Safe AND Secure Infrastructures? - Studying Human Aspects of Safety and Security Incidents with Experts from both Domains

Verena Zimmermann
ETH Zürich
Zürich, Switzerland
verena.zimmermann@gess.ethz.ch

Jasmin Haunschild
Technical University of Darmstadt
Darmstadt, Germany
haunschild@peasec.tu-darmstadt.de

Alina Stöver
Technical University of Darmstadt
Darmstadt, Germany
alina.stoever@tu-darmstadt.de

Nina Gerber
Technical University of Darmstadt
Darmstadt, Germany
nina.gerber@tu-darmstadt.de

ABSTRACT

In today's digitalized and interconnected world, the traditionally distinct concepts security and safety are increasingly intertwined. For example, a cyber attack on a hospital can negatively impact the patients' physical safety. Thus, security research and practice should consider these interactions. To explore human-related challenges at the intersection of safety and security, we conducted three focus group workshops with N= 16 experts from both domains. We introduced two scenarios leading to a power outage, one with a safety-related cause (snow storm) and one with a security-related cause (cyber attack). The experts discussed interactions, differences and parallels in coping with the scenarios. Additionally, potential solutions for building response capacity by including volunteers were explored. The findings indicate similar consequences resulting from the safety- vs. security-related incidents. However, the experts identified relevant differences in the challenges preparing for and coping with the scenarios. While security-related challenges included the incalculable time horizon, impact and cascading effects as well as lack of emergency plans and training, safety challenges mainly concerned accessibility of the affected area. The implications for future work are discussed.

KEYWORDS

security, safety, human factors, expert, focus group, workshop

1 INTRODUCTION

In today's world, previously non-digital devices, processes and infrastructures have become increasingly digitalized. Examples include smart home devices, digital citizen services, or smart grids. This trend provides a variety of benefits, e.g. with regards to efficiency, quality of life, or cost reduction [18]. One example for the increasing digitalization across devices, services and infrastructures is provided by the Smart City concept. It aims to increase a city's intelligence and efficiency by using technology [24, 28]. However, the increasing digitalization also comes with challenges. One such challenge is the increasing complexity of socio-technical systems due to their interconnectedness. This concerns not only the devices or the exchanged information itself but their safety and IT security, as well.

Safety and IT security have traditionally been considered different concepts with safety focusing on operation safety and the prevention of unintentional accidents and IT security focusing on the protection from intentional attacks [3, 15]. The topics have often been treated in different disciplines or organisational departments, e.g., the IT security department and the safety department. With the quickly evolving technological and digital advancements, however, the concepts have become increasingly interwoven, requiring an integrated analysis [15]. For example, an IT security attack targeting a hospital's health devices or patients' data may easily also endanger the patient safety as could be seen in cyber attacks on hospitals in France [22], the US [7] and other countries across the world. In addition, a large variety of cyber attacks before and after the invasion of Ukraine by Russia has demonstrated the increased potential of large-scale cyber attacks to disrupt safety-critical infrastructures, such as the energy supply [21].

In addition, the potential distinctions and parallels of safety and security as well as their implications are not well understood as can be seen in differing and ambiguous definitions of the terms [4]. Yet, anticipating shared safety- and security-related challenges is essential for being able to develop measures that support human actors in preventing them or coping with them. For this, the skill sets of both disciplines need to be combined to ensure understanding of both perspectives [2], e.g., not all safety experts are also experts for cyber attacks. Thus, communication and feedback are essential [2]. As such, the focus of this research is on the human-centered aspects of safety and security, such as communication, cooperation, and decision-making, and involves safety as well as security experts.

Our research aims are thus:

(1) to get a better understanding of safety- and security-related challenges that experts of both domains currently face or expect to arise in the future.
(2) to explore interactions, differences and parallels in dealing with safety- as compared to security-related incidents.
(3) to collect ideas for coping with the identified safety- and security-related challenges by including volunteers.

Veröffentlicht durch die Gesellschaft für Informatik e.V.
in P. Fröhlich & V. Cobus (Hrsg.):
Mensch und Computer 2023 – Workshopband, 03.-06. September 2023, Rapperswil (SG)

https://doi.org/10.18420/muc2023-mci-ws01-225

As an initial research step, we conducted three focus groups workshops with N=16 safety as well as security experts across Smart City infrastructures, industries, and research. The idea was to foster exchange among the experts with different perspectives and backgrounds. Within the workshops, we jointly discussed the handling and potential challenges of safety-and security-related scenarios. Furthermore, we collected ideas for building capacity to deal with these challenges. We then explored specifically the concept of including volunteers in the handling of major cybersecurity incidents, as this is already widely used and accepted for physical safety and security incidents. Our results show that the experts perceived safety-related outages as more predictable and had more awareness of required response procedures. In contrast, with regard to outages caused by IT security attacks, more insecurity exists related to the duration of the failure and the scope of the compromised systems. The employment of trained volunteers for large-scale cyber attacks was sometimes mentioned as a viable solution strategy, while at the same time, participants primarily held notions of ad-hoc volunteers and found it difficult to envision how a successful integration of volunteers might be possible.

