sustainability

MDPI

Communication

Sustainable Digital Transformation of Disaster Risk—Integrating New Types of Digital Social Vulnerability and Interdependencies with Critical Infrastructure

Alexander Fekete [1,*] and Jakob Rhyner [2]

[1] Institute of Rescue Engineering and Civil Protection, TH Köln—University of Applied Sciences, 50679 Cologne, Germany
[2] Bonn Alliance for Sustainability Research/Innovation Campus Bonn (ICB), University of Bonn, D-53113 Bonn, Germany; rhyner@uni-bonn.de
* Correspondence: alexander.fekete@th-koeln.de

Received: 4 October 2020; Accepted: 9 November 2020; Published: 10 November 2020

Abstract: This article explores the relationship between digital transformation and disaster risk. Vulnerability studies aim at differentiating impacts and losses by using fine-grained information from demographic, social, and personal characteristics of humans. With ongoing digital development, these characteristics will transform and result in new traits, which need to be identified and integrated. Digital transformations will produce new social groups, partly human, semi-human, or non-human—some of which already exist, and some which can be foreseen by extrapolating from recent developments in the field of brain wearables, robotics, and software engineering. Though involved in the process of digital transformation, many researchers and practitioners in the field of Disaster Risk Reduction or Climate Change Adaptation are not yet aware of the repercussions for disaster and vulnerability assessments. Emerging vulnerabilities are due to a growing dependency on digital services and tools in the case of a severe emergency or crisis. This article depicts the different implications for future theoretical frameworks when identifying novel semi-human groups and their vulnerabilities to disaster risks. Findings include assumed changes within common indicators of social vulnerability, new indicators, a typology of humans, and human interrelations with digital extensions and two different perspectives on these groups and their dependencies with critical infrastructure.

Keywords: societal resilience; uncertainty; climate change adaptation; sustainable development; transhumanism; brain wearables; disaster risk management; artificial intelligence; contingency planning; cybersecurity

1. Introduction

People at risk, their resilience, or social vulnerability are key topics often highlighted in research and international agendas on sustainable development, disaster risk reduction (DRR), or climate change adaptation (CCA) [1–3]. However, while such agendas promote pro-active approaches, preparedness and transformation, research, as well as action, they mostly focus on human individuals, social groups, or communities as they are at present. The lineage of research that has brought innovation to the field of disaster research by emphasising the need to address a social vulnerability [4–7] typically focuses on existing social contexts. Some studies expanded the notion of this static picture by introducing frameworks that included dynamic pressures and causal models of development [4,8] to present detrimental situations that render people vulnerable [9], or "at risk" [4]. Preparedness and recovery studies often project perceptions of people and groups as they are now into the near future.

Transformation research does emphasise changes and future states [10]; however, in many cases, this is limited to either political developments or interactions of people with external changes, be it digital technologies or global climate change. Typically, social vulnerability assessments are snapshots of the present, and critique around such approaches has highlighted limitations of such static approaches [11].

Another topic evolving at the moment is critical infrastructure (CI) which covers electricity, water, food, and other supply and investigates dependencies of humans on such services [1,12]. While such dependencies have long existed, there is growing interest in how more development and higher rates of the provision of such infrastructure services lead to a vulnerability paradox. This paradox states that the more development takes place, people adapt their life to infrastructure services being reliably available, and hence become more vulnerable to shocks when this supply is suddenly interrupted [13]. The development of CI at the moment is driven by the digitalisation of so-called smart grids and smart meters for a better distribution of power consumption to the individual smart homes [14]. While this has many benefits of reducing power consumption and thereby reducing CO_2 emissions and enables control and monitoring of users at home as well as by the utility providers, certain caveats also are addressed in research. These caveats include the possibilities of cyber-attacks and an increasing dependency on the information provided remotely [15]. CI, therefore, is a field demonstrating the transformation from purely physical to semi-digital types of infrastructure. And in the field of CI protection, conceptual transformations also include a change from viewing CI only as technical infrastructure to include human users and maintenance staff being part of this infrastructure as much as the environment in which they operate [16].

While there is growing awareness on the close interlinkage between social vulnerability and CI, current literature hardly addresses the possibility that people or groups themselves may change by their exposure to digital services, and new groups may occur. Aspects of digital transformation in technologies such as Early Warning [17], social media analysis [18], and related virtual crisis operation groups [19] are addressed at the present state, but there is no conceptual overview on the range of social digital groups or, which new types of human or semi-digital human groups may evolve in the future. This article focuses on exploring the repercussions for disaster risk reduction (DRR) [1], climate change adaptation (CCA) with relation to disasters as extreme events [3], and sustainability [2].

This article aims to provide a conceptual overview on the impacts of digital transformation on how social vulnerability and human risk groups have to be reconsidered to include not only already existing physical human beings, but their digital extensions as well.

We are focusing on the question of how vulnerabilities of human and semi-human groups will develop in view of an on-going digital transformation.

This objective is addressed by the following specific research questions:

- How can the concept of social vulnerability be extended to new semi-digital contexts?
- Which interdependencies with digital and physical critical infrastructure have to be taken into account?

While it is fully acknowledged that with these new developments, not only risks but also chances emerge, the main focus of this paper is on vulnerabilities and risks, since chances are widely studied already. Current developments such as the vast possibilities of robot services in search and rescue, communication, forecast, Industry 4.0 for reconstruction, etc. are not the main focus of this article since the ambition is to capture a bigger picture of implications by and for novel human and semi-human groups and not on single technological developments. The aim is to highlight areas for future research on these topics and to suggest possible methodologies for this kind of research. The article especially intends to characterize human and semi-human groups concerning their social vulnerability, and how it may transform in context to on-going digitalisation, particularly in view of evolving digital infrastructures.

This paper will conduct a brief assessment of the background of social vulnerability, critical infrastructure, and digital transformation research in Section 2, then identify specific indicators for

characterising social vulnerability at present and for future applications in Section 3. Section 3 also investigates which adjustments of such indicators are conceivable when dealing with emerging novel groups of vulnerable humans and semi-humans. In Section 4, a conceptual framework outlining a typology of such groups and implications for further theoretical frameworks is presented, especially concerning critical infrastructure service dependency.

2. Interrelations of Social Vulnerability, CI and Digital Transformation

Within sustainable development, DRR and CCA, mutual interactions and interdependencies between humans and their environment are analysed, often within a system theory understanding [20]. The system environment consists of both natural and man-made elements and processes and in DRR is perceived mainly regarding impacts on humans and society, for instance, through natural hazards such as earthquakes or floods, or man-made hazards and threats such as technical failures. Humans also interact and (re)shape their environment, for example by river training or deforestation, and also create their own built environment including supply infrastructure. This interrelation is then expressed as a social-ecological or social-environmental system (SES) [21,22]. With the on-going digital development, this article aims to investigate how it reshapes the human system environment, and hence, human vulnerability to hazards, both natural and technical. This may imply reconsidering SES as social-digital-environmental system in the future.

2.1. Human and Social Vulnerability

Vulnerability studies emphasise the deeper analysis of factors on the impact side of stressors, hazards, and changes [23]. Research on vulnerable people and groups has emerged from humanitarian aid and development cooperation [6], especially from impressions from on-site work of practitioners in areas affected by disasters such as refugee camps [24], taking into account needs and skills of affected people [25]. Based on a critique of the dominance of hazard, physical, technical, and organisational foci on disaster risks [7], the emphasis has been given on social, cultural, political, economic, and other conditions and drivers that also render people "at-risk" [4]. This led to a stream of research on what is termed social vulnerability or community resilience [5,26], also currently known as societal resilience [27]. While pressure and release frameworks have their origins in fields of dose-response models [28] and include notions of "dynamic pressures" linked to "root causes" [4], they do not explicitly guide new types of social groups, especially not for digital social groups. In this line of research, a focus on existing groups and on (historical) drivers is predominant. It is also necessary to note the difference to the term "vulnerability," as it is used within information technology for systemic security risks [29]. In different hazard contexts or depending on culture and language, similar terms are used, such as "at-risk groups" or "risk groups" concerning COVID-19 [30,31]. While transformation has become a recent focus in some areas related specifically to social-political conditions and concerning global climate change [10], there is less research on the interrelations between the digital transformation and social vulnerability or critical infrastructure.

