Editorial

Marc-André Kaufhold*, Tilo Mentler, Simon Nestler and Christian Reuter

The tension of usable safety, security and privacy

https://doi.org/10.1515/icom-2025-0009

Abstract: Local disasters such as the Ahr Valley flood in Germany, the international backdrop of the Russo-Ukrainian War, or the global impact of the COVID-19 pandemic place high demands on the people and organisations that are involved in these situations and contexts to save lives, mitigate damage, provide comfort, or organise reconstruction. Novel technologies are constantly making their way into everyday life, such as artificial intelligence, big data, decentralised networks, internet of things, or virtual reality. Their adaptation, acceptance, usability, usefulness, and legal framework conditions for safety-critical systems must be researched and tested thoroughly. In this special issue, we investigate the use of computer-based solutions in areas and situations of direct relevance to people's lives and well-being (Usable Safety), as well as contributions to user-oriented resilience concepts of sociotechnical systems concerning potential attacks (Usable Security) and data protection mechanisms (Usable Privacy).

Keywords: usable safety; usable security; safety-critical systems; human-centered computing

1 Introduction

Local disasters such as the Ahr Valley flood in Germany,[1] the international consequences of the Russian invasion of Ukraine,[2] the global COVID-19 pandemic,[3] the long-term effects of biodiversity loss and climate change,[4] as well as numerous conflicts and crises such as the Gaza war[5] place high demands on the people and organisations that are involved in these situations and contexts to save lives, mitigate damage, provide comfort, or organise reconstruction.

Although computer-based solutions have become indispensable, new technologies are constantly making their way into everyday life, such as big data and artificial intelligence,[6,7] the Internet of Things (IoT) and the development of disruption-tolerant networks,[8,9] or the development of so-called digital twins in virtual reality,[10,11] whose adaptation, acceptance, usability, usefulness, and legal framework conditions for safety-critical systems must be researched and tested thoroughly.[12]

These technologies also pose new challenges and problems for people and organisations in safety-critical situations, which must be considered in both research and practice. While social media, for example, can help to mobilise volunteers and improve situational awareness,[7,13] inconsistent and incorrect information, the flood of information in large-scale emergencies, uncoordinated activities and a lack of financial and human resources can increase the complexity of tasks for organisations.[14,15]

Past research has showcased how different actors, such as citizens,[16,17] computer emergency response teams,[18,19] control room operators,[20] emergency services,[21,22] medical staff,[23,24] or law enforcement agencies,[25,26] amongst others, have been expressing changing and diverse needs for technology adoption and design. To address these challenges, the research domain of human-computer interaction (HCI) has brought up a plentitude of user-centred design and evaluation methods.[27,28]

In this editorial, we provide a concise background on the relationship between usable safety and security (Section 2) and present the scope of this special issue, reflecting our call for contributions (Section 3). We then present five accepted articles on usable safety (Section 4) and a further five accepted articles on usable safety, which also include contributions to privacy (Section 5). We end with a brief conclusion and outline potential for future directions (Section 6).

***Corresponding author: Marc-André Kaufhold**, Knowledge Engineering (KE), Technical University of Darmstadt, Darmstadt, Germany, E-mail: kaufhold@peasec.tu-darmstadt.de.
https://orcid.org/0000-0002-0387-9597
Tilo Mentler, Human Computer Interaction und User Experience, Trier University of Applied Sciences, Trier, Germany,
E-mail: T.Mentler@inf.hochschule-trier.de.
https://orcid.org/0000-0002-8138-6536
Simon Nestler, Faculty of Computer Science, Technische Hochschule Ingolstadt, Ingolstadt, Germany,
E-mail: Simon.Nestler@thi.de. https://orcid.org/0000-0002-6392-8127
Christian Reuter, Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt, Darmstadt, Germany,
E-mail: reuter@peasec.tu-darmstadt.de.
https://orcid.org/0000-0003-1920-038X

2 Background

What's the relationship between usability and security in interactive systems? The introduction[29] of the textbook "Safety Critical Human-Computer-Interaction"[30] elaborates on their relationship. Accordingly, the key question is whether these two aspects are inherently opposed – meaning that improving security comes at the expense of usability, and vice versa – or whether they can actually reinforce each other, with increased usability leading to greater security.

There are different perspectives on this issue:[29] Some argue that overly simple systems cannot be secure, while others suggest that security should be established first, with usability optimized as much as possible within those constraints. A third viewpoint claims that intuitive and well-designed usability can actually enhance security.[29] Supports this latter perspective and explores ways to achieve both usability and security simultaneously.

