical factors on total disruption	30% - 70%	70% - 90%
Processing	Overall factor of digital technical factors on total disruption	60% - 80%	80% - 100%
Retail	Overall factor of digital technical factors on total disruption	60% - 80%	80% - 100%
Electricity grid	Overall factor of Internet disruption on electricity grid	0% - 20%	20% - 40%
Gasoline infrastructure	Overall factor of Internet disruption on gasoline infrastructure	0% - 20%	20% - 40%

Coordinated Cyberattacks

As we have established in the scenario development section, a coordinated cyberattack on the electricity grid is a plausible and maybe even likely scenario that could lead to CEL. In Table 3, we summarize the scenario-specific parameter values that we estimated for this scenario.

Table 3. An overview of the model parameters varied for the coordinated cyberattacks scenario. See the online appendix for a justification of the assigned parameter values.

Location	**Description**	**Value**
Electricity grid	Fraction of primary electricity grid disruption	90%
Electricity grid	Minimum recovery time for disruption	14 – 45 days
Gasoline infrastructure	Fraction of primary gasoline infrastructure disruption	0%
Gasoline infrastructure	Minimum recovery time for disruption	1 – 3 days
Internet	Fraction of primary Internet disruption	0%
Internet	Minimum recovery time for disruption	1 – 2 days

The results of the two Monte Carlo simulation runs for the two key dependent variables in this experiment are visualized as boxplots in Figure 4. Visual inspection of the diagrams suggests, and the statistical analysis of the results confirms, a highly significant positive difference between the control and treatment condition for both dependent variables.[20] In absolute and relative numbers, the difference in outcomes is notable. The mean peak number of people without access to food in the control condition is around 137 million (~42% of the U.S. population), whereas the mean for the treatment condition is around 183 million (~55% of the U.S. population; ~34% increase), and the mean cumulative number of person days without access to food in the control condition is around 3 billion (on average ~22 days loss of access to food per affected person), whereas the mean for the treatment condition is around 4 billion (~33% total increase, on average ~22 days loss of access to food per affected person). Thus, we can accept both hypotheses we investigated for this CEL scenario simulation experiment.

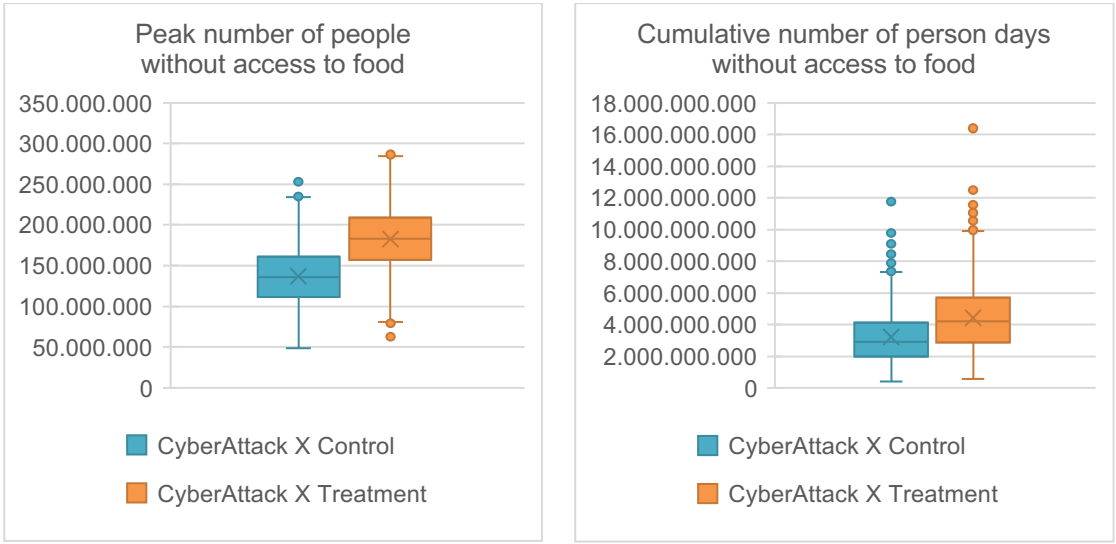

Figure 4. Main results for the cyberattack scenario simulation experiment.

[20] Both variables are significantly different between control and treatment condition at 99,9% confidence (Peak number of people without access to food, p-value = 2,2913E-286; Cumulative number of person days without access to food, p-value = 2,09283E-92).

High-altitude Electromagnetic Pulse

As we have highlighted in the scenario development section, the use of HEMP weapons would likely be devastating for a digital-infused infrastructures and result in very severe CEL. In Table 3, we summarize the scenario-specific parameter values that we estimated for this simulation experiment.

Table 4. An overview of the model parameters varied for the HEMP scenario. See the online appendix for a justification of the assigned parameter values.

Location	Description	Value
Electricity grid	Fraction of primary electricity grid disruption	60%
Electricity grid	Minimum recovery time for disruption	60 – 530 days
Gasoline infrastructure	Fraction of primary gasoline infrastructure disruption	60%
Gasoline infrastructure	Minimum recovery time for disruption	60 – 355 days
Internet	Fraction of primary Internet disruption	60%
Internet	Minimum recovery time for disruption	60 – 355 days

The results of the two Monte Carlo simulation runs for the key dependent variables in this experiment are visualized as boxplots in Figure 5. Again, visual inspection of the diagrams suggests, and the statistical analysis of the results confirms, a highly significant positive difference between the control and treatment condition for both dependent variables.[21] In absolute and relative numbers, the difference in outcomes is again notable. The mean peak number of people without access to food in the control condition is around 172 million (~52% of the U.S. population), whereas the mean for the treatment condition

[21] Both variables are significantly different between control and treatment condition at 99,9% confidence (Peak number of people without access to food, p-value = 2,34197E-27; Cumulative number of person days without access to food, p-value = 1,47921E-21).

is around 189 million (~57% of the U.S. population; ~10% increase), and the mean cumulative number of person days without access to food in the control condition is around 35 billion (on average ~203 days loss of access to food per affected person), whereas the mean for the treatment condition is around 44 billion (~26% total increase, on average ~233 days loss of access to food per affected person).[22] Thus, we can accept both hypotheses we investigated for this CEL scenario simulation experiment.

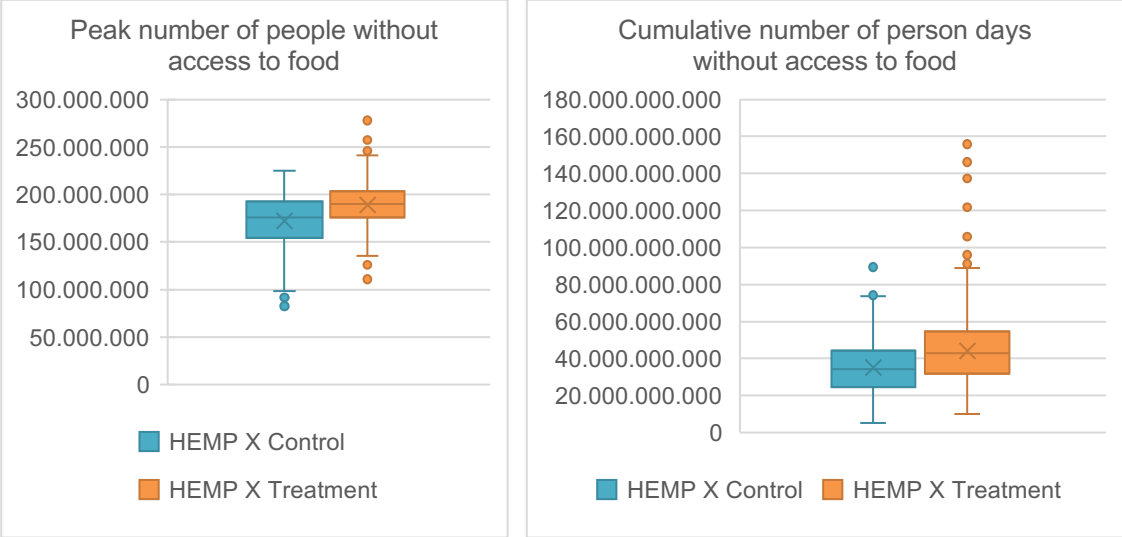

Figure 5. Main results for the HEMP scenario simulation experiment.

DISCUSSION

Uncovering The Risk of Digital Fragility

The simulation experiment results suggest that the ongoing digital transformation of societies may have potentially catastrophic consequences if a CEL scenario would ever come to pass. As demonstrated in our simulation experiments, the digital entanglement and interdependence driven by the digital transformation of societies reinforces and ex-

[22] It needs to be acknowledged that our model does not consider the possibility of people dying to starvation, which would certainly start to become a possibility and potentially a major driver of disruption dynamics in the case of this scenario given the severity of the simulation results. As such, the numbers should not be taken at face value and only be seen as indicators of relative disruption severity between the treatment and the control condition.

acerbates catastrophic failure cascades in CEL scenarios, so that ultimately entire countries may be brought down on their knees (Denkenberger et al., 2017; Heino et al., 2019; Petermann et al., 2011; Rinaldi et al., 2001; Stockton and EIS Council, 2016). We suggest to look at such scenarios as being driven by *the risk of digital fragility*: vulnerabilities affecting large fractions of digital systems and services.

As visualized in Figure 6, we find the risk of digital fragility to be brought about by the same features of digital systems and services that also spur the promise of digital agility: standardization and interconnectedness. However, instead of highlighting their potential positive consequences as is the case for the promise of digital agility, the risk of digital fragility highlights their potential negative consequences.