2 RELATED WORK

Given their increased interconnectedness in digitalized socio- technical systems, the need to jointly consider the concepts safety and security, which have previously been treated as separate, has been recognized by researchers concerned with estimating risks and hazards in the engineering process. For example, Lisova et al. [15] reviewed numerous articles on systems engineering approaches that consider both safety and security. Roudier and Aprville [23], for instance, aim to analyse the potential impact of security technologies on safety-related functions in cyber-physical systems using an approach based on Systems Modeling Language, i.e., SysML-Sec. Young and Leveson suggest an integrated approach based on systems theory [29, 30] that considers both concepts in a model called STPA-Sec, that is a System-Theoretic Process Analysis extended by security analysis. Yet, Lisova et al. [15] found that the co-analysis is an emerging field that currently is often driven by need or technological advances and that requires further research.

In a book on the coupling of safety and security, Pettersen Gould and Bieder [19] highlight the historically increased emphasis on security, which was previously mainly connected to state security, but is now, alongside safety, also gaining relevance for organizations. Yet, they also identify challenges of bringing the two concepts together, such as ambiguity of the terms and definitions [4] or safety and security sometimes being in conflict with each other [20]. In this regard, Amorim et al. [1] list five reasons for why safety and security have not been successfully combined yet. These are differences in (1) the user perspective (safety assumes well-intended users while security mistrusts them), (2) quantifying risk (statistical hazard estimation in safety vs. difficult to anticipate attack occurrence), (3) protection effort (safety as nonnegotiable and security as a trade-off), (4) temporal aspects (safety being rather static and security highly dynamic), and (5) use of tested products (safety can benefit from tested off-the-shelf products while security can be endangered by publicly available design and related vulnerabilities). All these aspects contribute to organizations being in doubt on whether previously separated departments for managing safety and security should be merged [19]. Another aspect where stark differences in managing safety and security incidents can be observed is the involvement of volunteers. While this is common practice in safety incidents, where volunteers e.g., provide interim infrastructure, this is currently only starting to be considered for cybersecurity incidents, especially those affecting digital and cyber infrastructure. However, it is a strategy that is being used in the highly digitalized Estonia [6], and it is something that is currently tentatively supported by governments. For example, in Germany the coalition contract states that an established volunteer organization should expand its capabilities in cyber support [5, VI]. It is also a solution that has been put forward by a the German expert network for critical infrastructure, KRITIS [13], and a project to enhance cyber resilience in the canton Zurich [9]. While in cases of cyber incidents, professional cybersecurity teams or external experts are typically engaged to ensure an appropriate response and mitigate potential damage effectively, it is suggested that volunteers might be neccessary in cases of large-scale cyer attacks to ensure rapid response and scalability. However, is currently unclear what challenges infrastructure providers see and under which conditions they might envision working such a solution.

Thus, our research aims to shine light on these issues and unsolved questions with regard to critical infrastructure management. This domain, to the best of our knowledge, has not been analysed with regard to how safety and security are currently handled in practice, e.g., how organizations prepare for and deal with safety as compared to security incidents. In addition, we aim to explore which parallels, differences, and challenges exist from experts' view.

3 METHOD

To analyze (1) current security- and safety-related challenges from an expert's perspective, (2) differences, parallels and interactions when handling safety as compared to security incidents, and (3) ideas for including volunteers in dealing with cyber incidents, we conducted three expert focus group workshops. The next sections will detail the sample and the procedure.

3.1 Sample

The sample consisted of N=16 (IT) security as well as safety experts from various areas in critical infrastructures (N=5, e.g. smart grids, water distribution), authorities (N=6, e.g. national and regional security agencies, insurances), emergency services (N=2, e.g. emergency response personnel, police), and research (N=3, e.g. researchers at universities).

To recruit experts, we first identified numerous organisations, authorities, and universities within our country and across the categories of critical infrastructures (CI) as clustered by the Federal Office of Civil Protection and Disaster Assistance [17], that is: water, energy, food, finance and insurance, health, information technology and telecommunication, media and culture, state and administration, and transport and traffic. We either directly contacted security/safety experts with personalized invitation e-mails where available, or used general contact details for inquiries. When we had a critical mass of four experts available for a certain date, we sent them further information. The experts were compensated

with 20€ for their participation, however, some of them waived the offer. We aimed for diversity with regards to the targeted organisations and a balance with regards to safety and security experts but also other demographics such as gender. Yet, the final sample composition was highly influenced by the responses and availability of the contacted experts. In addition to this, the percentage of women compared to men working in cybersecurity in the country of this study is lower than 20%, making a higher number of male participants likely [12].

Therefore, of the 16 experts, N=15 identified as male and N=1 as female.