While social vulnerability and community resilience mostly address groups of people, there is also research on individual vulnerability. Less clearly defined and used in varying notions ranging from individuals to groups is the term human vulnerability, for example. However, as with social vulnerability, human vulnerability research also mainly addresses existing humans and their characteristics [32–34], not future or digital vulnerabilities related to disaster risk. Individual factors that render people at risk to disaster or crisis impacts are covered in related fields such as risk perception dealing with fear [35]. Individual or group-related social aspects of overcoming crises are also found in fields dealing with psychology and sociology to other types of risks than just natural hazards [36,37]. However, there is a lack of integration between the individual and group aspects of different fields of research on fear, threats, or hazards already, and the more so concerning future forms of vulnerabilities and resilience.

2.2. Critical Infrastructure and Cybersecurity

Critical infrastructure research deals with the determination of the relevance (termed criticality) of supply infrastructure services such as water, food, electricity, heat, information, etc. for governance and society [12,38]. In humanitarian and security research, related terms are lifelines or vital assets [39,40].

From a critical infrastructure perspective, the interdependencies between humans and technological products and services increase, especially within information technology and electricity [41,42]. This dependency of human daily life on infrastructure services, aggravated in times of crises, is already one of the key vulnerabilities of human societies [43,44]. Research on critical infrastructure mainly deals with technical aspects, threat assessment, failures, and interdependencies aggravating hazards and cascading effects in a field called Critical Infrastructure Protection—CIP [38,45]. It does take into account the digital transformation in terms of cybersecurity and smart grids, etc. [14]. This field of CIP is therefore dealing more with digital transformation than social vulnerability research so far; however, it often neglects the human and social dimension [16]. Even under the term Critical Infrastructure Resilience [46], aspects of human agency and vulnerability only begin to be introduced to assessments and decision support models [47,48]. The field of CIP or resilience is also connected to Supply Chain Risks [49] and Business Continuity Management [50], that both are affected by the digital transformation, but also do not focus on human agency that much yet. The Corona SARS-CoV2 pandemic has helped to raise global and individual awareness about the dependency on daily goods and infrastructure services [51,52]. Key personnel has become known as "system-relevant" [53]. However, since this virus only affects physical human beings, the digital aspects and semi-digital groups have not been included in the notion of social vulnerability research yet.

2.3. Digital Transformation and Transhumanism

Digital transformation concerning risk and security research includes developments in the fields connected to the internet, mobile devices, artificial intelligence, Industry 4.0, robotics, or internet-of-things already [15,54–56]. Digital transformation of health-care systems such as hospitals or public health services is analysed given how patient-doctor interaction may change due to online meetings or monitoring of health parameters by wearable devices [57,58]. However, there is still little research on how human behaviour or social groups will emerge or transform, in contrast to the analysis of technical and organisational opportunities and certain ethical questions. Research on new applications of brain implants for restoring eyesight or mobility after paralysis is prevalent in fields such as biomedical engineering, neuroscience or psychology; however, it is hardly connected to questions of human and social vulnerability, which is of particular importance in the connection with disaster risk.

Digital transformation inspired the research of transhumanism, which influences related fields such as sustainability or cybersecurity already. A theory within the transhumanist idea [59–61] states that robotics and digital technologies have become elaborate enough that humankind will soon enter the next level of hybrid coexistence with technology and even transcend into a "singularity" [62], also related to cyberspace or metaverse, as a kind of digital universe. While this seems a still distant future, new developments such as "neurotechnologies" (e.g., brain wearables) raise awareness that some changes already take place, which may lead to a "global mindset change" [63]. Critically reflecting upon it [64], characteristics for the transhumanist movement show signs of an overall belief in biomedical enhancement, technology, grappling with exciting upcoming technologies, and a keen interest for future developments sparked by technological inventions. The strong interlinkages with technology and materialism are also taken up in research on posthumanism, technogenesis, or new materialism [65]. Technological impact assessment analyses technological advancement, taking into account technical as well as ethical aspects [66]. Research on human aspects of co-development with new technologies can result in cultural and ethical questions, too. Whether such phenomena are only the result of technological change or also due to social/cultural transformation is a topic in research [67] with recent conceptual developments indicating an integrative or inclusive approach [68]. In summary,

digital transformation applications are developed, but social vulnerability aspects are not integrated yet. Additionally, there is a lack of integration of existing risk and disaster conceptual frameworks with theoretical developments of digital transformation.

2.4. Transformation of Crisis and Disaster Management

Application of digital new products and also those in connection to new forms of digital social groups are already being used widely in disaster risk management in certain fields. Examples are BigData [69,70], crowd mapping [71], social media mining [72], Volunteered Geographic Information [73], Virtual Operation Support Teams [19], rescue robotics [74], unmanned aerial vehicles (UAVs) [75], wireless sensor networks [76], and many more. Tensions between formal "command-and-control" and informal social media activated self-organising information is a typical example on how digital transformation plays a role in many areas of disaster risk management at the moment, be it dealing with COVID-19 [18], volunteers appearing to help in flood risk management, or daily emergency management [77]. The implications of digital transformations on command and control paradigms would warrant another article, but social vulnerability is a major gap and will be addressed first. Humans are mainly regarded as personnel and affected people are summarised as "population" in many cases. Critical infrastructure dependencies receive much awareness [43], but as mentioned in the sections above, the connection between social vulnerability and critical infrastructure is hardly made yet. As an intermediate conclusion, new forms of digital social groups and their social vulnerabilities need more research in disaster risk management as well as in sustainable development.

3. Modifications of Social Vulnerability

In this section, social vulnerability indicators are selected as an example to outline methodological implications of change through the digital transformation. This selection is based on the relative coherence of such indicators that over decades have continued to use the same variables with few modifications and variations worldwide [11,28,78,79], being aware that there is also a critique on such indicators—for example, for not fully addressing human characteristics, or being reliant on data and others [80]. Based on the assessment of the state of the art presented above and on social vulnerability indicators in literature, further conclusions are derived on this section (a) on how existing social vulnerability indicators may have to be reconsidered and (b) which new indicators might become relevant for semi-digital and digital vulnerable groups.

3.1. Modifications of Social Vulnerability Indicators of Existing Groups

With an ongoing digital transformation, it may become relevant to reconsider and if necessary expand traditional social vulnerability variables or indicators, such as age, social group/ethnicity, knowledge, language skills, etc. [78]. Novel social vulnerability aspects may emerge and will have to be included, such as degree of digitalisation, smart grids, cities, dependency on energy, information supply, and other factors. The range of disaster risks therefore covers a wide range typically used in critical infrastructure research but also increasingly, in disaster risk reduction; the so-called all-hazard approach that integrates natural and man-made hazards [81]. This broad approach is based on the recognition that not only hazards themselves must be analysed, but vulnerabilities as well [82]. Based on context, vulnerabilities, as well as hazard impact chains, differ. Factors influencing vulnerability may have different (positive and negative) effects on different vulnerabilities, and some factors may be uninfluential as well [11]. The following Table 1 shows examples of certain demographic characteristics typically used in social vulnerability indicator research [78]. Table 1 shows the underlying hypotheses and what these characteristics mean for higher or lower vulnerability to disaster risks. Furthermore, it projects a possible change within these characteristics when the current trend of digital development and internet interconnectivity continues. Certainly, based on hazard or cultural, economic, political, or situational context, these vulnerability indicators must be analysed differently [11,28,82]. While these are still projections, they help to illustrate how important it is to document the underlying hypotheses

and assumptions for later studies that might use the same characteristics but interpret them differently concerning theoretical implications for vulnerability. It also shows certain future developments and possible modifications of underlying assumptions that have to be taken into account today when applying agendas such as the Sendai Framework that enacts measures until 2030 [1].

Table 1. Common indicators of social vulnerability and assumed changes.

Demographic Characteristics	Indication Hypothesis Today	Indication Change Hypothesis for the Year 2100 [1]
(Old) Age	Old age means higher vulnerability due to increasing health issues and dependency on other persons and services	Vulnerability decreases due to better health care system, technical monitoring, and support systems, but vulnerability in terms of technical dependency increases
(Very young—baby) age	Same as cell above, but dependency on parents greater (on average)	Same as cell above
Functional needs (water, food, etc.)	Vulnerability is similar to most people, but access (distance, time, income) makes a difference	Vulnerability decreases: more automated food delivery, smart water systems
Language proficiency	Higher vulnerability when warning messages cannot be understood	Vulnerability decreases: automated language translation on the fly
Diversity: race and ethnicity, family structure, gender	Different human group attributions render them vulnerable or resilient. Social media groups have emerged with new options of sharing knowledge or even disaster help thus reducing vulnerability	Diversification of human groups expands (degrees of semi-humanisms and robots), while certain digital devices connect traditional groups and create novel (digital) social groups

[1] Assumed change: more digital technology, more interconnectivity.