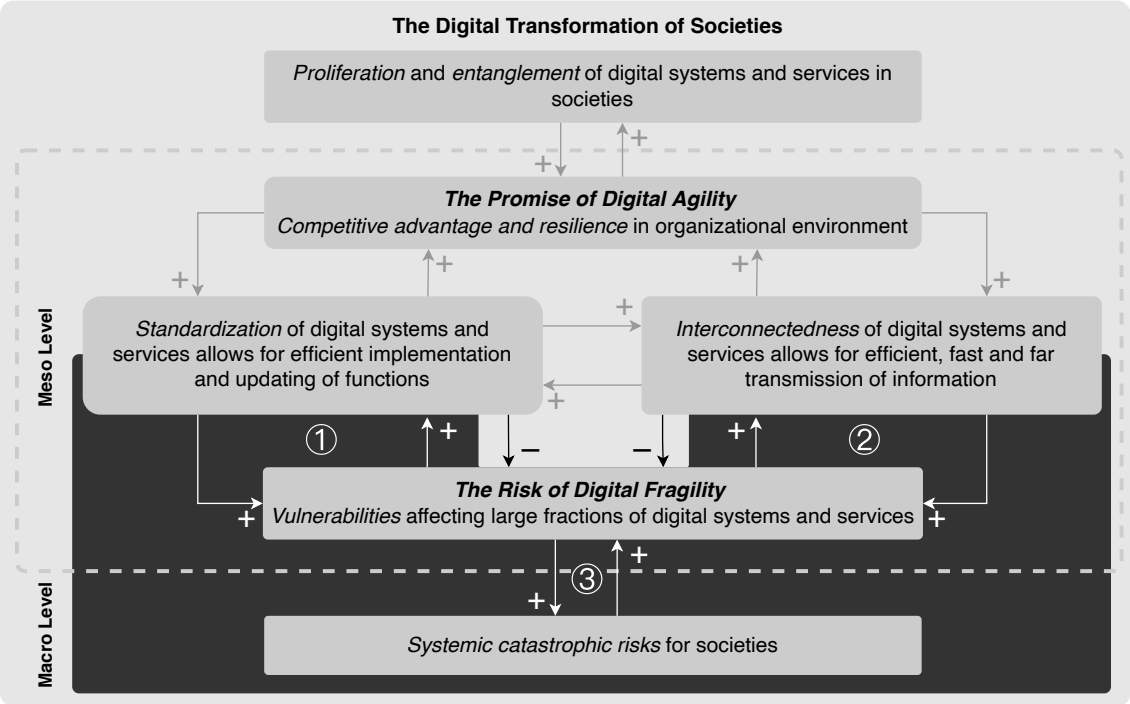

Figure 6. The risk of digital fragility as the driver of dark side of the digital transformation of societies. It describes how competitive dynamics at the center of the digital transformation of societies could cause systemic catastrophic risks. The figure builds on and extends the preceding Figure 1. Numbers label relationships explained in the text.

Referring to (1) in Figure 6, the *standardization* of digital systems and services leads to a comparatively homogenous population of technologies, systems and services on the lower levels of the modular-layered architecture of digital technologies (Yoo et al., 2010),

which means that some vulnerabilities can affect a large fraction of digital systems. For instance, a bug in a low-level instruction set architecture (ISA) implies that all digital systems using that ISA are vulnerable to that risk (Abu-Ghazaleh et al., 2019). Moreover, as discussed throughout this paper, all digital systems and services are vulnerable to electricity loss. Interestingly, this very risk of exploitable vulnerabilities generally leads to further attempts of standardization around best practices and the most trusted digital systems and services. For instance, there have been multiple attempts to standardize smart grid components to increase the safety of the smart grid (Leszczyna, 2018). However, this reinforcing feedback loop is balanced by the fact that the standardization of digital systems and services also generally enables rapid updating of functions (Yoo et al., 2010). Once discovered, vulnerabilities can often be closed quite quickly. Thus, the risk of digital fragility may also be reduced through the effective and security-minded use of standardization. Nevertheless, this ability to remediate vulnerabilities is not perfect and often limited by situational constraints as illustrated by the slow update cycles associated with a vast majority of Android devices (Mahmoudi and Nadi, 2018).

Regarding (2) in Figure 6, the *interconnectedness* of digital systems and services allows for a rapid propagation of cyber contagions (e.g., a computer virus or worm) or the disruption of only remotely connected digital systems and services, which means that the vulnerabilities which do exist (and are inadvertently triggered or intentionally exploited) can lead to massively cascading disruptions. For instance, increasing interconnectedness has so far also tended to contribute to the centralization of information exchange to a few large-scale digital platforms (Evans and Gawer, 2016; Zuboff, 2019). Thus, vulnerabilities in such platforms could have an outsized impact on the rest of the world.[23] In addition,

[23] As an example, recently many large websites were taken offline after a vulnerability in the systems of the cloud provider Fastly was accidentally triggered by an unwitting customer (Satariano, 2021).

the risks emerging from interconnectedness tend to further strengthen the interconnectedness of digital systems and services as this allows for more adaptive responses to the spreading of disruptions. For instance, the first solution to the increased spreading of computer viruses was not to reduce the interconnectedness of digital systems and services but rather to create antivirus software backed by centralized digital services that further increased the interconnectedness of digital systems and services (Nachenberg, 1997). However, this reinforcing feedback loop is balanced by the fact that interconnectedness of digital systems and services may also allow for the rapid propagation of fixes to vulnerabilities. Extending the antivirus example, if the antivirus system works as advertised the risk of digital fragility may be reduced by the additional connection to the digital services of the antivirus provider. Nevertheless, it must be acknowledged that there are often situational and institutional constraints in place, which limit our collective ability to remove vulnerabilities in an effective and efficient manner (Dunn Cavelty, 2014).

Related to (3) in Figure 6, we argue that these system dynamics contribute to systemic catastrophic risks in the context of the digital transformation of societies because they raise the likelihood for the emergence of disruptive, critical transitions (i.e., catastrophic scenarios) if repeated or large-scale stressors are ever to occur (Scheffer et al., 2012). As network science suggests (Scheffer et al., 2012), highly interconnected networks of standardized nodes are able to deal well with small perturbations where local adaptations can distribute the incurred stress in a safe way.[24] However, repeated perturbations or large-scale stressors affecting many nodes can more readily lead to the crossing of a tipping point. As a tipping point is crossed, the capacity for local adaptation is exhausted and catastrophic failure cascades emerge. With the results of our simulation experiments, we

[24] In the case of the electricity grid, this can be illustrated with the observation that increased interconnectivity between nodes may enable a better balancing of loads and increase resilience in the face of small or random failures in parts of the network (Korkali et al., 2017).

have demonstrated this pattern of behavior in CEL scenarios. If the power goes out for an extended period of time, the local adaptive capacities afforded by digital systems and services and the promise of digital agility are overwhelmed by the continuous stress inflicted through electricity loss. A catastrophic failure cascade ensues and sweeps through all interconnected critical sectors of our societies. Importantly, these patterns of behavior are not just limited to CEL scenarios. We suggest that the general dynamics hold irrespective of any specific catastrophic scenario. Loss of electricity is simply a very potent vulnerability that affects all digital systems and services (as well as many non-digital technical systems). As we have discussed in this section, other vulnerabilities that affect large fractions of digital systems and services are poised to emerge over time as the standardization and interconnectedness of digital systems and services continue to increase. As such, the risk of digital fragility may ultimately turn out to be a seriously dangerous Achilles' heel for our societies (Graham, 2011; Manheim, 2020).

Strategies to Mitigate the Risk of Digital Fragility

In a further step of reflection, we now discuss possible general strategies to mitigate the risk of digital fragility. Our thinking in this section is informed by (a) the available literature on catastrophic risks and emergency preparedness (e.g., Stockton and EIS Council, 2016, 2018), and (b) the general notion of antifragility (Taleb, 2012), which describes generic strategies for overcoming fragility such as creating optionality and redundancy in the system (Derbyshire and Wright, 2014). Altogether, we suggest a tentative set of seven promising strategies to mitigate the risk of digital fragility that provide promising avenues for future research:

- Modularity through protected enclaves;
- Optionality through alternative communication systems and power sources;

- Redundancy through readily available replacement parts;
- Diversity through small-scale experimentation;
- Hormesis through bug bounty programs;
- Better preparedness through financial incentives; and
- Cooperative response through legal obligations.

Modularity Through Protected Enclaves

Increasing the modularity of networks has been shown to reduce the spread of perturbation impact in experimental settings (Gilarranz et al., 2017). Analogously, modularization of CIs through the deliberate construction of protected enclaves has been proposed as an important means of improving our societies resilience to cascading failures (Monken, 2015). For instance, backup facilities should be deliberately located in a way that they have minimal interdependencies with the facilities they ought to replace in case of disaster. One promising avenue for reducing interdependencies in the electricity grid is through loosely coupled microgrids (Hirsch et al., 2018). In the case of cascading failures, microgrids can be operated independently from the main grid, which means that failure cascades can be stopped. Protected enclaves are especially relevant in the case of large-scale disruptions such as CEL scenarios because restoration efforts critically depend on incremental restoration pathways. The most challenging and delicate restoration process is the one which does not have any incremental steps that allow for the bootstrapping of further restoration efforts (c.f. the story of tempus and horus in Simon, 1962). Protected enclaves provide the necessary starting points and foot holes from which to plan and coordinate restoration efforts. However, protected enclaves need to be deliberately designed and developed. IS researchers have demonstrated their ability to develop novel research approaches and solutions that could potentially contribute to the planning, design and de-

velopment of protected enclaves (e.g., Ketter et al., 2013, 2016). For instance, the simulation model we developed could be used and extended to further investigate the role and potential positive impact of protected enclaves in the context of the food supply chain.