3.2 Study Procedure

Due to the Covid-19 pandemic, we conducted online focus group workshops via Zoom. To ensure local storage of the audio recording, we used Open Broadcaster Software (OBS, [8]). To structure the focus groups into different tasks and to allow for collaborative working, we prepared a Mural board [16] that participants could join by clicking on a link without having to create an account. The duration of the focus groups was 1.5 hours. While two researchers moderated the workshop, a third researcher was present as a backup in case of connection problems and to provide support with technical issues. Information on the study, the used software and an informed consent sheet were already shared with the participants before the workshop.

The focus groups were structured as follows:

(1) **Welcome & Introductions.** First, we explained the purpose and structure of the focus group and ensured that all participants could access the Mural board. The Mural board also contained the agenda items and important definitions, e.g., of the terms safety and security, as a reminder for the participants. Before starting the audio recording we again asked all participants for their consent. This was followed by a round of introductions using Mural tools (e.g., post-its) to familiarize the participants with using Mural.
(2) **Scenarios.** We then presented two related scenarios in which safety (power outage due to a snow storm) or security (power outage based on a cyber attack on the smart grid infrastructure) were focused on. The aim was to learn more about the different experts' perspectives with regards to the consequences resulting from the scenario, the actions undertaken to deal with it, and current challenges. The focus was on the human factor rather than technical processes, i.e. we aimed to find out how that scenario affected different groups of people (e.g., citizens, employees), which actions were undertaken with regards to other people (e.g., communication, cooperation) and which challenges were seen regarding human aspects. Figure 1 illustrates this research step as structured on the Mural board. The complete scenario descriptions and the accompanying questions and tasks can be found in the Appendix A.
   – **Focus on Safety.** The first scenario described a power outage due to a snow storm. It was inspired by major power outage in Germany following a snowstorm that resulted in snapping electricity pylons in 2005 [26].
   – **Focus on Security.** The second scenario described a power outage based on a cyber attack on the smart grid infrastructure inspired by cyber attacks on the Ukrainian infrastructure in 2015 and 2017 [25, 27].
(3) **Potential Solutions including Volunteers.** In a third step, potential solutions for addressing major safety- and security-related incidents regardless of their reason were discussed. As one option, the idea to include volunteers to support in emergency situations and to address the current lack of IT experts was introduced and discussed. From previous discussions, were aware that this idea bears challenges such as volunteers not being granted access to highly sensitive technical systems in critical infrastructures. To help the participants focus on conditions that might enable a successful employment of volunteers as compared to only focus on the challenges, the discussion was framed around a *miracle question*. Such a question is typically asked in solution-focused therapy to help clients envision a desirable situation [10]. We adapted the question to focus on what enabled the miracle: After introducing the scenario of a large-scale cyber attack that sought to encrypt data from infrastructures and agencies, we stated: "A cyber volunteer force contributed to avoiding the disruption of important services. The employment is evaluated as a big success from all sides. What enabled this successful employment?" Afterwards, alternatives were collected. The complete instruction can be found in the Appendix B.
(4) **Conclusion.** We concluded the expert workshops by collecting the most import "take-away" from each expert, providing the option to exchange contact details, and thanking all participants again.

The study design followed ethical guidelines proposed by our university's ethics committee. As such, all participants received an informed consent sheet and had the option to abort the study at any moment without negative consequences. Participant data was anonymized and handled in accordance with relevant data protection laws. The study did not include any deception or stress levels exceeding everyday occurrences.

4 FINDINGS

In this paper, we will focus on the analysis of the results of the discussion outcomes visualized on the Mural board and the challenges associated with exploring options for including volunteers in coping with threats. The results with regards to the safety and security scenarios will be structured according to the Mural board outlined in Figure 1. Afterwards, the discussed potential solutions for including volunteers in coping with security incidents will be summarized.

4.1 Level of Preparation

Figure 2 shows the perceived level of preparation of the experts' organizations for the safety- as compared to the security-focused scenario across all three workshops. Circles with the same number indicate the rating by the same expert. The colors indicate the focus group. The figure shows that generally more points are located on the upper half of the scale. While six experts felt their organizations