3.2. Adding New Types of Humans and Social Groups to the List of Vulnerabilities

Implementing new vulnerability indicators will first mean to raise awareness of future developments of emerging new groups of humans. These humans will increasingly interact and later blend in with digital technologies. As it may sound like distant future topics, it is important to highlight that certain interrelations between humans and machines and digital technology already exist, that we outline below. While this may still have very limited application, it can see rapid development as soon as certain technologies become available.

At present, social vulnerability indicators mainly deal with physical human individuals or physical human groups (Figure 1). Humans also already use or wear technical extensions of many kinds which represent already existing dependencies—for example, bicycles or cars for mobility, infrastructure for power or water supply, clothing for protection, and so forth.

Risks exist in the form of an acquired dependency which humans often realise only during loss or failure [83]. Concerning vulnerability, this becomes apparent at the example of prosthetics of any kind, such as crutches, as well as machines for dialysis which constrains people to evacuate in a disaster. As another type of technical gear or equipment, all kinds of computers, mobile devices, or wearables such as watches typically symbolise digital transformation. However, just as with crutches (Figure 1), these can still be put on and off, and are not necessarily connected to the internet or digital information sensors. Therefore, they can be grouped into the upper part of Figure 1, symbolising existing predominantly physical individuals and groups. The first extension, however, is recognising that there may be groups of people or individuals that carry specific vulnerability characteristics based

on their regular usages, such as prosthetics, machines, or other physical dependencies. Such physical dependencies of course also include emotional detachments to other human beings or groups such as family or relatives, friends, and even pets that play an important role in determining risk behaviour such as readiness for evacuation [84,85].

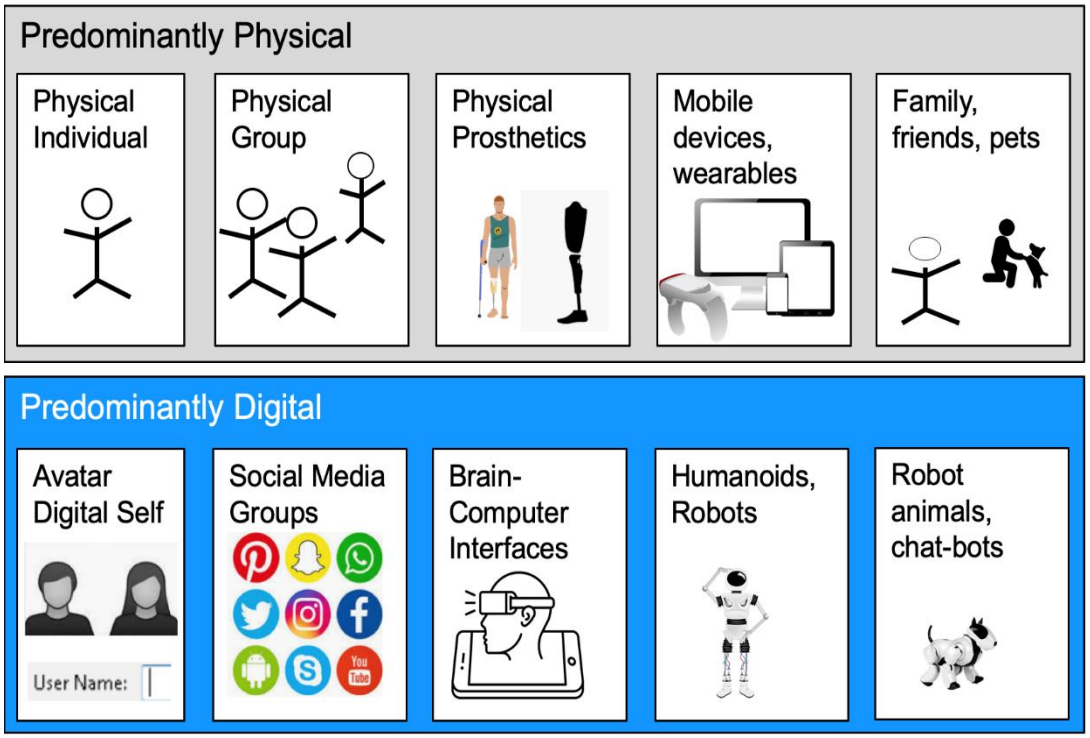

Figure 1. Expanding the range of "vulnerable people and groups."

The lower box in Figure 1 then symbolises predominantly digital individuals or groups. Many humans are familiar with login-ins to internet profiles or social media groups already. Social media groups are an example of already existing groups of people interconnected by a common topic of interest, thereby exposing certain peculiar vulnerabilities, too. For example, hazard exposure to cybercrime, susceptibilities to fake news, and so forth. This is connected to individual profiles of users, too. Some users use visual representations of themselves by a photo uploaded or are using a digital representative, an avatar. The digital self is a disembodied representation or upload of a human profile and permits symbolic interaction with others, which also has implications on behaviour [86]. For vulnerability characteristics, this has important implications beyond exposure related to physical presence but including changes of behaviour and personality. Caveats must be expressed concerning this schematic representation of types of vulnerable individuals and groups, too. For example, it is often stressed that not all humans are connected to the internet, depending on broadband access [87]. Moreover, gender, income, location, risk behaviour, or other factors can result in digital inequalities [88] or different forms of equity [27]. It is important to consider in future vulnerability research that this also means that common ideas about indicators may change during a human life as well as vary between groups. The subsets of young adult groups, for instance, may differ into those whose life is predominantly digitised and those who are not. Age groups themselves must be even more differentiated than is the case now. Interruptions of digital or power supply through the supporting infrastructure due to disasters may make them more vulnerable than those who are qualified as vulnerable by physical indicators alone. As another side-effect, certain vulnerability groups (elderly, poor, minorities, etc.) could be further marginalised if they cannot catch up with advancing technologies, the so-called digital divide. Risk literacy will also have to take those transformations into account and create more awareness on dependencies of different vulnerable sub-groups.

The schematic representation (Figure 1) also tries to include the range from purely physical over temporarily digital to fully digital individuals and groups. Therefore, novel and upcoming machines and interfaces are also included, which may represent digital extensions and "prosthetics" such as robots, chatbots, and robot pets (Figure 1). Just as with existing physical beings and machines, it can be expected that humans will become reliant on them, too—for example on medical robots for surgery [89], or healthcare robots [90]. Again, this creates external dependencies, and in some cases also emotional attachments. Additionally, biological-technical interfaces are being used already that generate a permanent interrelation between humans and machines. While the announced "brain-computer interface" by the company Neuralink, owned by Elon Musk, raises awareness as well as ethical concerns [91,92], there are already existing examples. Electronic implants in the brain have been used for restoring rudimentary eye-sight capability for a blind man called "Jerry," who had electrodes implanted and connected to a camera mounted on his eyeglasses in 1978 [93]. A colour-blind person from the UK with a camera connected to his brain was termed "cyborg" in his passport for international air travel [94]. A fully paralysed person after a cycling accident had his reaching and grasping ability restored by similar technology [95]. Using electroencephalography (EEG), controlling of computer cursors, for example, by brain activity are also installed in so-called brain wearables, that can be worn and taken off just like headphones [93,96,97]. This summarises some developments that expand the digital and technological capabilities of humans and introduce new susceptibilities such as loss of devices or special treatment and care during evacuations, for example.

Regarding specific hazard exposures, attackers may jeopardise the internet, which could especially affect devices such as brain wearables or brain-interfaces. Information for control, regulation, or intelligence of the wearables can be compromised. Additionally, life support systems will become much more vulnerable to attacks and also, to natural hazards. Examples are a woman hit by lightning while carrying an implant [98] or a human "cyborg" allegedly being "hacked" [94]. These are still rare anecdotes, but can be expected to occur more often, not by exposure to lightning or malicious attack alone, but due to technical problems. In summary, there are novel characteristics concerning social vulnerability to take into account in a range from humans completely without electronic or digital devices, to humans carrying devices to biological-digital interfaces on to fully digital hardware and software (Table 2).