Optionality Through Alternative Communication Systems and Power Sources

According to Derbyshire and Wright (2014) creating optionality is part of a "truly non-deterministic and non-causal approach to preparation for the future" (p. 220). Having distinct (i.e., largely uncorrelated) options allows to bound potential losses in the face of a broad variety of causes while not limiting potential upsides.

Taking the Internet as an example, it has enabled humanity to coordinate and cooperate on unprecedented scales which has created unprecedented levels of wealth. However, in turn, our systems of organizing have become dependent on the Internet—without it (e.g., in CEL scenarios), we would be crippled (Petermann et al., 2011; Siegel, 2018; Stockton and EIS Council, 2018). Here, the creation of optionality via alternative communication systems that could take over key functions of the Internet but are not tightly linked to the Internet (e.g., they work by different mechanisms) provides a valid strategy to bound the negative effects associated with the loss of the Internet—no matter the cause (Stockton and EIS Council, 2018). Currently, efforts are underway to develop such alternative communication systems based on radio technology and mesh networking (Stockton and EIS Council, 2018). However, given the scale of the task at hand, additional research is likely needed and helpful to create optionality regarding our communication systems (Sakurai et al., 2014). For example, the development of approaches that can integrate existing mobile devices into self-organizing emergency mesh networks could help to create novel and cost effective alternative forms of communication in crisis situations (e.g., Banerjee et al., 2021).

Another key challenge during the onset of catastrophic scenarios such as CEL is maintaining power for lifeline CI, such as drinking water, food, medical services, communication services, and emergency services as well as electrical grid and CI recovery activities (Stockton and EIS Council, 2016). Emergency generators at key facilities provide some availability for lifeline infrastructure; however, the longer a blackout lasts, the higher the likelihood of such generators running out of fuel or failing (Petermann et al., 2011). As such, creating optionality by having additional power sources available in emergency situations seems like a prudent goal. Against this backdrop, hybrid electric vehicles (HEVs) have been identified as useful and cost-effective sources of flexible and mobile power generation, which could help to provide emergency power in crisis situations (Rahimi and Davoudi, 2018; Ustun et al., 2015). IS research could build on such results and investigate novel and cost-effective ways for the organization and use of HEVs in emergency situations. For instance, a smartphone based emergency communication system connected via a mesh network (e.g., Banerjee et al., 2021) could integrate a registry for HEV owners willing to assist during a CEL. Such a system could provide a cost-effective infrastructure for the coordination and deployment of a fleet of portable power generators, potentially greatly improving resilience and recovery efforts in disaster scenarios.

Redundancy Through Readily Available Replacement Parts

Enhancing redundancy and spare capacity is seen as another part of a well-considered strategy to prepare for an inherently uncertain and unpredictable future (Derbyshire and Wright, 2014; Taleb, 2012). While redundancy decreases efficiency, it can be seen as an investment that can provide significant upsides in the case of emergencies (Derbyshire and Wright, 2014). For instance, hospitals and companies with reserves of personal protective equipment or ventilators were well positioned when the COVID-19 pandemic hit,

whereas hospitals or companies without reserves quickly found themselves in a precarious situation.

In the context of the CEL scenarios we discussed, redundancy in relation to SCADA systems emerged as potential mitigation strategy. The latest generation of SCADA systems is characterized by their use of commercial off the shelf (COTS) parts, the use of open source software, and a shift in focus from custom hardware to custom software (Good, 2012). While the homogeneity induced by such standardization developments introduces risks, it also opens up a new opportunity for increases in redundancy as defective parts may be more easily replaced with standard computer parts that may have not been damaged as part of a cyberattack or HEMP. Thus, having dedicated stockpiles of standard chips and other computer parts for essential SCADA systems seems like a worthwhile investment in case of emergency. However, how to organize and finance such initiatives is generally an open question as market pressures do not seem to incentivize investments in redundancy and resilience (Little, 2005) as demonstrated by the recent (February 2021) blackouts in Texas, one of the most deregulated electrical grids in the world (Makholm, 2021). Thus, future IS research could look into creative ways to enhance the availability of replacement parts for digital systems in CIs. IS research on the circular economy may provide a fruitful starting point for such endeavors (e.g., Zeiss et al., 2021).

Diversity Through Small-Scale Experimentation

Considering the combination of the modularity, optionality, and redundancy strategies, we arrive at the realization that having a certain level of diversity in a system is desirable as it allows for the evolution of uncorrelated mechanisms that contribute to similar goals

and, thus, increase redundancy and resilience.[25] A viable strategy to induce such diversity is the use of small-scale experimentation to establish a diversified portfolio of projects, approaches, and technologies that is conducive to the emergence of redundancy and resilience in a system (Derbyshire and Wright, 2014).

In relation to the risk of digital fragility, small-scale experimentation could take the form of open innovation initiatives (Chesbrough et al., 2006) aimed at developing a variety of projects, approaches, and technologies that could be evaluated in terms of their systemic effects and made use of accordingly. However, open innovation initiatives are still in the early phases of being adopted in the critical sectors of our societies (Greco et al., 2017; Kankanhalli et al., 2017). IS research would seems well positioned to play a leading role in fostering this adoption. For instance, lessons learned from existing open innovation initiatives (Chesbrough et al., 2006) could be used to help leverage the potential of open innovation for mitigating the risks of digital fragility.

Hormesis Through Bug Bounty Programs

Hormesis generally refers to the biological mechanism by which an organism overcompensates in reaction to the presence of a small dose of toxin and thereby prepares itself for future encounters (Pech and Oakley, 2005). Analogously, in the context of planning for rare and potentially catastrophic events, hormesis stands for the deliberate seeking out of stressors that can help to prepare an organization for worse scenarios (Derbyshire and Wright, 2014; Taleb, 2012).

In relation to digital fragility and CEL scenarios, bug bounty programs (BBPs; Malladi and Subramanian, 2020) seem like a promising means of realizing hormesis in an cost-

[25] This thinking is in line with modern portfolio theory (Markowitz, 2010) which argues that investors can reduce their overall risk exposure without reducing returns by investing in a diversified portfolio of assets (i.e., not holding perfectly positively correlated assets).

effective, controllable and safe way. In general, a BBP is understood to be a form of crowdsourcing, where the organizers of the program determine a target system as well as certain rules of engagement and use prizes to incentivize the crowd to find vulnerabilities in the target system (Malladi and Subramanian, 2020). In particular, BBPs can be designed to help identify and fix vulnerabilities in specific products, services or systems and even consider their interdependencies. Moreover, BBPs can be deliberately limited to test environments, where no real harm can occur even if the target system is completely taken over or destroyed. As such, BBPs would lend themselves very well to the identification of specific vulnerabilities in critical sectors of our societies that are introduced by the digital transformation. In particular, BBPs could incentivize an ongoing examination and discovery of unanticipated and potentially catastrophic interdependencies in digital systems and services. IS research would seem to be in a great position to design and steer such efforts, for instance, building on and extending the aforementioned work on open innovation initiatives (Chesbrough et al., 2006).

Better Preparedness Through Financial Incentives

The creation of financial instruments that incentivize disaster preparedness is another potentially effective strategy for mitigating the risks of digital fragility. Here, resilience bonds have been proposed as an instrument to incentivize projects aimed at reducing the negative effects from very severe, relatively rare catastrophes (Vaijhala and Rhodes, 2018). Similar to insurance policies, resilience bonds are paid for in normal times and pay out in the case of disaster. However, in addition to a simple insurance mechanism, probabilistic catastrophe models are leveraged to identify worthwhile risk reduction efforts which may be paid for through discounts to the premium amount. Thus, risk reduction projects could be paid for in a structured and long-term way that is easier to manage and justify for potentially cash-strapped organizations and businesses. Moreover, forward

thinking regulation could consider instituting mandatory resilience bonds for CI sectors (similar to banking regulations in the financial sector), which would strongly incentivize more active engagement with cost-effective means of disaster preparedness as a cost cutting measure. Such an incentive structure could potentially overcome the traditional lack of investments into the long-term resilience and sustainability of CIs (Little, 2005). Despite this promising potential, open questions regarding resilience bonds remain, for instance, as of yet the realistic modelling of CI risks and associated risk reduction measures is still viewed as a difficult scientific challenge (Helbing, 2013). As such more work is needed to help establish resilience bonds more broadly in practice. IS research could contribute to such efforts through the design and evaluation of simulation models. For instance, the simulation model developed as part of this paper could be extended and refined to allow for the assessment of potential disaster risk reduction measures in relation to the food supply chain.

Cooperative Response Through Legal Obligations

The final strategy that we consider is to create legally binding agreements for companies that are part of CIs to cooperate more and freely share their resources in the case of extreme disasters. Given the rarity of such events, it would only pose small financial burdens on companies to agree to such legislation but it could prove vital if such events do occur. For example, there already exist agreements that allow cell phones to make emergency calls regardless of subscription status if network coverage is available. Such regulations could be extended to other aspects of CIs. For instance, internet service providers (ISPs) should suspend payment requirements for cyber real estate (i.e., domain names) in countries where a disaster occurs so that information dissemination is not impinged by comparatively trivial technicalities. Another avenue would be to study coopetition strategies

during the COVID-19 pandemic (Crick and Crick, 2020) to identify and establish effective mechanisms that support cooperation in disaster scenarios. One challenge that such legal obligations would face is to find effective means of specifying when they become activated as time may be of the essence. For instance, some electric utility providers have contributed to a cascading blackout because they were only willing to act in their narrow self-interest rather than cooperate for the benefit of the stability of the overarching grid (Little, 2005). Finding appropriate governance arrangements and systems that would effectively avoid such situations is an interesting question that future IS research might be able to contribute to. For instance, coordination methods and platforms could be designed and evaluated to guide and inform policy making.