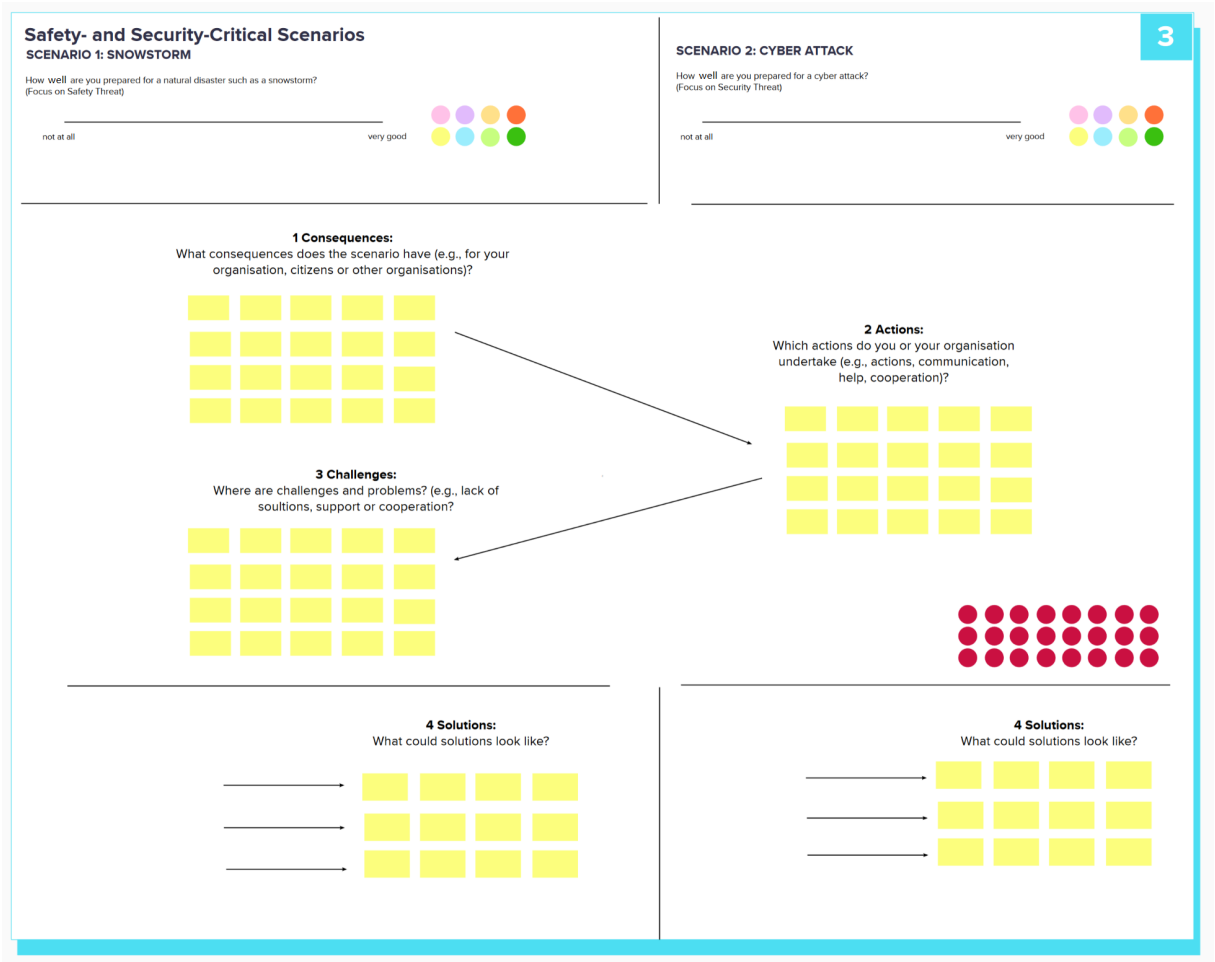

Figure 1: Layout and structure of the safety and security scenario task as presented on the Mural board.

were better prepared for safety threats (3, 5, 6, 11, 14, 15), six felt better prepared for security threats (1, 2, 7, 9, 10, 12). The remaining experts perceived the level of their organization's preparation as equal (4, 13) or did not provide a security rating (8, 16).

4.2 Consequences & Challenges

The consequences of a power outage, being either caused by a snow storm (safety) or a cyber attack (security), anticipated by the experts did not differ a lot. For example, in both cases, emergency power supply and additional resources (e.g. fuel, food, personnel) would be needed. In both cases, there might be a feeling of loss of control and fear among the public and an increased need for information provision. However, the experts pointed out differences in the challenges related to either safety or security threats. The main challenges associated with security threats were the lack of early warnings to prepare, the unclear time horizon of the attack, the impact not being locally limited, possible cascading effects, and the lack of response teams with emergency plans and training. In contrast, safety threats were associated with being locally confined, warning plans in place, and established response teams and training. However, an additional safety challenge was seen in a potentially reduced mobility (e.g. in case of snow blocking the roads).

Table 1 summarizes the challenges rated as most relevant by the participants using three votes per expert and the potential solutions collected to address them. Where the experts actively distinguished between safety and security-related solutions these are also distinguished in the table.

4.3 Volunteer Inclusion

One potential challenge in case of major security incidents is the limited number of available security experts that might not be sufficient to deal with the consequences across all affected organizations and entities. To explore opportunities to include volunteers in coping with major incidents to build capacity, we asked the following in the first focus group:

- Could you imagine the employment of volunteers specifically in your organization? Why/Why not?
- Which measures could help overcome the challenges and obstacles? What might be preconditions for the use of volunteers?