Table 2. Typology of humans, and human interrelations with digital extensions.

Humans without Digital Access to Information	Humans with Some (Removable) Access to Digital Services and Machines	Humans with Digital Implants	Hardware, with a Digital Interface	Software
Certain Tribal indigenous groups Elderly citizens Sick or disabled people Homeless Temporarily without access Voluntarily without access Prisoners Children	Social web-based networks Job-related access Private access (Brain) wearables Other mobile devices (phones, etc.)	Medical enhancement (hearing, heart, prostheses) Brain implants for information enhancement or access	Computers Mobile devices (from Nano to Macro) Robots Androids	Software Uploads of humans (bots with voice and memory of deceased, etc.)

3.3. Adding New Social Vulnerability Indicator Criteria for Semi-Digital or Fully Digital Groups

Based on the identification of vulnerable individuals and groups above, and common social vulnerability aspects [4,11,28,78], additional aspects to consider for future assessments are outlined (Table 3). The relation of vulnerability to hazard-exposure, susceptibilities, and capacities/resilience follows common approaches in vulnerability research [23,28,78].

Table 3. New vulnerability aspects of semi-digital and digital vulnerable individuals and groups.

Vulnerable Individuals and Groups	Specific Hazard-Exposure	Susceptibilities	Capacities or Resilience
Avatar, Digital Self	Electromagnetic storm or impulse, identity theft, deepfakes	Backup, data coherence, and updating Accessibility to a person	Stored and processed information and algorithms
Social Media Groups	Electromagnetic storm or impulse	Fake news, data coherence, and updating Access by everyone	Shared information and storage
Chat-bots	Electromagnetic storm or impulse	Information coherence and updating Access by everyone	Stored and processed information and algorithms
Brain-Computer Interface individuals	Lightning, hacking, day and night exposure	Biological and electronic susceptibility, access restriction, updating	Embedded availability
Humanoids, Robots	Roads, transport, charging points	Physical susceptibility, climatic conditions, maintenance, updates	Mobility
Robot animals	Roads, transport, charging points	Physical susceptibility, climatic conditions, maintenance, updates	Mobility

Table 3 only shows examples and such that are specific for each group. Hazard-exposures to internet and electricity are assumed in various degrees for all groups and are therefore not mentioned, and likewise, susceptibilities to cyberattacks. Both groups are exposed to natural and man-made hazards of many kinds, with the difference that online representations or data from individuals or groups experience losses indirectly through the hardware they are hosted on, or supply infrastructure. All are exposed to electromagnetic storms or impulse, but losses vary in degrees depending on whether they are just hardware carrying software that can be reprogrammed, or whether they purely exist online and hence may risk losing all identity in case all memories are erased by the same event. There exist specific threats such as deepfakes which undermine the credibility of video content, just as forging maps and photos are problems in the physical world, too.

All groups in Table 3 share susceptibility related to cybersecurity problems or system crash. What differs is the physical susceptibility of external devices (robots, UAVs, etc.) that are similar to physical human beings or machines. Furthermore, internal devices such as brain implants differ again since they are personal, hence related to or dependent also on physical susceptibility of the human body. But they are susceptible both to electronic connections as well as to the biological environment inside the body. Purely digital representations such as avatars or social media groups or chat-bots are highly susceptible to online loss of memory. They are also susceptible still to interaction with humans and other external devices in moments when backups, maintenance, and updates are installed.

Capacities, capabilities, and skills to compensate such vulnerabilities may directly address and counter such exposures or susceptibilities. This is a wide range and again, Table 3 is not at all exhaustive, it rather resembles a starting point for further consideration. Specific capacities may include protection, backup, and emergency management devices and processes just as they exist in the physical world. What is a bit different is the huge global decentralisation of memory such as cloud space and the

internet. Even a huge solar storm typically affecting regions close to the poles [99] should leave areas near the equator unharmed, therefore allowing the restoration of many copies of personal identities and data content. Interestingly, privacy protection and decentralised control and storage of data may constrain the recovery of data for disaster events that affect large areas such as solar storms or power blackouts. Mobility of robots in a physical sense is an advantage in an evacuation if such machines are permitted autonomy or are programmed accordingly. Resilience in an encompassing meaning or in the sense of robustness, redundancies, and other aspects [100] would warrant further analysis than briefly outlined here.

What needs to be added, when considering future changes, is the rise in digital devices that are connected to the individual in a way that they become part of the human body. For example, a leg prosthesis is carried during daytime activities and a brain implant for hearing is always with the human. These transformations bring their own novel needs and dependencies, but some other physical dependencies of the biological body do not exist anymore, and are hence not a vulnerability anymore.

4. Interdependencies with Critical Infrastructure

Dependency on supply infrastructure such as water, food, energy, etc. is also termed "critical infrastructure" when a failure of delivery can result in death, detrimental health effects, or other damages [12]. Non-physical services such as information, knowledge, regulations, and law enforcement, etc. can also become critical, especially, of course, in crisis situations. Critical infrastructure research has raised awareness of the dependency of humans on such infrastructure services, as well as awareness of the intricate interrelations between many modern infrastructures that render them interdependent, be it through physical (shared location), cyber-related (information), or other means [45].

Socially vulnerable groups are already dependent on a range of infrastructure services for physical survival (food, water, heating etc.), logistics, and transport for such goods, but also on emergency teams and a range of other infrastructures (Figure 2). It is assumed that vulnerabilities and dependencies will change when humans are increasingly reliant on mobile phones, wearables, or robots to assist them. Apart from this dependency, digital resources are also prone to rather new forms of loss (digital memory loss) and specific hazards (cyber-attacks), etc., even more so, of course, if human knowledge is uploaded and stored in digital form (see Sections 2 and 3).

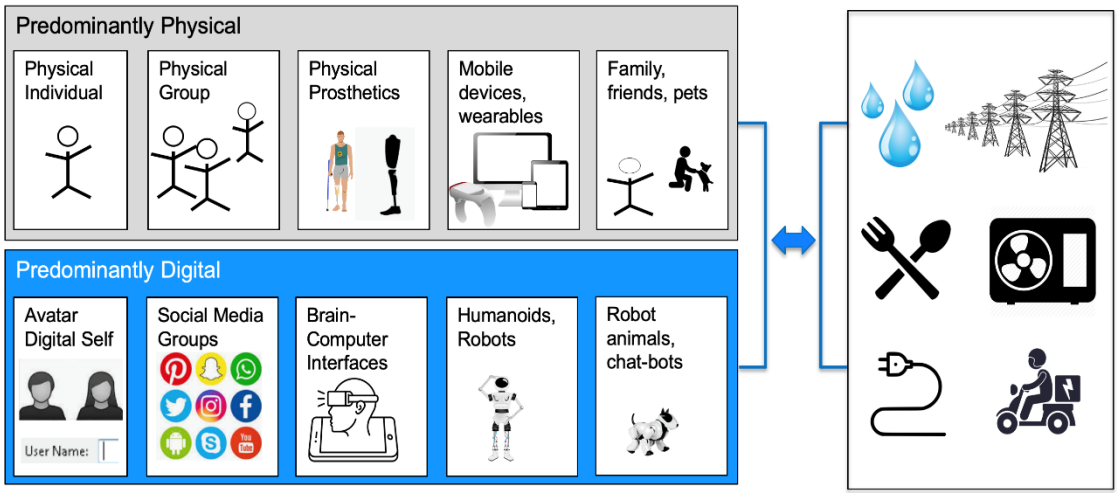

Figure 2. Expanding the range of "vulnerable people and groups" and their dependency on infrastructure.

However, it may be hypothesised that the criteria for analysing such vulnerabilities and dependencies are also dependent on the observation model applied. Hence, it could be interesting to map out the existing observation model of the human being as an individual (Figure 3) and expand it to include dependencies on first order assistants and services (those that are used mainly as personal

devices by that individual) and second-order dependencies [45] on devices shared with many other users. Biological and digital self both possess first order devices or tools, machines of their personal perusal. But the "self," as well as the devices, are also dependent on the second-order of other devices and services often outside their immediate control, such as the electric grid or water pipes, etc. Figure 3 thereby represents an interdependency model of humans in exchange with other infrastructure surrounding them.