Implications for Information Systems Research

Given our preceding discussion, what are the main takeaways for IS research? Primarily, we have used two simulation experiments to illustrate the potentially catastrophic effects of the digital transformation of societies in the case of CEL scenarios. The results of our experiments should raise awareness about the risk of digital fragility as an important concern that IS researchers should deliberately address going forward. As stewards of the digital transformation of our societies, we have the moral responsibility to ensure that our societies can continue on (or at least quickly recover) when at some point the lights go out as part of a prolonged blackout. Thus, we believe that IS research should play an important role in the further investigation of the risk of digital fragility as well as in the development of novel solutions that help to mitigate it. We started this endeavor by suggesting seven broad strategies for future work that IS researchers are encouraged to build on.

However, additional steps are necessary. The risk of digital fragility is not a property of an information system that could easily be designed out of the system using a design theory (Gregor and Jones, 2007). Rather it is an ongoing dynamic that needs to be continually managed rather than solved (Ackoff, 1967; Manheim, 2020). This will require systematic research from a variety of fields as well was cooperation and continued well-informed interventions on an unprecedented scale (Helbing, 2013). In many ways IS research seems well positioned to contribute to—or even play a leading role in—such an endeavor, since, as a community, we undoubtedly have a strong history in very relevant sociotechnical systems research (Sarker et al., 2019). Thus, we hope that IS research will rise to the challenge and start to consciously address the risk of digital fragility going forward.

Implications for Information Systems Practice

In terms of implications for IS practice, we mostly want to emphasize the importance of understanding the scope of the potential catastrophic consequences of the risk of digital fragility. It seems fair to say that most IS practitioners today are probably unaware that by promoting the digital transformation of our societies they might be contributing to systemic catastrophic risks that could upend life as we know it. Educating IS practitioners about the risk of digital fragility and ways of mitigating it (e.g., using the seven strategies that we outlined) could become an important concern for IS education. We hope that the framing of the risk of digital fragility as we have presented it in this paper is conducive to this endeavor.

Implications for Policy Making

Our suggested strategies for mitigating the risk of digital fragility provide important insights for policy makers. Rather than interpreting our warnings as a call

to stop investing in the digital transformation of our societies, our strategies suggest that more investments into the deliberate and thoughtful transformation of CIs seem necessary to counterbalance the risk of digital fragility rather than less. A focus on a *differential* digital transformation of societies (i.e., digital transformation directed at advancing resilience and sustainability disproportionately to mere technological capability and efficiency gains) seems important in this regard and could be supported through innovative financial instruments such as resilience bonds (Vaijhala and Rhodes, 2018). Moreover, well thought-out regulation informed by the seven strategies that we have outlined seems like another avenue worthwhile exploring.

LIMITATIONS AND FUTURE WORK

Our work is not without limitations. While we believe that the simulation experiments presented in this paper make a rigorous case for the potentially catastrophic consequences of the risk of digital fragility in CEL scenarios, we have to acknowledge that our investigation did not look at the positive outcomes of the promise of digital agility in times without infrastructure disruptions. As such, we cannot make any claims regarding the overall costs and benefits associated with the digital transformation of societies. However, we can highlight that in the case of CEL scenarios we expect a high degree of digitalization to lead to a more intense and overall larger disruption of the food system. This result allows us shine a bright light on a heretofore unrecognized unintended consequence or dark side of the digital transformation of societies. We hope that our work will inspire future work to further investigate the risk of digital fragility and potential mitigation strategies in a variety of scenarios beyond CEL and a diversity of contexts other than the food system. In addition, the SD-based model of the U.S. food supply chain we developed also

provides a fruitful foundation for future work. For instance, the model could be used to investigate the impacts of potential mitigation strategies for the risk of digital fragility.

CONCLUSION

In this paper, we have played the devil's advocate to the digital transformation of societies and investigated what would happen when the machines stopped. We have done this by conducting two simulation experiments of extreme but plausible CEL scenarios and how they would affect the U.S. food supply chain. Our results suggest that a high degree of digitalization in a society increases the intensity and size of disruptions in CEL scenarios. We trace this result to the risk of digital fragility, which is induced by the underlying dynamics of the digital transformation of our societies. Informed by extant literature we direct future research to further investigate seven strategies for mitigating the risks of digital fragility. We then summarize key implications for IS research, IS practice, and policy making.

Finally, we want to close this paper with a call to action for the IS research community. As our paper aims to demonstrate, the digital transformation that we are not only researching but often also heavily promoting may have severe unintended consequences we might not be aware of. At the same time, our actions are setting the foundation for future scholars and directing our attention. Let us become aware of this responsibility, broaden our horizons to the possibility of disaster—and then work diligently to prevent it.

> *"The price of greatness is responsibility."*
>
> — *Winston Churchill*

APPENDIX

APPENDIX A: Literature Review Summary

We have conducted a series of three systematic literature reviews to assess the relevance of prior IS research in relation to the topics of this paper. All literature reviews were carried out on the 25th of May 2022 via the Web of Science database (https://www.webofscience.com) using the eight publications of the Senior Scholar's Basket as a filter. In addition, we used a set of queries to search the topic field (equivalent to searching "title, keyword, and abstract" in other databases). We investigated the results in two steps. First, we read all titles and abstracts to assess potential relevance of the articles. Then we further read into the articles we found broadly relevant to our topic to identify directly related prior work. However, no IS research considering the role of the digital transformation of societies in relation to severe infrastructure disruption scenarios such as blackouts could be found. In particular, we did not find any paper considering the dependency of digital systems and services on electric energy in any detail.

Query	Total Results	Broadly Relevant	Directly Related
catastroph OR disaster* OR crisis OR "extreme event*" OR "black sky" OR blackout* OR "power loss" OR "power outage" OR "electricity loss" OR "product failure*" OR resilience OR fragility*	150	45	0
"dark side" OR "unintended consequence"*	57	2	0
"cyber war" OR "cyber attack" OR "cyber security" OR cybersecurity OR malware*	37	14	0

APPENDIX B: Simulation Model Validation

Table B.1. An overview of the simulation model validation based on Fang et al. (2018).

	Test	What to Test	Implementation in this Study
Direct Structural Tests	Structure Assessment	Model structure is consistent with relevant descriptive knowledge of the system.	The model is based on the peer-reviewed model of the U.S. food supply chain by Huff et al. (2015). We have also sent our updated version of the model to the original authors for feedback but have not heard back so far.
	Parameter Assessment	Parameter values are consistent with and reasonable to descriptive and numerical knowledge of the system.	Judgmental methods were applied by the author team to estimate most of the relevant parameters. Where appropriate, we deferred to the parameter values suggested in Huff et al. (2015). We documented and justified our estimates in the online appendix.
	Boundary Adequacy	The important concepts for addressing the problem are endogenous to the model.	Key concepts related to the disruption of CIs as well as the degree of digitalization are endogenous in the model.
	Dimension Consistency	Each equation is dimensionally consistent without the use of parameters having no real-world meaning.	The model passes the dimension consistency check utility in Vensim PLE+.
Structure Oriented Behavior Test	Extreme Conditions	Model responds plausibly when extreme policies apply.	The model exhibited anticipated behaviors when extreme values were assigned to key constants in the model. A documentation of the behaviors can be found in the online appendix.
	Sensitivity Test	This is the extent to which numerical values and behaviors change significantly.	The simulation experiment was itself a sensitivity test in the form of two Monte Carlo simulations. The model produced the anticipated behaviors.
	Integration Error	Results are not sensitive to the choice of time step or numerical integrating method.	The model was tested with a halving of the time step as well as with, both, the Euler and the Runge-Kutta integration methods.

Behavior Test	Behavior Reproduction	Model reproduces the behavior of interest in the system.	We used two baseline scenarios of smaller scale disruptions to the electricity grid to assess the appropriateness of the model outputs. We found the outputs to be broadly plausible and in line with expectations. Documentation can be found in the online appendix.

APPENDIX C: SCENARIO FRAMEWORK

In this appendix, we present the scenario framework which we used as a backdrop for the development of our scenarios. The framework is adapted from the work of Cotton-Barratt et al. (2020), who conceived of a comprehensive classification of extinction risks for the purpose of defending against them. We found this framework to be the best choice for our purposes because it provided us with an exhaustive overview of general logics by which catastrophic risks could unfold. We have adopted most of the terminology used by Cotton-Barratt et al. (2020) but have made some adjustments to adapt them to the specifics of our use case.[26] In our adapted framework, catastrophic risks are characterized along three dimensions, which may be used to systematically develop plausible CEL scenarios: the *origin*, the *scaling mechanism*, and the *impact mechanism* of the risk.

Origin of a Catastrophic Risk

For a catastrophic risk to become a problem at all, it has to have an *origin* or a beginning. Based on Cotton-Barratt et al.'s (2020) work, Table 1 lists a categorization of catastrophic risk origins in terms of human involvement and intentionality, which together lead to a classification of six risk types for catastrophic shocks caused by humans (i.e., anthropogenic risk) and one type for natural risk:

- *Unseen risks* are those where a few people cause a shock that was unforeseen and unintentional. For example, a critical bug in the Linux kernel disables large parts of the internet.