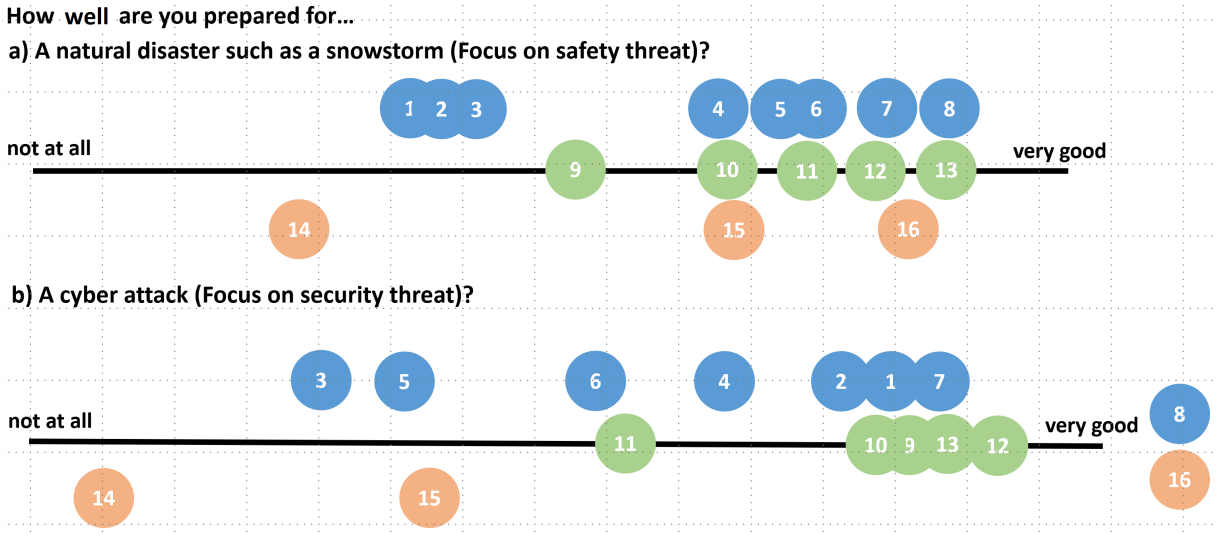

Figure 2: Level of preparation of the experts' organizations as rated by the experts. Note: blue - focus group 1, green - focus group 2, orange - focus group 3. Two experts (8, 16) did not provide a rating with regards to the security scenario.

Table 1: Summary of relevant challenges and potential solutions to them

Challenge	Safety Solutions	Security Solutions
Lack of awareness and expertise	Media campaigns, (sustainable) education, change of structures, political task to change use of technology, sensitization and building awareness	Redundancy (robust and physical), work with minimal supplies
Education	Anti-Decentralization or provincialization, structure cannot break down based on break-down of single organisations, make technology "visible", change relationship with technology, "understand" technology, solve "technology as a myth"	
Lack of resources/ decentralized infrastructures (e.g. emergency power supply)	Decentralisation, secure municipalities independently (e.g. own wind farms), prioritization of parts of the infrastructure, release funding	
Provision of Information	Emergency plan, define and establish ways for reporting	
Possible temporal break-down of IT infrastructure	Offline Backup, emergency documents, consider complete supply chain	Testing of backup systems, offline storage, switch to analog (as far as possible)
Increased number of emergency calls, time-delayed handling (personnel)	Building of a personnel/emergency reserve, pro-active information of public, media support through announcements	
Insurance of internal communication	Own communication channels or SAT connections, backup networks (non-public)	
Cascades (incalculable/ unlimited)	[no solutions collected]	

While participants stressed both the usefulness of a volunteer force, as well as the need to come up with conceptual solutions to enable a successful employment of such a force, they appeared to be struggling with focusing on conditions that might enable such a deployment. Perceived challenges centered around the potentially required but impossible access of volunteers to security-critical technical systems. Instead of focusing only on the challenges of

that approach, we were interested in exploring ways in which volunteers could contribute to the handling of incidents, perhaps outside of accessing sensitive systems, and the conditions enabling these efforts. Therefore, we reframed the discussion in focus group 2 and 3 by asking a *miracle question*, as described in the methods section.

One participant suggested that the challenges might be clustered according to whether people *can*, *want to*, and *are allowed to* work as volunteers. For the first aspect, participants suggested that ad-hoc volunteering might be feasible for support needed in private households and small enterprises, but not in larger companies, critical infrastructures and agencies. As a possible solution, training and on-site exercises were mentioned and regarded as necessary for volunteers to familiarise themselves with the used components and processes. Interestingly, little concern existed regarding whether people would want to volunteer, possibly because emergency management volunteering is very common in the country of study (blinded for review). In contrast, a large part of the discussion centered around whether volunteers would be allowed to support. Participants mentioned having contracts with external cyber experts, who were trusted and whose interventions were regulated by contracts. The participants did not envision how such contractual binding might be enabled with volunteers. Overall, participants had trouble envisioning how the conditions that enable expert support might be transferred to volunteers and to envision a lasting, trusted and knowledgeable support organization that would be admitted to a company's IT system, which was referred to as "the holy of holies".