Moreover, safety and security cannot be ensured through technical measures alone. While valid theoretical assumptions, appropriate mechanisms, and their correct technical implementation form a necessary foundation, the crucial question remains: Is this sufficient, or do additional challenges arise from human-system interaction?

True safety and security emerge when mechanisms are easy to understand, seamlessly integrated into system use, and do not create unnecessary obstacles. Only when humans and machines "understand" each other can a system be both secure and user-friendly. This principle applies not only to security, which protects against attacks and misuse but also to safety, which refers to protection from accidents and malfunctions. In both areas, optimized human-computer interaction helps ensure that protective systems provide greater security through improved usability.[29]

Usable security[31] focus addresses the usability of security concepts themselves and develops approaches to enhance users' security awareness. In research, it is often combined with the field of usable privacy.[32] In contrast, *usable safety* explores human-computer interaction in safety-critical contexts, such as control rooms, healthcare, disaster management, and the automotive sector – considering both potential threat scenarios and functional safety aspects.

The special interest group *Usable Safety and Security* was originally founded in 2015 under the name *Human-Machine Interaction in Safety-Critical Systems* within the Human-Computer Interaction division of the German Informatics Society (GI). The group is dedicated to a holistic examination of the intersection between human-computer interaction and security.[33] In 2025, so a decade after it's foundation, this special issue presents some current advancements in the field.

3 Call for contributions

In this special issue, we invited contributions that investigate the use of computer-based solutions in areas and situations of direct relevance to people's lives and well-being (Usable Safety), as well as contributions to user-oriented concepts of the resilience of sociotechnical systems concerning potential attacks (Usable Security). Possible topics included but were not limited to:

- Usability and user experience in safety-critical contexts (e.g. cybersecurity, healthcare, crisis management, process management, traffic management)
- Case studies and evaluations on usable safety or usable security in different target groups (e.g. authorities, citizens, enterprises, or emergency organisations)
- Algorithms and systems for user-centred and comprehensible big data analytics (e.g. artificial intelligence, visual analytics) in the context of safety-critical human-computer interaction
- Resilience and training in crises, disasters, and conflicts (including resilience, population warning, first aid, extended reality, recommendations for action, and emergency prevention)
- Participation and social media (including neighbourhood and self-help, crowdsourcing, digital volunteers, virtual operations support teams, and crisis mapping)
- Ethical, legal, and social implications in safety-critical systems (e.g. inclusive and ability-based design, value-sensitive design)
- Methods and tools for modelling and validating usable safety and security in sociotechnical systems (e.g. cyber-physical systems, human-robot collaboration, or digital twins)
- Sustainable human-machine-environment interaction in safety-critical contexts (e.g. limiting biodiversity loss, adapting to, and mitigating global warming).

We welcomed a broad range of contribution types, such as systematisation of knowledge (survey) research, conceptual and methodological research, qualitative and quantitative empirical research, and design and evaluation research. We received numerous submissions. After two rounds of rigorous review, the following 10 articles were accepted for publication.

4 Usable safety

A first selection of papers deals with crisis informatics and management, including the topics of control room collaboration, crisis management exercises, citizen warning, infection prevention, and hate speech detection.

First, the evolving role of human operators in control rooms for safety-critical systems such as power grids, emergency response, and transportation networks is a timeless topic. As automation and autonomous decision-making continue to advance, the paper *Keeping the Human in the Loop: Are Autonomous Decisions Inevitable?* of Jonas Pöhler, Nadine Flegel, Tilo Mentler, and Kristof Van Laerhoven (University of Siegen and Trier University of Applied Sciences) examines how to balance efficiency gains with the need to retain human intuition and ethical oversight, especially in high-stakes situations. By analyzing current trends, operator perspectives, and human-computer collaboration models, the authors identify key challenges, including the risks of deskilling, automation bias, and accountability gaps. The study advocates for a hybrid approach of collaborative autonomy, in which human operators and automated systems work in partnership to ensure transparency, trust, and adaptability in decision-making.