[26] In particular, we reframe extinction risk in terms of catastrophic risks because we suggest that the classification of Cotton-Barratt et al. (2020) can be usefully applied to smaller scales than human extinction if a catastrophic risk is interpreted not in an absolute sense but relative to a focal system under investigation. For instance, on the one hand, given a company as the focal system a catastrophic risk might be seen as anything that causes the breakdown of the company. On the other hand, given the global ecosystem of CIs as the focal system a catastrophic risk is more similar to what Cotton-Barratt et al. (2020) called extinction risk.

- *Latent risks* are those where many people together cause a shock that was unforeseen and unintentional. For example, pervasive use of social media creates increasingly resilient filter bubbles which cause a complete breakdown of epistemic security and subsequently social order.
- *Accident risks* are those where a few people cause a shock that was foreseen but unintentional. For example, the unintentional release of a virulent disease causes a pandemic.
- *Commons risks* are those where many people together cause a shock that was foreseen but unintentional. For example, large hurricanes caused by man-made climate change.
- *Malicious risks* are those where a few people cause a shock that was intentional. For example, a coordinated cyberattack by terrorists.
- *Conflict risks* are those where many people together cause a shock that was intentional. For example, multiple HEMP attacks as part of a great power war.
- *Natural risks* are those where a shock is not caused by humans. For example, a 1 in 10,000 year solar storm disables a significant fraction of extra high voltage (EHV) transformers globally.

Table C.1. A categorization of risk types according to their origin based on Cotton-Barratt et al. (2020).

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="2">Anthropogenic Risk</th><th>Natural Risk</th></tr>
<tr><th>Few People Cause Shock</th><th>Many People Cause Shock</th><th>No People Cause Shock</th></tr>
<tr><td rowspan="2">Unintentional Harm</td><td>Unforeseen Harm</td><td>Unseen Risk</td><td>Latent Risk</td><td rowspan="3">Natural Risk</td></tr>
<tr><td>Foreseen Harm</td><td>Accident Risk</td><td>Commons Risk</td></tr>
<tr><td colspan="2">Intentional Harm</td><td>Malicious Risk</td><td>Conflict Risk</td></tr>
</table>

Scaling Mechanism of a Catastrophic Risk

Once a catastrophic risk has begun to unfold, it has to reach a certain scale to substantially start disrupting and breaking down the functioning of the focal system. According to Cotton-Barratt et al. (2020), it is useful to characterize the process of disruption along two dimensions: (a) the amount of disruption done before a response is possible, and (b) the largest one-step increase in disruption. Based on those dimensions they suggest a classification of three different risk types:

- *Leverage risks* are those where only a low amount of disruption is caused before a response is possible but a large one-step increase in disruption can be observed. For example, a nuclear attack with intercontinental missiles could be detected early without much disruption caused but disruption would rapidly escalate once the missile reached its target.

- *Cascading risks* are those where only a low amount of disruption is caused before a response is possible and the one-step increases in disruption remain small. For example, a virus which only ever causes small amounts of disruptions on the micro-level but could quickly cascade to large-scale disruptions due to self-propagating and exponential growth.

- *Large risks* are those where already a large amount of disruption is caused before a response is possible. For example, a gamma ray burst from a source close to earth could cause irreparable disruption to CIs on a global scale within seconds.

Table C.2. A categorization of risk types according to their scaling mechanism based on Cotton-Barratt et al. (2020).

		Amount of Disruption before We can Respond	
		Low	**High**
Largest One-step Increase in Disruption	**High**	Leverage Risk	Large Risk
	Low	Cascading Risk	

Impact Mechanism of a Catastrophic Risk

Finally, it is possible to classify catastrophic risks by the mechanism with which they impact the functioning of the focal system. Inspired by Cotton-Barratt et al. (2020), we suggest three risk types based on whether they directly or indirectly affect the focal system:

- *Functioning risks* are those where the focal system's ability to carry out behaviors that fulfill desired functions is directly impacted. For example, a hurricane physically impacts the electricity grid.
- *Infrastructure risks* are those where the focal system is indirectly impacted by failures in the supporting infrastructure. For example, a disruption of the internet impacts the proper functioning of the energy markets.
- *Environment risks* are those where the focal system is indirectly impacted by shocks or changes in the environment. For example, after the nuclear accident in Fukushima the political climate around nuclear power changed dramatically, which led to the early retirement of otherwise well working nuclear power plants.

Table C.3. A categorization of risk types according to their impact mechanism.

	Impact		
	Direct	**Indirect**	
Focal System	*Functioning Risk*	*Infrastructure Risk*	*Environment Risk*

APPENDIX D: PLAUSIBILITY OF THE COORDINATED CYBERATTACK SCENARIO

The potential for cyber threats to impact electricity infrastructure was first uncovered during the 'Aurora experiment' during which a replica power plant's control systems were hacked causing it to self-destruct (Mackinnon et al., 2013). The ability for cyber risks to cause physical damage to CIs was later realized when the Stuxnet computer worm damaged a uranium enrichment facility in Iran in 2009 – 2010 (Nicolas et al., 2011). Stuxnet was likely able to infiltrate air gapped networks by infecting USB devices that crossed the air gap. It then exploited vulnerabilities in SCADA systems, infecting programmable logic controllers (PLCs) involved in controlling gas centrifuge speed. By covertly fluctuating rotation speeds, Stuxnet was able to destroy hundreds of gas centrifuges. The Stuxnet worm was so infectious that it has been found in control systems of various CI networks outside of Iran, including Chevron's network in 2010 (King, 2012; Nicolas et al., 2011). The targeting of SCADA system components by Stuxnet demonstrates the vulnerability of CI processes to cyberattacks.

The increasing connectivity of SCADA systems and utilization of distributed architectures increases the risk of cyberattacks. Wireless SCADA systems using the Internet are increasing in popularity (Pliatsios et al., 2020). As opposed to having to physically interact with hardwired SCADA systems, the increasingly commonplace connection of SCADA systems to corporate networks and even the Internet means that remote attacks should be expected (Kang et al., 2014; Nicholson et al., 2012). Coupled with the utilization of standard protocols to streamline control processes the likelihood of process-aware attacks[27] is increasing (Khorrami et al., 2016). A similar method as the Stuxnet worm may

[27] Attacks which change run-time parameters or control logic in computational nodes across multiple similar processes.

be used to infiltrate SCADA systems, hack into gateways or edge devices, and take control of entire CI nodes. Reprogramming the SCADA system would allow maloperation or self-destruction (Stockton and EIS Council, 2016).

Thus, it is entirely plausible and prudent to be concerned about a coordinated cyberattack that can take down the electric grid by attacking SCADA systems (Onyeji et al., 2014). For instance, there already exist multiple instances of the hacking of SCADA systems in electrical infrastructure (Byres et al., 2007; Kuvshinkova, 2003). Such an attack is of special concern because it could be widespread and have long-term destructive consequences.

Outside of SCADA system vulnerabilities, there exist other ways the electrical grid could be attacked. A recent example is the shutdown of a large pipeline network on the East Coast of the US due to a ransomware attack by the cybercrime group DarkSide (Sanger and Perlroth, 2021). In this cyberattack only the business network of the pipeline company was attacked but due to low confidence in the cybersecurity measures of the company, even operational systems had to be shut. Thus, even relatively simple cyberattacks without the intent to cause catastrophic harm can cascade to become significant events with potentially devastating consequences. If the shutdown had persisted for only a few days longer, it is very likely that even more severe cascade effects across several CIs would have started to appear (Sanger and Perlroth, 2021).

Disconcertingly, the risk of such events may further increase due to the accelerated digital transformation of business practices in response to the COVID-19 pandemic. In particular, an increase in remote work facilitated by greater utilization of digital technologies can be observed (Dwivedi et al., 2020; Papadopoulos et al., 2020), which presents new vectors that malicious actors could potentially exploit, in order to gain information, or

interfere with processes. Already a strong increase in damages caused by cybercrime can be observed (IC3, 2021), even with deaths being attributed to ransomware attacks on hospitals (Wolff, 2020).

Given this climate of increasingly prevalent cybercrime, a troubling development is that emerging smart grids appear to be particularly vulnerable to cyberattacks due to increased reliance on communication networks to provide enhanced efficiency and reliability (Wang and Lu, 2013). Moreover, even non-smart electrical grids are vulnerable to cyberattacks. For instance, security researchers have demonstrated how botnets[28] could push non-smart electricity grids into an unstable state by modulating the power consumption of hacked devices in a coordinated way (Dabrowski et al., 2017; Soltan and Mittal, 2018).

Altogether, we conclude that current trends and developments make a CEL scenario due to a coordinated cyberattack at least plausible or even likely in the future.

[28] A botnet is a network of a large number of hacked devices which is under the control of an adversary.

APPENDIX E: PLAUSIBILITY OF THE HIGH-ALTITUDE ELECTROMAGNETIC PULSE SCENARIO

On July 9th, 1962 a 1.4 Megaton of TNT equivalent test nuclear warhead known as "Starfish Prime" was detonated 400 km above a remote region in the Pacific, causing a HEMP. 750 miles away and seconds after the blast, telephone communications failed between Kauai, Hawaii and the rest of Hawaii. 900 miles away in Oahu, Hawaii, hundreds of street lights failed, car ignition systems were fused, and high frequency radio equipment was damaged. Based on publicly available information, between a few days and 6 months after the attack most satellites failed due to the explosion (National Coordinating Center for Communications, 2019).