5 DISCUSSION

The analysis of the visually collected workshop results show that there are indeed differences regarding the handling of safety- or security-focused threat scenarios. This becomes apparent in the large number of experts feeling better prepared either for security or safety threats. In addition, this shows in the different notions when describing security- or safety-related actions or consequences. Comparing our results with the challenges identified for combining safety and security [1], we find evidence for relevant challenges in anticipating cyber attacks and resulting from lower protection efforts with regard to cybersecurity as compared to safety. Security is viewed as highly dynamic and difficult to predict in terms of its temporal aspects compared to safety incidents with similar effects.

The collected challenges and proposed solutions can be clustered into five areas:

- *Awareness and Education:* Safety training and procedures (e.g. first aid training, fire alarm training) as well as emergency support (e.g. emergency response teams, police, technical emergency services) were found to be established in many cases. In contrast, this was described as an open challenge concerning the awareness and training for as well as handling of IT security-related incidents.
- *Decentralisation of Resources:* While a centralized approach was called for education and awareness, this was not the case for resources and infrastructures. Several experts mentioned that resources such as emergency power supply should be decentralized to be independent from a single supplier.
- *Emergency Communication:* One concern centered around ensuring (internal) communication in times of crisis given the strong reliance on digital communication channels. The experts, e.g., called for separate communication channels and backup networks.
- *Technology as a Blackbox:* Another challenge identified was the perception of and interaction with technology. IT-related incidents were associated with uncertainty regarding time and impact. From the experts' point of view, technology should be made visible, understandable and de-mystified to foster technology education.
- *Volunteer Inclusion:* More research is needed to identify IT security support that is needed in large-scale cyber incidents by different groups. The discussions suggest that private households, small businesses, large businesses, critical infrastructures and agencies should be differentiated with regards to tasks that could be given to trained volunteers. Volunteers are predominantly understood as ad-hoc volunteers, which impedes the imagining of trained volunteers and trusted relationships.

5.1 Limitations

Due to the Covid-19-related hygiene regulations that were in place at the time of the study, we had to conduct the focus group workshops online. While this increased the availability of experts across the country, in-person workshops might have contributed to an even more intense exchange among the experts. Furthermore, based on the lessons learned in the first focus group with regards to time constraints and the discussion on including volunteers in coping with threats, we shortened the round of introductions and adapted the volunteer-related question as described in the results section. To preserve the anonymity of the involved experts, the collection of socio-demographic data was reduced to a minimum. However, more knowledge on the experts' background such as for how many years they have been working in the safety/security area and their previous experience with the scenarios discussed in the focus group or similar incidents would have been beneficial to better assess their expertise and potential differences between different types of experts. Unfortunately, the number of experts from different industry sectors was to small to meaningfully compare differences between safety and security experts. Whereas the aim of the focus group was on fostering exchange about these topics among experts from different domains and leveraging their joint expertise to inform our future research, future work could explore qualitative and quantitative differences between safety and security experts or experts from different industries in handling safety- and security-relate incidents.

5.2 Future Work

The next step will be the detailed analysis of the audio transcripts to get an in-depth understanding of the visually collected challenges and ideas as well as aspects that were mentioned verbally but were not captured on the Mural board. Furthermore, we plan to enhance the expert perspectives with an extensive literature review on safety- and security-related challenges and interactions to adequately include findings from related work. Using both the

focus group workshops and the literature review as a basis, we intend to then develop and evaluate human-centered solutions that support human actors (e.g. infrastructure operators, security experts and also volunteers or citizens) in coping with identified safety- and security-related challenges. Furthermore, we aim to enable human actors to actively contribute to safety and security through enhancing, e.g., communication, cooperation, reporting or decision-making. Promising approaches for including human actors as safety/security factors are, for example, provided by an anti-phishing training that makes use of crowd intelligence [14] or the human-as-sensor framework [11], which among others describes how humans can enhance sensor data. In addition, future research should investigate the IT security needs of different CI providers in cases of large-scale cyber incidents, especially the role of external IT experts, as different CI providers appear to have different options with regards to external support. As there are many misconceptions regarding volunteering, more groundwork needs to be laid before discussing the concept. When exploring volunteers as part of a solution to lacking resources, researchers should clearly differentiate organized and trained volunteers from ad-hoc volunteering and provide more background information into how emergency volunteering is organized.

ACKNOWLEDGMENTS

This research work has been co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 251805230/GRK 2050, and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