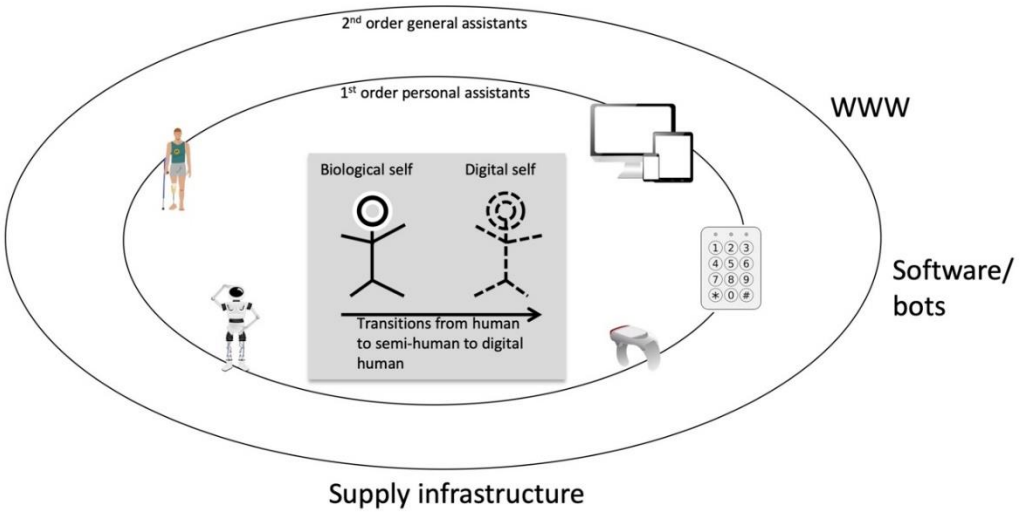

Figure 3. Interdependencies from an ego-centric (individualistic) view on first and second order assistants and infrastructure.

An alternative model to the individualistic representation above would be placing the internet into the centre and humans into the role of second-order assistants providing empirical knowledge uploads into the shared memory and knowledge (Figure 4).

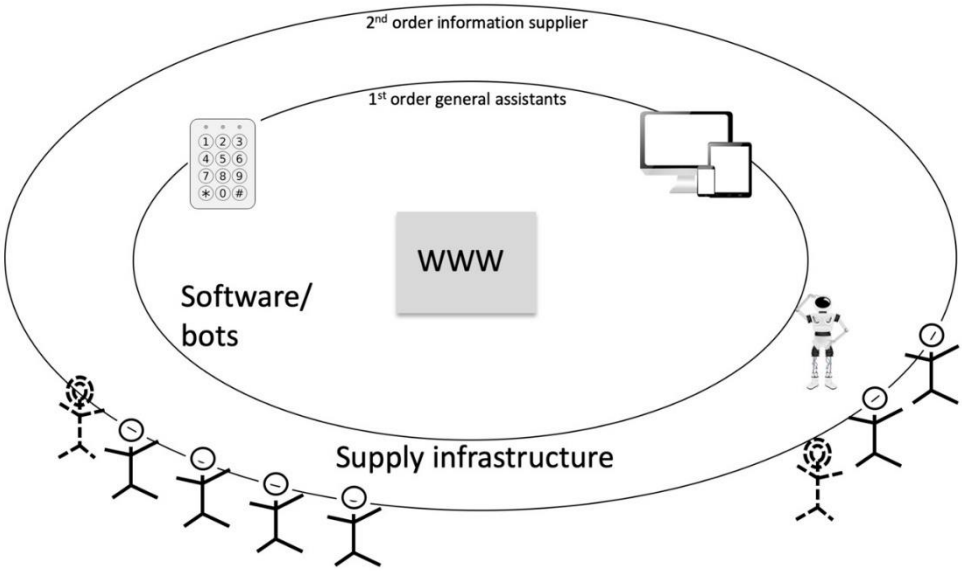

Figure 4. Interdependencies from an internet-centric view on first and second order assistants and infrastructure.

Both representations (Figures 3 and 4) are different perspectives and highlight a different aspect of the entire human digital system. For explanatory purposes, it helps to contrast both models, since the

vulnerabilities and dependency views on, for example, supply infrastructure vary, depending on the analytic perspective.

The general difference between human and digital aspects mainly lies in biological needs versus purely digital needs. However, even software and code (still) require certain physical storage such as hard drives or biological cells. Therefore, even software does not fully omit physical vulnerability to destruction by, for example, an earthquake or solar storm. So far, these differences are hardly included in any risk or resilience framework, and therefore Figures 1–4 outline some of the conceptual differences when analysing risk, resilience, or vulnerability according to the different groups of humans or digital individuals or groups.

While Figures 3 and 4 are perhaps oversimplifying, they may serve as starting points for more elaborate frameworks to be developed that capture social vulnerability, critical infrastructure, and digital transformation. The choice of perspective is important since, at the moment, the biological and physical health of the human body is considered a priority. However, since more and more human knowledge and culture are digitally uploaded, and since social media groups and online representations develop their own culture, it will be helpful to reconsider priorities and perspectives and level up digital data and knowledge. Currently, discussion of priorities between values to protect such as human lives in balance with economic survival and personal freedom are visible in the SARS-CiV2/COVID-19 pandemic. And in literature, new risks and risk groups are debated, as well as vulnerability characteristics such as digital inequalities, but also capacities such as " ... the digitally resourced have additional tools to mitigate some of the risks associated with the pandemic" [101]. Similarly, this discussion needs to be extended on digital representations of human and social groups when it comes to questions of protection and resilience.

5. Conclusions

This article has investigated how future vulnerabilities of various emerging human and semi-human groups might develop in view of an on-going digital transformation. Breaking down this encompassing main question, two fields have been addressed specifically; social vulnerability and critical infrastructure. It has been identified that within social vulnerability research on indicators, static perspectives of existing human individual and social groups prevail. New forms of humans and groups that emerge due to the digital technologies existing already are not included in many social vulnerability assessments. In the same vein, critical infrastructure and social vulnerability only begin to be integrated as digital transformation is a good example to outline these interdependencies. Additionally, dependencies of human individuals and groups on their immediate first order and also second-order infrastructure supply will increase during continuing digital development. But depending on the conceptual framework and perspective, these dependencies become interdependencies when humans become part of the digital infrastructure. The article outlines assumed changes within common indicators of social vulnerability (Table 1) and sets up a typology of humans, and human interrelations with digital extensions (Table 2). It suggests new vulnerability aspects of semi-digital and digital vulnerable individuals and groups (Table 3) and visualises these groups and their dependencies with critical infrastructure (Figures 1 and 2). To illustrate the range of first and second-order interdependencies, two juxtaposing schemes show the individualistic versus the internet-centric arrangement of first and second-order assistants and infrastructure (Figures 3 and 4). This intends to support future research on (i) identification of new digital vulnerable groups, (ii) their vulnerability characteristics, and (iii) integrating these characteristics with existing concepts and indicators of social vulnerability. It furthermore aims at (iv) assisting the assessment of dependence of socially vulnerable individuals and groups on infrastructure. Overall, this will also contribute to v) tracking digital transformation and (vi) developing conceptual frameworks that integrate social vulnerability, critical infrastructure, and digital transformation.

Digital transformation could imply several future states. One could be that risk management would be governed still primarily by humans concerning the final overview and taking major decisions.

This could be challenged by software and machines being much better capable of healing humans and identifying illnesses or vaccines. Additionally, information processing speed in the analysis of complex interdependencies is especially helpful in disaster events. However, it also plays out for long-term planning processes such as climate change or droughts when crisis signals can be detected well in advance and small but broadly distributed adjustments can be efficiently coordinated. A major advantage of machines deployed in rescue operations and firefighting is not risking human lives. The question seems not if machines and software will increasingly be deployed for both planning and action tasks, but to which degree they can take decisions autonomously.