While no HEMPs have been tested since the nuclear test ban treaty of 1963, HEMPs may still be used today by a nuclear enabled nation-state to disable the industry of one or many adversary nation-states. For instance, there have been indications that at least one country (Iran) has been practicing for a HEMP attack (Wilson, 2008) and China as well as Russia consider HEMP attacks as part of the arsenal of modern information warfare with lower thresholds for use than traditional nuclear attacks (Pry, 2020, 2021). Nuclear proliferation, the increased reliance on sensitive digital components for adversary nations' CIs, and the possibility that a HEMP might not induce the deterrence of mutually assured destruction (MAD) increase the plausibility of near-term HEMP attacks (Wilson, 2008). While research estimating the likelihood of a HEMP attack is lacking, previous work estimates a probability of 0.3% per year for full-scale nuclear war (Denkenberger and Pearce, 2018). We suspect the probability of a HEMP attack is likely as high or higher than full-scale nuclear war, due to game theoretic considerations concerning whether HEMP would elicit a full nuclear response. Thus, we conclude that current trends and developments make a CEL scenario due to a HEMP a hopefully unlikely but still plausible scenario in the future.

REFERENCES

Abdelkhaliq M, Denkenberger D, Cole D, et al. (2016) Non Food Needs if Industry is Disabled. In: *Proceedings of the 6th International Disaster and Risk Conference*, Davos, Switzerland, 2016.

Abu-Ghazaleh N, Ponomarev D and Evtyushkin D (2019) How the spectre and meltdown hacks really worked. *IEEE Spectrum* 56(3): 42–49. DOI: 10.1109/MSPEC.2019.8651934.

Ackoff RL (1967) Management misinformation systems. *Management science* 14(4): B147–B156.

Amer M, Daim TU and Jetter A (2013) A review of scenario planning. *Futures* 46: 23–40. DOI: 10.1016/j.futures.2012.10.003.

Banerjee I, Warnier M, Brazier FMT, et al. (2021) Introducing participatory fairness in emergency communication can support self-organization for survival. *Scientific Reports* 11(1). 1. Nature Publishing Group: 7209. DOI: 10.1038/s41598-021-86635-y.

Barley WC, Leonardi PM and Bailey DE (2012) Engineering Objects for Collaboration: Strategies of Ambiguity and Clarity at Knowledge Boundaries. *Human Communication Research* 38(3): 280–308. DOI: 10.1111/j.1468-2958.2012.01430.x.

Buldyrev SV, Parshani R, Paul G, et al. (2010) Catastrophic cascade of failures in interdependent networks. *Nature* 464(7291). 7291. Nature Publishing Group: 1025–1028. DOI: 10.1038/nature08932.

Byres E, Leversage D and Kube N (2007) Security incident and trends in SCADA and process industries: A statistical review of the Industrial Security Incident Database (ISID). *White Paper, Symantec Corporation, Cupertino, California*.

Camp M and Garbe H (2006) Susceptibility of Personal Computer Systems to Fast Transient Electromagnetic Pulses. *IEEE Journals & Magazine*. Available at: https://ieeexplore.ieee.org/abstract/document/4014644 (accessed 27 November 2020).

Centeno MA, Nag M, Patterson TS, et al. (2015) The Emergence of Global Systemic Risk. *Annual Review of Sociology* 41(1): 65–85. DOI: 10.1146/annurev-soc-073014-112317.

Chang SE, McDaniels TL, Mikawoz J, et al. (2007) Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 Ice Storm. *Natural Hazards* 41(2): 337–358. DOI: 10.1007/s11069-006-9039-4.

Chesbrough H, Vanhaverbeke W and West J (2006) *Open Innovation: Researching a New Paradigm*. OUP Oxford.

Cole DD, Denkenberger D, Griswold M, et al. (2016) Feeding Everyone if Industry is Disabled. In: *IDRC DAVOS 2016 Integrative Risk Management - Towards Resilient Cities*, Davos, Switzerland, August 2016. Available at: https://hal.archives-ouvertes.fr/hal-02113486 (accessed 15 August 2019).

Cotton-Barratt O, Daniel M and Sandberg A (2020) Defence in Depth Against Human Extinction: Prevention, Response, Resilience, and Why They All Matter. *Global Policy* 11(3): 271–282. DOI: 10.1111/1758-5899.12786.

Crick JM and Crick D (2020) Coopetition and COVID-19: Collaborative business-to-business marketing strategies in a pandemic crisis. *Industrial Marketing Management* 88: 206–213. DOI: 10.1016/j.indmarman.2020.05.016.

Dabrowski A, Ullrich J and Weippl ER (2017) Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. In: *Proceedings of the 33rd Annual Computer Security Applications Conference*, New York, NY, USA, 4 December 2017, pp. 303–314. ACSAC 2017. Association for Computing Machinery. DOI: 10.1145/3134600.3134639.

D'Arcy J, Gupta A, Tarafdar M, et al. (2012) Reflecting on the 'Dark Side' of Information Technology Use. *Communications of the Association for Information Systems* 35: 5. DOI: 10.17705/1cais.03505.

Denkenberger DC and Pearce JM (2018) Cost-effectiveness of interventions for alternate food in the United States to address agricultural catastrophes. *International journal of disaster risk reduction* 27. Elsevier: 278–289. DOI: https://doi.org/10.1016/j.ijdrr.2017.10.014.

Denkenberger DC, Cole DD, Abdelkhaliq M, et al. (2017) Feeding everyone if the sun is obscured and industry is disabled. *International Journal of Disaster Risk Reduction* 21: 284–290. DOI: 10.1016/j.ijdrr.2016.12.018.

Derbyshire J and Wright G (2014) Preparing for the future: Development of an 'antifragile' methodology that complements scenario planning by omitting causation. *Technological Forecasting and Social Change* 82: 215–225. DOI: 10.1016/j.techfore.2013.07.001.

Dobson I, Carreras BA, Lynch VE, et al. (2007) Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos: An Interdisciplinary Journal of Nonlinear Science* 17(2). American Institute of Physics: 026103. DOI: 10.1063/1.2737822.

Dolan TE (2018) *The London Black Sky Seminar 2018: Infrastructure and Societal Resilience to Black Sky Hazards*. *The London Black Sky Resilience Workshops*. Report, 26 February. Washington DC, USA: EIS (Electric Infrastructure Security) Council. Available at: https://www.eiscouncil.org/App_Data/Upload/3f6282a1-4b27-498c-b4c6-c67219d75a30.pdf (accessed 25 September 2020).

Dong JQ (2022) Using Simulation in Information Systems Research. *Journal of the Association for Information Systems* 23(2): 408–417. DOI: 10.17705/1jais.00743.

Dopfer K, Foster J and Potts J (2004) Micro-meso-macro. *Journal of Evolutionary Economics* 14(3): 263–279. DOI: 10.1007/s00191-004-0193-0.

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

Dwivedi YK, Hughes DL, Coombs C, et al. (2020) Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management* 55. Impact of COVID-19 Pandemic on Information Management Research and Practice: Editorial Perspectives: 102211. DOI: 10.1016/j.ijinfomgt.2020.102211.

Evans PC and Gawer A (2016) *The Rise of the Platform Enterprise: A Global Survey*. THE EMERGING PLATFORM ECONOMY SERIES. The Center for Global Enterprise.

Fang Y, Lim K, Qian Y, et al. (2018) System Dynamics Modeling for Information Systems Research: Theory of Development and Practical Application. *Management Information Systems Quarterly* 42(4): 1303–1329.

Foster J, Gjelde E, Graham WR, et al. (2008) *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*. 1 April. Available at: https://apps.dtic.mil/sti/citations/ADA484672 (accessed 27 November 2020).

Gao J, Buldyrev SV, Stanley HE, et al. (2012) Networks formed from interdependent networks. *Nature Physics* 8(1). 1. Nature Publishing Group: 40–48. DOI: 10.1038/nphys2180.

Giermindl LM, Strich F, Christ O, et al. (2022) The dark sides of people analytics: reviewing the perils for organisations and employees. *EUROPEAN JOURNAL OF INFORMATION SYSTEMS*. 2-4 PARK SQUARE, MILTON PARK, ABINGDON OR14 4RN, OXON, ENGLAND: TAYLOR & FRANCIS LTD. DOI: 10.1080/0960085X.2021.1927213.

Gilarranz LJ, Rayfield B, Liñán-Cembrano G, et al. (2017) Effects of network modularity on the spread of perturbation impact in experimental metapopulations. *Science* 357(6347): 199–201. DOI: 10.1126/science.aal4122.

Gladwell M (2000) *The Tipping Point: How Little Things Can Make a Big Difference*. 1st ed. Boston: Little, Brown.

Good J (2012) *Blackstarting the North American power grid after a nuclear electromagnetic pulse (EMP) event or major solar storm*. James Madison University. Available at: https://www.semanticscholar.org/paper/Blackstarting-the-North-American-power-grid-after-a-Good/55c6a413e94ccb0523ed17e9002d10312c590306 (accessed 27 November 2020).

Goodwin P and Wright G (2010) The limits of forecasting methods in anticipating rare events. *Technological Forecasting and Social Change* 77(3): 355–368. DOI: 10.1016/j.techfore.2009.10.008.

Graham S (2011) Disrupted Cities: Infrastructure Disruptions as the Achilles Heel of Urbanized Societies.: 15.