REFERENCES

[1] Tiago Amorim, Daniel Schneider, Viet Yen Nguyen, Christoph Schmittner, and Erwin Schoitsch. 2015. Five major reasons why safety and security haven't married (yet). *ERCIM News* 102 (2015), 16–17.
[2] Fredrik Asplund, John McDermid, Robert Oates, and Jonathan Roberts. 2018. Rapid integration of CPS security and safety. *IEEE Embedded Systems Letters* 11, 4 (2018), 111–114.
[3] Peter J Blokland and Genserik L Reniers. 2020. The Concepts of Risk, Safety, and Security: A Fundamental Exploration and Understanding of Similarities and Differences. In *The Coupling of Safety and Security*. Springer, Cham, Switzerland, 9–16.
[4] Max Boholm, Niklas Möller, and Sven Ove Hansson. 2016. The concepts of risk, safety, and security: applications in everyday language. *Risk analysis* 36, 2 (2016), 320–338.
[5] Bundesregierung. 2021. Mehr Fortschritt Wagen. Bündnis Für Freiheit, Gerechtigkeit Und Nachhaltigkeit. Koalitionsvertrag Zwischen SPD, Bündnis 90/Die Grünen Und FDP. https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (zuletzt aufgerufen am 18.03. 2022).
[6] Sharon L. Cardash, Frank J. Cilluffo, and Rain Ottis. 2013. Estonia's Cyber Defence League: A Model for the United States? *Studies in Conflict and Terrorism* 36, 9 (2013), 777–787. https://doi.org/10.1080/1057610X.2013.813273
[7] Kevin Collier. 2022. Ransomware attack delays patient care at hospitals across the U.S. Retrieved 24th April 2023 from: https://www.nbcnews.com/tech/security/ransomware-attack-delays-patient-care-hospitals-us-rcna50919.
[8] OBS Studio Contributors. 2021/2022. OBS Open Broadcaster Software - OBS Studio. Retrieved 24th April 2023 from: https://obsproject.com/de.
[9] CYREN ZH. 2023. CYREN ZH: Cyber Resilience Network For The Canton Of Zurich. https://www.dsi.uzh.ch/de/research/projects/third-party/cyren-zh.html
[10] Peter De Jong and Insoo Kim Berg. 2014. *Lösungen (er) finden: das Werkstattbuch der lösungsorientierten Kurztherapie*. verlag modernes lernen.
[11] Ryan Heartfield, George Loukas, Anatolij Bezemskij, and Emmanouil Panaousis. 2020. Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning. *IEEE Transactions on Information Forensics and Security* 16 (2020), 1720–1735.
[12] (ISC)2. 2022. (ISC)2 CYBERSECURITY WORKFORCE STUDY. Retrieved 24th April 2023 from: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.
[13] AG KRITIS. 2022. Das Cyber-Hilfswerk Konzept Zur Steigerung Der Bewältigungskapazitäten Cyber-Großschadenslage. https://ag.kritis.info/wp-content/uploads/2022/11/chw-konzept_v1.1_final.pdf
[14] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. 2022. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, NY, USA, 842–859.
[15] Elena Lisova, Irfan Šljivo, and Aida Čaušević. 2018. Safety and security co-analyses: A systematic literature review. *IEEE Systems Journal* 13, 3 (2018), 2189–2200.
[16] MURAL. 2022. MURAL. Retrieved 24th April 2023 from: https://mural.co/.
[17] German Federal Office of Civil Protection and Disaster Assistance. 2022. Sektoren und Branchen KRITIS. Retrieved 24th April 2023 from: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html.
[18] Päivi Parviainen, Maarit Tihinen, Jukka Kääriäinen, and Susanna Teppola. 2017. Tackling the digitalization challenge: how to benefit from digitalization in practice. *International journal of information systems and project management* 5, 1 (2017), 63–77.
[19] Kenneth Pettersen and Corinne Bieder. 2020. Safety and security: the challenges of bringing them together. In *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*. Springer International Publishing, Cham, Switzerland, 1–8.
[20] Kenneth A Pettersen and Torkel Bjørnskau. 2015. Organizational contradictions between safety and security–Perceived challenges and ways of integrating critical infrastructure protection in civil aviation. *Safety science* 71 (2015), 167–177.
[21] Jakub Przetacznik and Simona Tarpova. 2022. *Russia's war on Ukraine: Timeline of cyber-attacks*. Technical Report March. European Parlament. 7 pages. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS{_}BRI(2022)733549{_}EN.pdf
[22] RFI. 2022. Paralysed French hospital fights cyber attack as hackers lower ransom. Retrieved 24th April 2023 from: https://www.rfi.fr/en/france/20220902-paralysed-french-hospital-fights-cyber-attack-as-hackers-lower-ransom-demand.
[23] Yves Roudier and Ludovic Apvrille. 2015. SysML-Sec: A model driven approach for designing safe and secure systems. In *2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*. IEEE, New York, NY, ACM, 655–664.
[24] Kehua Su, Jie Li, and Hongbo Fu. 2011. Smart city and the applications. In *2011 international conference on electronics, communications and control (ICECC)*. IEEE, New York, NY, USA, 1028–1031.
[25] Wikipedia. 2022. 2017 Ukraine ransomware attacks. Retrieved 24th April 2023 from: https://en.wikipedia.org/wiki/2017_Ukraine_ransomware_attacks.
[26] Wikipedia. 2022. Münsterländer Schneechaos. Retrieved 24th April 2023 from: https://de.wikipedia.org/wiki/M%C3%BCnsterl%C3%A4nder_Schneechaos.
[27] Wikipedia. 2022. Ukraine power grid hack. Retrieved 24th April 2023 from: https://en.wikipedia.org/wiki/Ukraine_power_grid_hack.
[28] ChuanTao Yin, Zhang Xiong, Hui Chen, JingYuan Wang, Daven Cooper, and Bertrand David. 2015. A literature survey on smart cities. *Science China Information Sciences* 58, 10 (2015), 1–18.
[29] William Young and Nancy Leveson. 2013. Systems thinking for safety and security. In *Proceedings of the 29th Annual Computer Security Applications Conference*. ACM, New York, NY, USA, 1–8.
[30] William Young and Nancy G Leveson. 2014. An integrated approach to safety and security based on systems theory. *Commun. ACM* 57, 2 (2014), 31–35.