Second, crisis management exercises provide a unique opportunity to study situational awareness in real-time scenarios. However, the federated structure of large-scale crisis management, involving multiple decentralized teams, imposes additional challenges for researchers aiming to capture comprehensive situational awareness data. Moreover, since the primary goal of these exercises is operational readiness rather than academic research, any experimental setup must be non-intrusive and place minimal extra-demand on participants. In the paper *iSAM – Towards a Cost-Efficient and Unobtrusive Experimental Setup for Situational Awareness Measurement in Administrative Crisis Management Exercises* Tobias Hellmund, Henrik Kayser, and Jürgen Moßgraber (Fraunhofer IOSB) present a methodology supported by software that allows situational awareness assessments. Given that crisis managers operate spatially distributed during a large-scale disaster or exercise and that they lack the resources to be physically present at all locations, the introduced software aims to conduct the experiment without a researcher in every situation room. This approach facilitates comprehensive data collection and analysis without setting up a complex research environment in every situation room, thereby allowing us to meet both scientific and operational objectives effectively.

Third, in crisis situations, citizens' situational awareness is paramount for effective response. While warning apps offer location-based alerts, their usage is relatively low. In the paper *Breaking Down Barriers to Warning Technology Adoption: Usability and Usefulness of a Messenger App Warning Bot*, the authors Jasmin Haunschild, Markus Henkel, and Christian Reuter (TU Darmstadt) propose a personalised messaging app channel as an alternative, presenting a warning bot that may lower adoption barriers. They employ the design science research process to define user requirements and iteratively evaluate and improve the bot's usability and usefulness. The results showcase high usability, with over 40 % expressing an interest in utilising such a warning channel, stressing the added value of proactive warnings for personalised locations while not requiring a separate app. The derived requirements and design solutions, such as graphically enhanced user interface elements as guardrails for effective and error-free communication, demonstrate that a suitable warning chatbot does not necessarily require complex language processing capabilities. Additionally, the findings facilitate further research on accessibility via conversational design in the realm of crisis warnings.

Fourth, learning from the COVID-19 pandemic is an important precursor for preparedness and response capabilities in future pandemics. The paper *Use of Context-Based Adaptation to Avoid Threatening Situations in Times of a Pandemic* of Andrej Sibirski and Dirk Veiel (University of Hagen) explores the limitations of traditional contact tracing in containing infectious disease outbreaks, particularly during the COVID-19 pandemic. The authors propose a novel digital infection prevention system that goes beyond mere contact tracing by dynamically assessing and mitigating infection risks in real-time. Their approach utilizes context-aware adaptation, incorporating individual situational data and proximity to potential infection sources to deliver proactive recommendations. Unlike conventional methods, this system not only relies on Bluetooth-based distance estimation but also integrates an ontology-based context model to consider both direct and indirect transmission paths. The use of pathogen-specific prevention profiles ensures adaptable threat detection and targeted protective measures. A prototype Android application validates the feasibility of the approach, demonstrating its potential for managing infectious disease threats. The paper highlights key areas for future research, including improved sensor integration, privacy-preserving data sharing, and real-world empirical testing.

Fifth, German law enforcement agencies (LEAs) and dedicated reporting centers (RCs) engage in various

activities to counter illegal online hate speech (HS). Due to the high volume of such content and against the background of limited resources, their personnel can be confronted with the issue of information overload. To mitigate this issue, information filtering, classification, prioritization, and visualization technologies offer great potential. However, a nuanced understanding of situational awareness is required to inform the domain-sensitive implementation of supportive technology and adequate decision-making. Based on a qualitative research design employing a thematic analysis of qualitative expert interviews with practitioners from German LEAs and RCs ($N = 29$), the paper *Cyber Hate Awareness: Information Types and Technologies Relevant to the Law Enforcement and Reporting Center Domain* of Julian Bäumler, Georg Voronin, and Marc-André Kaufhold (TU Darmstadt and University of Potsdam) contributes to the state of research in human-computer interaction with a systematization of 23 information types of relevance for situational awareness of online HS in the law enforcement and RC domain. On that basis, they identify victim, perpetrator, context, evidence, legal, and threat awareness as domain-specific situational awareness sub-types and formulate ten implications for designing reporting, open-source intelligence, classification, and visual analytics tools.

5 Usable security and privacy

A second selection of papers focuses on usable security and privacy, including the topics of information security policies, digital identity wallets, insurance risk assessments, privacy assistants, and smart home privacy.