Greco M, Locatelli G and Lisi S (2017) Open innovation in the power & energy sector: Bringing together government policies, companies' interests, and academic essence. *Energy Policy* 104: 316–324. DOI: 10.1016/j.enpol.2017.01.049.

Gregor S and Jones D (2007) The Anatomy of a Design Theory. *Journal of AIS* 8(5): 312–335.

Haes Alhelou H, Hamedani-Golshan M, Njenda T, et al. (2019) A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges. *Energies* 12(4): 682. DOI: 10.3390/en12040682.

Haigh T (2022) Becoming universal. *Communications of the ACM* 65(2): 25–30. DOI: 10.1145/3506578.

Hanelt A, Bohnsack R, Marz D, et al. (2021) A systematic review of the literature on digital transformation: insights and implications for strategy and organizational change. *Journal of Management Studies* 58(5): 1159–1197. DOI: 10.1111/joms.12639.

Heino O, Takala A, Jukarainen P, et al. (2019) Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability* 11(3): 838. DOI: 10.3390/su11030838.

Helbing D (2013) Globally networked risks and how to respond. *Nature* 497(7447): 51–59. DOI: 10.1038/nature12047.

Herwix A and Haj-Bolouri A (2021) Revisiting the Problem of the Problem – An Ontology and Framework for Problem Assessment in IS Research. In: *Proceedings of the Twenty-Nineth European Conference on Information Systems (ECIS2021)*, 2021.

Hillis D (2010) The Age of Digital Entanglement. *Scientific American* 303(3). Scientific American: 93–93.

Hirsch A, Parag Y and Guerrero J (2018) Microgrids: A review of technologies, key drivers, and outstanding issues. *Renewable and Sustainable Energy Reviews* 90: 402–411. DOI: 10.1016/j.rser.2018.03.040.

Hollick M and Katzenbeisser S (2019) Resilient Critical Infrastructures. In: Reuter C (ed.) *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden: Springer Fachmedien, pp. 305–318. DOI: 10.1007/978-3-658-25652-4_14.

Huff AG, Beyeler WE, Kelley NS, et al. (2015) How resilient is the United States' food system to pandemics? *Journal of Environmental Studies and Sciences* 5(3): 337–347. DOI: 10.1007/s13412-015-0275-3.

IC3 (2021) *Internet Crime Report 2020*. FBI. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (accessed 28 May 2021).

Kahn H and Wiener AJ (1967) *The Year 2000; a Framework for Speculation on the next Thirty-Three Years*. New York, Macmillan. Available at: http://archive.org/details/year2000framewor00kahn (accessed 17 May 2021).

Kang D, Kim B and Na J (2014) Cyber threats and defence approaches in SCADA systems. In: *16th International Conference on Advanced Communication Technology*, February 2014, pp. 324–327. DOI: 10.1109/ICACT.2014.6778974.

Kankanhalli A, Zuiderwijk A and Tayi GK (2017) Open innovation in the public sector: A research agenda. *Government Information Quarterly* 34(1): 84–89. DOI: 10.1016/j.giq.2016.12.002.

Katina PF and Keating CB (2015) Critical infrastructures: a perspective from systems of systems. *International Journal of Critical Infrastructures* 11(4). Inderscience Publishers: 316–344. DOI: 10.1504/IJCIS.2015.073840.

Kenett DY, Perc M and Boccaletti S (2015) Networks of networks – An introduction. *Chaos, Solitons & Fractals* 80: 1–6. DOI: 10.1016/j.chaos.2015.03.016.

Ketter W, Collins J and Reddy P (2013) Power TAC: A competitive economic simulation of the smart grid. *Energy Economics* 39: 262–270. DOI: 10.1016/j.eneco.2013.04.015.

Ketter W, Peters M, Collins J, et al. (2016) COMPETITIVE BENCHMARKING: AN IS RESEARCH APPROACH TO ADDRESS WICKED PROBLEMS WITH BIG DATA AND ANALYTICS. *MIS Quarterly* 40(4): 34.

Khorrami F, Krishnamurthy P and Karri R (2016) Cybersecurity for Control Systems: A Process-Aware Perspective. *IEEE Design Test* 33(5): 75–83. DOI: 10.1109/MDAT.2016.2594178.

King A and Gallagher M (2020) *Cyberspace Solarium Commission*. Available at: https://www.solarium.gov/ (accessed 28 May 2021).

King R (2012) Virus Aimed at Iran Infected Chevron Network. *Wall Street Journal*, 9 November. Available at: https://online.wsj.com/article/SB10001424127887324894104578107223667421796.html (accessed 11 November 2020).

Korkali M, Veneman JG, Tivnan BF, et al. (2017) Reducing Cascading Failure Risk by Increasing Infrastructure Network Interdependence. *Scientific Reports* 7(1). 1. Nature Publishing Group: 44499. DOI: 10.1038/srep44499.

Kuvshinkova S (2003) SQL Slammer worm lessons learned for consideration by the electricity sector. *North American Electric Reliability Council* 1(2): 5.

Leszczyna R (2018) A review of standards with cybersecurity requirements for smart grid. *Computers & Security* 77: 262–276. DOI: 10.1016/j.cose.2018.03.011.

Little RG (2005) Tending the infrastructure commons: Ensuring the sustainability of our vital public systems. *Structure and Infrastructure Engineering* 1(4). Taylor & Francis: 263–270. DOI: 10.1080/15732470500103708.

Mackinnon L, Bacon L, Gan D, et al. (2013) Cyber Security Countermeasures to Combat Cyber Terrorism., pp. 234–257. DOI: 10.1016/B978-0-12-407191-9.00020-X.

Maher T and Baum S (2013) Adaptation to and Recovery from Global Catastrophe. *Sustainability* 5(4): 1461–1479. DOI: 10.3390/su5041461.

Mahmoudi M and Nadi S (2018) The Android update problem: an empirical study. In: *Proceedings of the 15th International Conference on Mining Software Repositories*, New York, NY, USA, 28 May 2018, pp. 220–230. MSR '18. Association for Computing Machinery. DOI: 10.1145/3196398.3196434.

Makholm JD (2021) The Texas Energy Debacle and the Economists. *Climate and Energy* 37(10): 19–25. DOI: https://doi.org/10.1002/gas.22229.

Malladi SS and Subramanian HC (2020) Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations. *IEEE Software* 37(1): 31–39. DOI: 10.1109/MS.2018.2880508.

Manheim D (2020) The Fragile World Hypothesis: Complexity, Fragility, and Systemic Existential Risk. *Futures* 122: 102570. DOI: 10.1016/j.futures.2020.102570.

Markowitz HM (2010) Portfolio Theory: As I Still See It. *Annual Review of Financial Economics* 2(1): 1–23. DOI: 10.1146/annurev-financial-011110-134602.

Mikalef P, Conboy K, Lundstrom JE, et al. (2022) Thinking responsibly about responsible AI and `the dark side' of AI. *EUROPEAN JOURNAL OF INFORMATION SYSTEMS*. 2-4 PARK SQUARE, MILTON PARK, ABINGDON OR14 4RN, OXON, ENGLAND: TAYLOR & FRANCIS LTD. DOI: 10.1080/0960085X.2022.2026621.

Monken J (2015) Black sky: Exposing electricity as the Achilles' heel of resilience. *Journal of Business Continuity & Emergency Planning* 9(1): 25–30.

Nachenberg C (1997) Computer virus-antivirus coevolution. *Communications of the ACM* 40(1): 46–51. DOI: 10.1145/242857.242869.

National Coordinating Center for Communications (2019) Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment. (2.2). Available at: https://www.cisa.gov/sites/default/files/publications/19_0307_CISA_EMP-Protection-Resilience-Guidelines.pdf.

NERC (2012) *Severe Impact Resilience: Considerations and Recommendations*. Severe Impact Resilience Task Force, 9 May. North American Electric Reliability Corporation. Available at: https://www.ourenergypolicy.org/wp-content/uploads/2012/05/SIRTF_Final_May_9_2012-Board_Accepted.pdf (accessed 24 October 2020).

Nicholson A, Webber S, Dyer S, et al. (2012) SCADA security in the light of Cyber-Warfare. *Computers & Security* 31(4): 418–436. DOI: 10.1016/j.cose.2012.02.009.

Nicolas F, Liam OM and Eric C (2011) *W32. Stuxnet Dossier*. Version 1.4, February. Available at: https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en (accessed 11 November 2020).

Onyeji I, Bazilian M and Bronk C (2014) Cyber Security and Critical Energy Infrastructure. *The Electricity Journal* 27(2): 52–60. DOI: 10.1016/j.tej.2014.01.011.

Papadopoulos T, Baltas KN and Balta ME (2020) The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice. *International Journal of Information Management* 55: 102192. DOI: 10.1016/j.ijinfomgt.2020.102192.

Parandehgheibi M and Modiano E (2013) Robustness of interdependent networks: The case of communication networks and the power grid. In: *2013 IEEE Global Communications Conference (GLOBECOM)*, December 2013, pp. 2164–2169. DOI: 10.1109/GLOCOM.2013.6831395.

Pech RJ and Oakley KE (2005) Hormesis: an evolutionary "predict and prepare" survival mechanism. *Leadership & Organization Development Journal* 26(8). Emerald Group Publishing Limited: 673–687. DOI: 10.1108/01437730510633737.

Petermann T, Bradke H, Lüllmann A, et al. (2011) *What happens during a blackout? Consequences of a prolonged and wide-ranging power outage*. OFFICE OF TECHNOLOGY ASSESSMENT AT THE GERMAN BUNDESTAG. Available at: https://www.tab-beim-bundestag.de/en/pdf/publications/books/petermann-etal-2011-141.pdf (accessed 12 May 2021).