A SCENARIO DESCRIPTIONS AND DISCUSSION QUESTIONS

A.1 Focus on Safety

Please imagine being in the following situation. A strong snow storm makes many electricity pylons break due to the heavy weight of the snow on them. The electricity lines are cut. Complete cities are without electricity. In addition, access to these cities is difficult because of blocked roads. The temperature in houses is quickly declining because of the cold outside. One concrete example for such a situation was a five day power outage in Münsterland in Germany in 2005.

A.2 Focus on Security

Please imagine being in the following situation. Hackers have attacked the computer and information systems of the power grid. The systems' purpose is to monitor and control the technical processes within the grid. The hackers disconnect several transformer stations via teleconnection technologies. Later, the hackers also attack the distribution centers so that the number of disconnected transformer station nearly doubles. The inhabitants of several cities are without electricity. Also, data files for restoring the systems have been deleted. The attack further concerns the call-center of one provider using a denial-of-service attack to hamper support services. Concrete examples for this scenario have been cyber attacks on the Ukrainian power grid in 2015 and 2016.

A.3 Task

The tasks and questions were similar for both scenarios. The participants started with discussing and reflecting on the first scenario. The focus of the second scenario mainly was on elaborating on parallels and differences between the two scenarios, i.e. what would be different if the power outage was caused by an attack rather than a natural disaster).

- 5 Minutes: Rating of the degree of preparation for that scenario on a rating scale included in the Mural board. Collection of reasons for the rating.
- 10 Minutes: Individual collection of answers to three questions on the Mural board using prepared post-its. The questions concerned the consequences, actions and challenges associated with the described scenario for the humans involved, i.e. the focus was on the human aspects of the safety- and security-related scenario.
- 10 Minutes: Summary and Discussion of collected answers.
- 5 Minutes: Rating of the challenges seen as most relevant. Each expert had three votes symbolized by red dots in mural. The three challenges with the highest umber of votes were selected for the next task.
- 10 Minutes: Discussion of measures and solutions to address the selected challenges,
- (Repetition of the procedure for the second scenario with a focus on parallels and differences)

B INTRODUCTION CYBER AID ORGANISATION

B.1 Introduction and Definition

In the following, let's consider the general outage of IT systems, that is all information- and communication-related systems, regardless of the reason for the outage. Many systems, e.g. for automating processes but also for communicating with with clients and providers, depend on digitalization. These systems are often interconnected and require Internet access to communicate with other systems and to get data.

As many organizations use similar components and providers, there is a concern, that an outage of IT systems would concern many companies and authorities at the same time. An example would be a ransomware attack in which data is encrypted and only released when paying a ransom. The current war in Ukraine also steered a discussion about attacks caused by state actors. Such a scenario, in which IT systems of many infrastructures are concerned at the same time, can be classified a major cyber catastrophic event.

While many organizations have their own IT experts and additional service providers that support in emergency cases, these could probably not cover the demand if many systems are concerned at the same time. There are some state organizations that could support in case of IT-related emergencies, such as mobile incident response teams. However, they have very limited capacity for local operations. Then, there are cyber emergency response teams. Yet, their focus is more on exchanging information. Finally, there are digital first aid teams that can be called for an initial remote analysis. Another useful organization could be the technical emergency services. So far, their aim is civil defense for physical infrastructures. Yet, this could be extended to also cover cyber-related support.

In addition, an organization consisting of volunteers to support in case of major cyber catastrophic events is discussed. It could be seen as an addition to state organizations with the aim to quickly restore and secure the public's supply with critical resources and and services. The voluntary cyber organization could for example help with providing new passwords on a large scale, the manual control of systems or installing updates. The organization would target people with IT expertise but also people who know the IT systems and can take over less specialized tasks. The main tasks of the volunteer organization would thus include the pooling and education of civil volunteers as well as the protection of the public from IT emergency-related consequences.

B.2 Task

Please consider the following scenario: There has been a major cyber catastrophic event. Data of many infrastructures and authorities has been encrypted on a large scale. A volunteer organization has contributed to the positive outcome that no major services were disrupted. The operation is viewed as a success.

Question: What has contributed to the success? How was this success possible?

- 10 Minutes: Group Discussion, Collection of ideas and comments on prepared Mural board
- 5 Minutes: Summary of the main challenges and measures or solutions
- 3 Minutes: Collection of alternatives for a volunteer organization