Some limitations and shortcomings of this article must be emphasised, too. For example, the article is based on the assumption that the interdependency between man and digital technology will increase in the long-term until the year 2100. While there are many good reasons for this assumption, it is not the only possible development, and in this sense strictly speaking a hypothesis or speculation. Different scenarios of different transformations and also hazard events can help to better explore the role and interdependencies between man and digital technology in further investigations. However, predictions are difficult, since they are based either on recent contexts and imagination [102] or taking into account temporal, cultural, and many other contexts that are dependent on the body of knowledge, attitude, and intention, but also on windows of opportunity and time-lags. As an example, resilience has emerged as a broadly used concept in many academic disciplines in recent years while it had already been discussed in certain disciplines of ecology or risk in the 1970s or even earlier [103]. As another example, artificial intelligence had seen major discussions in many system science fields in the 1980s with many discussions even stemming from research on computation or complexity even much earlier, too [104]. In this article, examples such as brain wearables are used to build up an assessment of likely impacts on composition and vulnerability of human and emerging semi-human groups. Therefore, this paper does not aim to give a unique prediction, but to contribute to a more general foresight, by working out one scenario and investigating it in view of new vulnerabilities for its actors, namely human and semi-human groups.

The history of disaster risk management could be told as a transition from complete individual or at least group autonomy without any use of "digital elements" to a gradually increased use of and co-existence with technical/digital entities and structures. The dependence of humans on digital technology has become very high in general, which should also be more researched in the future in connection with the growing role of digitalisation in sustainable development, DRR, and CCA. This could also imply a concomitant gradual decrease in the level of human control of operations. The transformation of human groups and their infrastructure support dependencies will continue under the developments driven by digitalisation. Acknowledging this will first of all demand rethinking human-environment interactions as social-digital-environmental systems. But how overall sustainability and risk management will transform and what this implies for the need to control will need to be investigated further in future studies.

Author Contributions: Conceptualization, Writing—original draft, Writing—review & editing, A.F. and J.R. All authors have read and agreed to the published version of the manuscript.

Funding: For Jakob Rhyner, support through the project "digitainable," funded by the German Federal Ministry for Education and Research (BMBF), is gratefully acknowledged.

Acknowledgments: The author is grateful to Roland Benedikter for his inspiring keynote on "Human Enhancement: An Example of the Growing Divide on How to Link Nature and Technology in the Age of Their Convergence" at INQUIMUS 2017: "INQUIMUS into Action—How can scientific assessments inform decisions for problem-solving in practice?", 19–21 September 2017, in Bolzano, Italy and the organisers Stefan Kienberger and Stefan Schneiderbauer of the workshop series "INQUIMUS—Integrating quantitative and qualitative assessment methodologies for multi-dimensional phenomena". Appreciation is expressed towards the session moderators and other speakers at the session "How will we save lives? Safeguarding Populations: The Impact of Digital Revolution", at the 6th Turkish-German Frontiers of Social Sciences Symposium, Alexander von Humboldt Foundation—Stiftung Mercator—Koç University, "Moving forward: The impact of the digital revolution on societies", 1–2 Oct 2020, held online.

Conflicts of Interest: The author declares no conflict of interest.

References

1. United Nations. *Sendai Framework for Disaster Risk Reduction 2015–2030*; United Nations: Geneva, Switzerland, 2015.
2. United Nations. *Transforming Our World: The 2030 Agenda for Sustainable Development. Resolution Adopted by the General Assembly on 25 September 2015*; United Nations: Geneva, Switzerland, 2015; p. 35.
3. IPCC. *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change—IPCC*; Barros, T.F., Stocker, D., Qin, D.J., Dokken, K.L., Ebi, M.D., Mastrandrea, K.J., Mach, G.K., Plattner, S.K., Allen, M., Eds.; Cambridge University Press: Cambridge, UK; New York, NY, USA, 2012.
4. Blaikie, P.; Cannon, T.; Davis, I.; Wisner, B. *At Risk—Natural Hazards, People's Vulnerability and Disasters*, 2nd ed.; Routledge: London, UK, 1994.
5. Bohle, H.G.; Downing, T.E.; Watts, M.J. Climate change and social vulnerability: Toward a sociology and geography of food insecurity. *Glob. Environ. Chang.* **1994**, *4*, 37–48. [CrossRef]
6. Cuny, F.C. *Disasters and Development*; Oxford University Press: New York, NY, USA, 1983.
7. Hewitt, K. (Ed.) *Interpretations of Calamity. From the Viewpoint of Human Ecology*; Allen & Unwin: Boston, MA, USA; London, UK; Sydney, NSW, Australia, 1983; p. 304.
8. Asghar, S.; Alahakoon, D.; Churilov, L. A comprehensive conceptual model for disaster management. *J. Humanit. Assist.* **2006**, *1360*, 1–15.
9. Bankoff, G. Rendering the World Unsafe: 'Vulnerability' as Western Discourse. *Disasters* **2001**, *25*, 19–35. [CrossRef] [PubMed]
10. Pelling, M. *Adaptation to Climate Change: From Resilience to Transformation*; Routledge: Oxon, UK, 2011.
11. De Sherbinin, A. Mapping the Unmeasurable? Spatial Analysis of Vulnerability to Climate Change and Climate Variability. Ph.D. Thesis, University of Twente, Enschede, The Netherlands, 2014.
12. US Government. *The President's Commission on Critical Infrastructure Protection (PCCIP), Executive Order 13010*; US Government: Washington, DC, USA, 1996.
13. NOTA—Rathenau-Instituut. *Stroomloos: Kwetsbaarheid van de Samenleving, Gevolgen van Verstoringen van de Elektriciteitsvoorziening (Blackout. Vulnerability of Society and Impacts of Electricity Supply Failure)*; Rathenau Instituut Den Haag: The Hague, The Netherlands, 1994; p. 264.
14. European Commission. *Cybersecurity of Smart Grids. Outcomes of the Expert Group on the Security and Resilience of Communications Networks and Information Systems for Smart Grids (2011–2012)*; European Commission: Brussels, Belgium, 2013.
15. Radanliev, P.; Montalvo, R.M.; Cannady, S.; Nicolescu, R.; De Roure, D.; Nurse, J.R.; Huth, M. Cyber Security Framework for the Internet-of-Things in Industry 4.0. *Preprints* **2019**, 2019030111. [CrossRef]
16. Fekete, A. Common Criteria for the Assessment of Critical Infrastructures. *Int. J. Disaster Risk Sci.* **2011**, *2*, 15–24. [CrossRef]
17. UN/ISDR. *Developing Early Warning Systems: A Checklist, Third International Conference on Early Warning (EWC III): From Concept to Action: 27–29 March 2006, Bonn, Germany*; UN/ISDR—Inter-Agency Secretariat of the International Strategy for Disaster Reduction: Geneva, Switzerland, 2006.
18. Mirbabaie, M.; Bunker, D.; Stieglitz, S.; Marx, J.; Ehnis, C. Social media in times of crisis: Learning from Hurricane Harvey for the coronavirus disease 2019 pandemic response. *J. Inf. Technol.* **2020**, *35*, 195–213. [CrossRef]
19. Roth, F.; Prior, T. Utility of virtual operation support teams: An international survey. *Aust. J. Emerg. Manag.* **2019**, *34*, 53–59.
20. Turner, B.L.; Kasperson, R.E.; Matson, P.A.; McCarthy, J.J.; Corell, R.W.; Christensen, L.; Eckley, N.; Kasperson, J.X.; Luers, A.; Martello, M.L.; et al. A framework for vulnerability analysis in sustainability science. *Proc. Natl. Acad. Sci. USA* **2003**, *100*, 8074–8079. [CrossRef]
21. Folke, C. Social-Ecological Resilience and Behavioral Responses. In *Individual and Structural Determinants of Environmental Practice*; Biel, A., Hansson, B., Mårtensson, M., Eds.; Ashgate Publishers: London, UK, 2003; pp. 226–287.
22. Walker, B.; Holling, C.S.; Carpenter, S.; Kinzig, A. Resilience, Adaptability and Transformability in Social-Ecological Systems. *Ecol. Soc.* **2004**, *9*, 5. [CrossRef]
23. Adger, W.N. Vulnerability. *Glob. Environ. Chang.* **2006**, *16*, 268–281. [CrossRef]