Pliatsios D, Sarigiannidis P and Lagkas T (2020) A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. *IEEE*. Available at: https://ieeexplore.ieee.org/document/9066892 (accessed 27 November 2020).

Pry PV (2020) *China: EMP Threat: The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack*. 10 June. EMP Task Force on National and Homeland Security. Available at: https://apps.dtic.mil/sti/citations/AD1102202 (accessed 28 May 2021).

Pry PV (2021) *Russia: EMP Threat. The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack*. 28 January. DHS. Available at: https://apps.dtic.mil/sti/citations/AD1124730 (accessed 28 May 2021).

Rahimi K and Davoudi M (2018) Electric vehicles for improving resilience of distribution systems. *Sustainable Cities and Society* 36: 246–256. DOI: 10.1016/j.scs.2017.10.006.

Rahmandad H and Sterman JD (2012) Reporting guidelines for simulation-based research in social sciences: Reporting Guidelines for Simulation-Based Research. *System Dynamics Review* 28(4): 396–411. DOI: 10.1002/sdr.1481.

Reed DA, Powell MD and Westerman JM (2010) Energy Supply System Performance for Hurricane Katrina. *Journal of Energy Engineering* 136(4): 95–102. DOI: 10.1061/(ASCE)EY.1943-7897.0000028.

Rinaldi SM (2004) Modeling and Simulating Critical Infrastructures and Their Interdependencies. *th Hawaii International Conference on System Sciences*: 8.

Rinaldi SM, Peerenboom JP and Kelly TK (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine* 21(6). Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.2276&rep=rep1&type=pdf (accessed 25 November 2020).

Román MO, Stokes EC, Shrestha R, et al. (2019) Satellite-based assessment of electricity restoration efforts in Puerto Rico after Hurricane Maria. *PLOS ONE* 14(6). Public Library of Science: e0218883. DOI: 10.1371/journal.pone.0218883.

Sakurai M, Watson RT, Abraham C, et al. (2014) Sustaining life during the early stages of disaster relief with a frugal information system: learning from the great east Japan earthquake. *IEEE Communications Magazine* 52(1): 176–185. DOI: 10.1109/MCOM.2014.6710081.

Sandberg J, Holmström J and Lyytinen K (2020) Digitization and Phase Transitions in Platform Organizing Logics: Evidence from the Process Automation Industry. *Management Information Systems Quarterly* 44(1): 129–153.

Sanger DE and Perlroth N (2021) Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity. *The New York Times*, 14 May. Available at: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html (accessed 28 May 2021).

Sarker S, Chatterjee S, Xiao Xiao, et al. (2019) The Sociotechnical Axis of Cohesion for the Is Discipline: Its Historical Legacy and Its Continued Relevance. *MIS Quarterly* 43(3): 695-A5. DOI: 10.25300/MISQ/2019/13747.

Satariano A (2021) What is Fastly, the company behind the worldwide internet outage? *The New York Times*, 8 June. Available at: https://www.nytimes.com/2021/06/08/business/fastly-internet-outage.html (accessed 15 June 2021).

Savage E, Gilbert J and Radaskey W (2010) *The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid*. January. Metatech Corporation. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.734.5078&rep=rep1&type=pdf.

Scheffer M, Carpenter SR, Lenton TM, et al. (2012) Anticipating critical transitions. *Science (New York, N.Y.)* 338(6105): 344–348. DOI: 10.1126/science.1225244.

Seger E, Avin S, Pearson G, et al. (2020) *Tackling threats to informed decision-making in democratic societies – Promoting epistemic security in a technologically-advanced world*. Alan Turing Institute. Available at: https://www.turing.ac.uk/sites/default/files/2020-10/epistemic-security-report_final.pdf (accessed 4 November 2020).

Siegel N (2018) Using Systems Engineering to Create a Survivable Communications System that will Operate in the Presence of "Black Sky" Hazards. In: Madni AM, Boehm B, Ghanem RG, et al. (eds) *Disciplinary Convergence in Systems Engineering Research*. Cham: Springer International Publishing, pp. 959–972. DOI: 10.1007/978-3-319-62217-0_67.

Simon HA (1962) The Architecture of Complexity. *Proceedings of the American Philosophical Society* 106(6): 467–482.

Soltan S and Mittal P (2018) BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In: *Proceedings of the 27th USENIX Security Symposium*, 2018, p. 19.

Stockton P and EIS Council (2016) *Electric Infrastructure Protection (E-PRO®) Handbook*. Available at: https://www.eiscouncil.org/App_Data/Upload/3dadf58f-7457-46bf-92a4-551c6608d925.pdf.

Stockton P and EIS Council (2018) *Electric Infrastructure Protection (E-PRO®) Handbook III*. Electric Infrastructure Security (EIS) Council.

Taleb NN (2010) *The Black Swan: The Impact of the Highly Improbable*. 2nd ed. Random House Trade Paperbacks.

Taleb NN (2012) *Antifragile: Things That Gain from Disorder*. Random House.

Tarafdar M, Gupta A and Turel O (2013) The dark side of information technology use. *Information Systems Journal* 23(3): 269–275. DOI: 10.1111/isj.12015.

Tarafdar M, Cooper CL and Stich J-F (2019) The technostress trifecta - techno eustress, techno distress and design: Theoretical directions and an agenda for research. *INFORMATION SYSTEMS JOURNAL*. 111 RIVER ST, HOBOKEN 07030-5774, NJ USA: WILEY. DOI: 10.1111/isj.12169.

Tehrani PM, Manap NA and Taji H (2013) Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review* 29(3): 207–215. DOI: 10.1016/j.clsr.2013.03.011.

The Threat: The State of Preparedness Against the Threat of an Electromagnetic Pulse (EMP) Event (2015). Available at: https://oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/Caruso-Statement-5-13-EMP.pdf (accessed 28 May 2021).

Traywick C, Chediak M, Naureen S Malik, et al. (2021) The Two Hours That Nearly Destroyed Texas's Electric Grid. *Bloomberg.com*, 20 February. Available at: https://www.bloomberg.com/news/features/2021-02-20/texas-blackout-how-the-electrical-grid-failed (accessed 12 May 2021).

U.S. Department of Energy (2014) *Large Power Transformers and the U.S. Electric Grid (2014 Update)*. Available at: https://www.energy.gov/sites/default/files/2014/04/f15/LPTStudyUpdate-040914.pdf (accessed 9 May 2022).

Ustun TS, Cali U and Kisacikoglu MC (2015) Energizing microgrids with electric vehicles during emergencies — Natural disasters, sabotage and warfare. In: *2015 IEEE International Telecommunications Energy Conference (INTELEC)*, Osaka, Japan, October 2015, pp. 1–6. IEEE. DOI: 10.1109/INTLEC.2015.7572377.

Vaijhala S and Rhodes J (2018) Resilience Bonds: a business-model for resilient infrastructure. *Field Actions Science Reports. The journal of field actions* (Special Issue 18). Special Issue 18. Institut Veolia: 58–63.

Vial G (2019) Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems* 28(2). SI: Review issue: 118–144. DOI: 10.1016/j.jsis.2019.01.003.

Wang W and Lu Z (2013) Cyber security in the Smart Grid: Survey and challenges. *Computer Networks* 57(5): 1344–1371. DOI: 10.1016/j.comnet.2012.12.017.

Wessel L, Baiyere A, Ologeanu-Taddei R, et al. (2021) Unpacking the Difference Between Digital Transformation and IT-Enabled Organizational Transformation. *Journal of the Association for Information Systems* 22(1). DOI: 10.17705/1jais.00655.

Wilkinson A, Kupers R and Mangalagiu D (2013) How plausibility-based scenario practices are grappling with complexity to appreciate and address 21st century challenges. *Technological Forecasting and Social Change* 80(4): 699–710. DOI: 10.1016/j.techfore.2012.10.031.

Wilson C (2008) *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*. CRS Report for Congress, 21 July.

Wolff J (2020) Opinion | How Ransomware Puts Your Hospital at Risk. *The New York Times*, 17 October. Available at: https://www.nytimes.com/2020/10/17/opinion/hospital-internet-security-ransomware.html (accessed 28 May 2021).

Wright A (2005) The role of scenarios as prospective sensemaking devices. *Management Decision* Chaharbaghi K (ed.) 43(1): 86–101. DOI: 10.1108/00251740510572506.

Wright G and Goodwin P (2009) Decision making and planning under low levels of predictability: Enhancing the scenario method. *International Journal of Forecasting* 25(4): 813–825. DOI: 10.1016/j.ijforecast.2009.05.019.

Yoo (2010) Computing in Everyday Life: A Call for Research on Experiential Computing. *MIS Quarterly* 34(2): 213. DOI: 10.2307/20721425.

Yoo Y, Henfridsson O and Lyytinen K (2010) Research commentary—the new organizing logic of digital innovation: an agenda for information systems research. *Information systems research* 21(4): 724–735.

Zanella A, Bui N, Castellani A, et al. (2014) Internet of Things for Smart Cities. *IEEE Internet of Things Journal* 1(1): 22–32. DOI: 10.1109/JIOT.2014.2306328.

Zeiss R, Ixmeier A, Recker J, et al. (2021) Mobilising information systems scholarship for a circular economy: Review, synthesis, and directions for future research. *Information Systems Journal* 31(1): 148–183. DOI: 10.1111/isj.12305.

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.