24. Cuny, F.C. Refugee camps and camp planning: The state of the art. *Disasters* **1977**, *1*, 125–143. [CrossRef] [PubMed]
25. Taylor, A.J. *Assessment of Victim Needs*; Intertect: Dallas, TX, USA, 1978.
26. Tobin, G.A. Sustainability and community resilience: The holy grail of hazards planning? *Glob. Environ. Chang. Part B Environ. Hazards* **1999**, *1*, 13–25. [CrossRef]
27. Onencan, A.M.; Liu, L.E.; Van de Walle, B. Design for Societal Resilience: The Risk Evaluation Diversity-Aiding Approach (RED-A). *Sustainability* **2020**, *12*, 5461. [CrossRef]
28. Birkmann, J. Measuring vulnerability to promote disaster-resilient societies: Conceptual frameworks and definitions. In *Measuring Vulnerability to Natural Hazards: Towards Disaster Resilient Societies*, 2nd ed.; Birkmann, J., Ed.; United Nations University Press: Tokyo, Japan, 2013; pp. 9–54.
29. Alves-Foss, J.; Barbosa, S. Assessing computer security vulnerability. *ACM SIGOPS Oper. Syst. Rev.* **1995**, *29*, 3–13. [CrossRef]
30. Koh, D. Occupational risks for COVID-19 infection. *Occup. Med. (Oxf. Engl.)* **2020**, *70*, 3. [CrossRef]
31. Pakpour, A.H.; Griffiths, M.D. The fear of COVID-19 and its role in preventive behaviors. *J. Concurr. Disord.* **2020**.
32. Peduzzi, P.; Dao, H.; Herold, C.; Mouton, F. Assessing global exposure and vulnerability towards natural hazards: The Disaster Risk Index. *Nat. Hazards Earth Syst. Sci.* **2009**, *9*, 1149–1159. [CrossRef]
33. Heltberg, R.; Siegel, P.B.; Jorgensen, S.L. Addressing human vulnerability to climate change: Toward a 'no-regrets' approach. *Glob. Environ. Chang.* **2009**, *19*, 89–99. [CrossRef]
34. Pelling, M.; Uitto, J.I. Small island developing states: Natural disaster vulnerability and global change. *Glob. Environ. Chang. Part B Environ. Hazards* **2001**, *3*, 49–62. [CrossRef]
35. Slovic, P. Perception of Risk. *Science* **1987**, *236*, 280–285. [CrossRef]
36. Werner, E. Vulnerable but invincible: High-risk children from birth to adulthood. *Acta Paediatr.* **1997**, *86*, 103–105. [CrossRef] [PubMed]
37. Werner, E.; Smith, R. *Journeys from Childhood to Midlife. Risk, Resilience, and Recovery*; Cornell University Press: Ithaca, NY, USA, 2001.
38. Moteff, J. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*; Congressional Research Service; The Library of Congress: Washington, DC, USA, 2005.
39. Robert, B. A method for the study of cascading effects within lifeline networks. *Int. J. Crit. Infrastruct.* **2004**, *1*, 86–99. [CrossRef]
40. Collier, S.J.; Lakoff, A. The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem. In *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation*; Kristensen, M.D.K.S., Ed.; Routledge: Abingdon, UK, 2008.
41. OECD. *Future Global Shocks Improving Risk Governance*; Organisation for Economic Co-Operation and Development: Paris, France, 2011; p. 137.
42. European Commission. COUNCIL DIRECTIVE 2008/114/ EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. *Off. J. Eur. Union* **2008**, *345*, 75–82.
43. Bouchon, S. *The Vulnerability of Interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art*; Institute for the Protection and Security of the Citizen, Joint Research Centre, European Commission: Ispra, Italy, 2006.
44. Yusta, J.M.; Correa, G.J.; Lacal-Arántegui, R. Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy* **2011**, *39*, 6100–6119. [CrossRef]
45. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Syst. Mag.* **2001**, *21*, 11–25.
46. Labaka, L.; Hernantes, J.; Sarriegi, J.M. A holistic framework for building critical infrastructure resilience. *Technol. Forecast. Soc. Chang.* **2016**, *103*, 21–33. [CrossRef]
47. Murdock, H.; de Bruijn, K.; Gersonius, B. Assessment of Critical Infrastructure Resilience to Flooding Using a Response Curve Approach. *Sustainability* **2018**, *10*, 3470. [CrossRef]
48. Croope, S.V.; McNeil, S. Improving resilience of critical infrastructure systems postdisaster: Recovery and mitigation. *Transp. Res. Rec.* **2011**, *2234*, 3–13. [CrossRef]
49. Giannopoulos, G.; Dorneanu, B.; Jonkeren, O. Risk Assessment Methodology for Critical Infrastructure Protection. In *JRC–Scientific and Policy Report*; JRC: Ispra, Italy, 2013.

50. Boin, A.; McConnell, A. Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. *J. contingencies Crisis Manag.* **2007**, *15*, 50–59. [CrossRef]
51. Golan, M.S.; Jernegan, L.H.; Linkov, I. Trends and applications of resilience analytics in supply chain modeling: Systematic literature review in the context of the COVID-19 pandemic. *Environ. Syst. Decis.* **2020**, *1*, 222–243. [CrossRef]
52. Remko, V.H. Research opportunities for a more resilient post-COVID-19 supply chain-closing the gap between research findings and industry practice. *Int. J. Oper. Prod. Manag.* **2020**, *40*, 341–355. [CrossRef]
53. Müller, S.M.; Mueller, G.F.; Navarini, A.A.; Brandt, O. National Publication Productivity during the COVID-19 Pandemic—A Preliminary Exploratory Analysis of the 30 Countries Most Affected. *Biology* **2020**, *9*, 271. [CrossRef] [PubMed]
54. Ivanov, D. New drivers for supply chain structural dynamics and resilience: Sustainability, industry 4.0, self-adaptation. In *Structural Dynamics and Resilience in Supply Chain Risk Management*; Springer: Cham, Switzerland, 2018; pp. 293–313.
55. Magid, E.; Pashkin, A.; Simakov, N.; Abbyasov, B.; Suthakorn, J.; Svinin, M.; Matsuno, F. Artificial intelligence based framework for robotic search and rescue operations conducted jointly by international teams. In *Proceedings of 14th International Conference on Electromechanics and Robotics "Zavalishin's Readings"*; Springer: Singapore, 2020; pp. 15–26.
56. Ogie, R.I.; Rho, J.C.; Clarke, R.J. Artificial intelligence in disaster risk communication: A systematic literature review. In *2018 5th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*; IEEE: Piscataway, NJ, USA, 2018; pp. 1–8.
57. Aşuroğlu, T.; Açıcı, K.; Erdaş, Ç.B.; Toprak, M.K.; Erdem, H.; Oğul, H. Parkinson's disease monitoring from gait analysis via foot-worn sensors. *Biocybern. Biomed. Eng.* **2018**, *38*, 760–772. [CrossRef]
58. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards the Internet of smart clothing: A review on IoT wearables and garments for creating intelligent connected e-textiles. *Electronics* **2018**, *7*, 405. [CrossRef]
59. Bostrom, N. Human Genetic Enhancements: A Transhumanist Perspective. *J. Value Inq.* **2003**, *37*, 493–506. [CrossRef]
60. Moore, M. The Philosophy of Transhumanism. In *The Transhumanist Reader: Classical and Contemporary Essays on the Science, Technology, and Philosophy of the Human Future*; Moore, M., Vita-More, N., Eds.; John Wiley & Sons, Inc.: Chichester, UK, 2013.
61. Huxley, J. Transhumanism. *J. Humanist. Psychol.* **1968**, *8*, 73–76. [CrossRef]
62. Kurzweil, R. *The Singularity is Near*; Penguin: New York, NY, USA, 2005; p. 652.
63. Benedikter, R.; Giordano, J.; Fitzgerald, K. The future of the self-image of the human being in the Age of Transhumanism, Neurotechnology and Global Transition. *Futures* **2010**, *42*, 1102–1109. [CrossRef]
64. McNamee, M.; Edwards, S. Transhumanism, medical technology and slippery slopes. *J. Med. Ethics* **2006**, *32*, 513–518. [CrossRef]
65. Ferrando, F. Posthumanism, transhumanism, antihumanism, metahumanism, and new materialisms. *Existenz* **2013**, *8*, 26–32.
66. Grunwald, A. *Technikfolgenabschätzung—Eine Einführung*, 2nd ed.; Edition Sigma: Berlin, Germany, 2010.
67. Petrie, K.J.; Wessely, S. Modern worries, new technology, and medicine. *BMJ* **2002**, *324*, 690–691. [CrossRef]
68. Dominici, P. For an inclusive innovation. Healing the fracture between the human and the technological in the hypercomplex society. *Eur. J. Futures Res.* **2018**, *6*, 3. [CrossRef]
69. Papadopoulos, T.; Gunasekaran, A.; Dubey, R.; Altay, N.; Childe, S.J.; Fosso-Wamba, S. The role of Big Data in explaining disaster resilience in supply chains for sustainability. *J. Clean. Prod.* **2017**, *142*, 1108–1118. [CrossRef]
70. Yu, M.; Yang, C.; Li, Y. Big data in natural disaster management: A review. *Geosciences* **2018**, *8*, 165. [CrossRef]
71. Shahid, A.R. The Impact of Crowdmapping on Humanitarian Response: A Structurational Analysis. Ph.D. Thesis, Royal Holloway, University of London, Egham, UK, 2016.
72. Gulnerman, A.G.; Karaman, H. Spatial Reliability Assessment of Social Media Mining Techniques with Regard to Disaster Domain-Based Filtering. *ISPRS Int. J. Geo-Inf.* **2020**, *9*, 245. [CrossRef]
73. Haworth, B.; Bruce, E. A review of volunteered geographic information for disaster management. *Geogr. Compass* **2015**, *9*, 237–250. [CrossRef]
74. Matsuno, F.; Tadokoro, S. Rescue robots and systems in Japan. In *2004 IEEE International Conference on Robotics and Biomimetics*; IEEE: Piscataway, NJ, USA, 2004; pp. 12–20.

75. Kerle, N.; Nex, F.; Gerke, M.; Duarte, D.; Vetrivel, A. UAV-Based Structural Damage Mapping: A Review. *ISPRS Int. J. Geo-Inf.* **2020**, *9*, 14. [CrossRef]
76. Aziz, N.A.A.; Aziz, K.A. Managing disaster with wireless sensor networks. In Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT2011), Gangwon-Do, Korea, 13–16 February 2011; pp. 202–207.
77. Twigg, J.; Mosel, I. Emergent groups and spontaneous volunteers in urban disaster response. *Environ. Urban.* **2017**, *29*, 443–458. [CrossRef]
78. Cutter, S.L.; Boruff, B.J.; Shirley, W.L. Social Vulnerability to Environmental Hazards. *Soc. Sci. Q.* **2003**, *84*, 242–261. [CrossRef]
79. Ziervogel, G.; Downing, T.E. Vulnerability Indicators and Mapping. Available online: https://www.sei.org/publications/vulnerability-indicators-mapping/ (accessed on 10 November 2020).
80. King, D. Uses and Limitations of Socioeconomic Indicators of Community Vulnerability to Natural Hazards: Data and Disasters in Northern Australia. *Nat. Hazards* **2001**, *24*, 147–156. [CrossRef]
81. Goss, K.C. *Guide for All-Hazard Emergency Operations Planning*; FEMA: Washington DC, USA, 1996.
82. Cannon, T. A hazard need not a disaster make: Vulnerability and the causes of 'natural' disasters. In *Natural Disasters: Protecting Vulnerable Communities: Proceedings of the Conference Held in London, UK, 13–15 October 1993*; Thomas Telford Publishing: London, UK, 1993; pp. 92–105.
83. Luhmann, N. *Risk: A Sociological Theory*; de Gruyter: Berlin, Germany, 1993.
84. Fischer, H.W.; Stine, G.F.; Stoker, B.L.; Trowbridge, M.L.; Drain, E.M. Evacuation behaviour: Why do some evacuate, while others do not? A case study of the Ephrata, Pennsylvania (USA) evacuation. *Disaster Prev. Manag. Int. J.* **1995**, *4*, 30–36. [CrossRef]
85. Heath, S.E.; Kass, P.H.; Beck, A.M.; Glickman, L.T. Human and pet-related risk factors for household evacuation failure during a natural disaster. *Am. J. Epidemiol.* **2001**, *153*, 659–665. [CrossRef] [PubMed]
86. Zhao, S. The digital self: Through the looking glass of telecopresent others. *Symb. Interact.* **2005**, *28*, 387–405. [CrossRef]
87. The Broadband Commission. *The State of Broadband: Broadband Catalyzing Sustainable Development*; ITU, UNESCO: Geneva, Switzerland, 2018; p. 90.
88. Donner, W.; Rodríguez, H. Population composition, migration and inequality: The influence of demographic changes on disaster risk and vulnerability. *Soc. Forces* **2008**, *87*, 1089–1114. [CrossRef]
89. Beasley, R.A. Medical robots: Current systems and research directions. *J. Robot.* **2012**, *2012*, 401613. [CrossRef]
90. Broadbent, E.; Stafford, R.; MacDonald, B. Acceptance of healthcare robots for the older population: Review and future directions. *Int. J. Soc. Robot.* **2009**, *1*, 319. [CrossRef]
91. Pisarchik, A.N.; Maksimenko, V.A.; Hramov, A.E. From novel technology to novel applications: Comment on "An integrated brain-machine interface platform with thousands of channels" by Elon Musk and Neuralink. *J. Med Internet Res.* **2019**, *21*, e16356. [CrossRef]
92. Gilbert, F.; Pham, C.; Viaña, J.; Gillam, W. Increasing brain-computer interface media depictions: Pressing ethical concerns. *Brain-Comput. Interfaces* **2019**, *6*, 49–70. [CrossRef]
93. Anupama, H.; Cauvery, N.; Lingaraju, G. Brain computer interface and its types-a study. *Int. J. Adv. Eng. Technol.* **2012**, *3*, 739.
94. Barfield, W.; Williams, A. Cyborgs and enhancement technology. *Philosophies* **2017**, *2*, 4. [CrossRef]
95. Ajiboye, A.B.; Willett, F.R.; Young, D.R.; Memberg, W.D.; Murphy, B.A.; Miller, J.P.; Walter, B.L.; Sweet, J.A.; Hoyen, H.A.; Keith, M.W. Restoration of reaching and grasping movements through brain-controlled muscle stimulation in a person with tetraplegia: A proof-of-concept demonstration. *Lancet* **2017**, *389*, 1821–1830. [CrossRef]
96. Byrom, B.; McCarthy, M.; Schueler, P.; Muehlhausen, W. Brain monitoring devices in neuroscience clinical research: The potential of remote monitoring using sensors, wearables, and mobile devices. *Clin. Pharmacol. Ther.* **2018**, *104*, 59–71. [CrossRef] [PubMed]
97. Picard, R.W.; Healey, J. Affective wearables. *Pers. Technol.* **1997**, *1*, 231–240. [CrossRef]
98. Neža, P.; Maja, T.; Dejan, G.; Dušan, F. Lightning may pose a danger to patients receiving deep brain stimulation: Case report. *J. Neurosurg. JNS* **2018**, 1–3. [CrossRef]
99. Cooper, C.; Sovacool, B.K. Not your father's Y2K: Preparing the north american power grid for the perfect solar storm. *Electr. J.* **2011**, *24*, 47–61.

100. Bruneau, M.; Chang, S.E.; Eguchi, R.T.; Lee, G.C.; O'Rourke, T.D.; Reinhorn, A.M.; Shinozuka, M.; Tierney, K.; Wallace, W.A.; von Winterfeld, D. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthq. Spectra* **2003**, *19*, 733–752. [CrossRef]
101. Robinson, L.; Schulz, J.; Khilnani, A.; Ono, H.; Cotten, S.R.; Mcclain, N.; Levine, L.; Chen, W.; Huang, G.; Casilli, A.A. Digital inequalities in time of pandemic: COVID-19 exposure risk profiles and new forms of vulnerability. *First Monday* **2020**, *25*. [CrossRef]
102. Gilbert, D.T.; Gill, M.J.; Wilson, T.D. The future is now: Temporal correction in affective forecasting. *Organ. Behav. Hum. Decis. Process.* **2002**, *88*, 430–444. [CrossRef]
103. Alexander, D. Resilience and disaster risk reduction. an etymological journey. *Nat. Hazards Earth Syst. Sci.* **2013**, *13*, 2707–2716. [CrossRef]
104. Waldrop, M.M. *Complexity: The Emerging Science at the Edge of Order and Chaos*; Edition of 1994; Penguin Books: London, UK, 1992.