Sixth, effective Information Security Policies (ISP) are crucial for organisations to mitigate information security threats and risks. However, poorly designed information security policies can lead to hidden costs and decreased compliance in daily work routines. The paper *From Usable Design Characteristics to Usable Information Security Policies: A Reconceptualisation* of Dennis Lawo and Gunnar Stevens (University of Siegen) deals with ISPs that need to be realized in a usable way in order to ensure compliance and cost effectiveness. A conceptual research approach is followed to assess the role of usability in ISPs. Following this approach, the authors provide arguments for considering usability as essential aspect of ISPs. They introduce the concept of Usable Information Security Policies (UISPs). It based on HCI and IT security research findings and combines security and safety measures. The authors argue that UISPs must be aligned with governmental, organisational and civil society policies. Furthermore, guidance on incorporating usability in policy-making processes is provided.

Seventh, digital identity wallets enable the storage and management of digital identities and verifiable credentials in one place on end users' devices. This includes discount vouchers or customer cards, and security-critical data such as ID cards or driving licences. However, digital identity wallets face significant challenges due to weaknesses in user experience and information security. Users often find it difficult to understand the concept of digital identity wallets, resulting in personal information being inadvertently shared with untrusted parties. Additionally, user experience and information security can influence each other, so that both aspects must be evaluated and improved together. The paper *A Case Study of the MEUSec Method to Enhance User Experience and Information Security of Digital Identity Wallets* of Max Sauer, Christoph Becker, Lukas Kneis, Andreas Oberweis, Simon Pfeifer, Akim Stark, and Jan Sürmeli (FZI Research Center for Information Technology) reports on an experimental application of the Method for Enhancing User Experience and Information Security (MEUSec) method to the wallet "Hidy" with two research goals: First, to evaluate the MEUSec method and the quality of its results against a set of criteria, and second, to collect suggestions for improving the user experience and information security of the Hidy wallet. In total, 41 weaknesses and 7 strengths of user experience and information security, 32 heuristics and 26 improvement suggestions for the Hidy wallet could be identified.

Eighth, automated decision-making algorithms are increasingly prevalent in consumer-facing industries, particularly in insurance risk assessments. The traceability of these decisions is crucial for trust, acceptance, and individual autonomy. While the General Data Protection Regulation (GDPR) grants individuals the right to information about such decisions, the implementation of this right remains under-researched from a usable privacy perspective. The paper *Evaluating GDPR Right to Information Implementation in Automated Insurance Decisions* of Timo Jakobi, Patrix Harms, and Salih Arslan (Nuremberg Institute of Technology Georg Simon Ohm) employs a qualitative exploratory approach with twelve participants exercising their right to be informed about automated decision-making with German household insurers. Through interviews and observations, the study investigates consumer requirements and prevailing implementation practices. The findings unveil actual process design practices that may undermine the usability and efficacy of this data subject right. By identifying these concerns and correlating them to existing deceptive patterns, the research contributes to usable privacy

by alerting process designers, data protection authorities, and enterprises to the significance of user-centric implementations. Furthermore, this study advances research on GDPR data subject rights, emphasizing the need for secure and usable interfaces in the context of automated decision-making systems. This work highlights the practical challenges of safeguarding usable implementation of regulatory compliance in the realm of data protection.

Ninth, for many users, protecting their digital privacy remains a challenging task, which is why personal privacy assistants have been emerging as a promising approach to help users manage their privacy. The paper *Human-Centered Design of a Privacy Assistant and its Impact on Perceived Transparency and Intervenability* by Lennart Kiss and Rachelle Sellung (University of Stuttgart) presents a user study on preferences and perceptions of data protection, particularly regarding transparency and intervenability, in a privacy assistant application. The tool is designed to help users maintain a high level of data protection with minimal effort. The study, involving 20 participants, employed a mixed-methods approach, including qualitative analysis, to assess user perceptions and usability. The findings highlight two key aspects: (1) understanding user requirements and attitudes toward data protection and privacy, and (2) evaluating whether the privacy assistant meets these requirements in terms of transparency, intervenability, user experience, and usability. The results indicate varying privacy attitudes and differing levels of GDPR knowledge among participants. The high-fidelity prototype demonstrated excellent usability and received positive evaluations across multiple user experience dimensions. These insights provide valuable guidance for improving the design and implementation of privacy assistant applications.

Tenth, large language models (LLMs) have demonstrated potential in automating data-driven tasks, enabling non-experts to analyze raw inputs such as tables or sensor data using conversational queries. Advances in machine learning and HCI have further reduced entry barriers, pairing sophisticated model capabilities and a wealth of background knowledge with user-friendly interfaces like chatbots. While empowering users, this raises critical privacy concerns when used to analyze data from personal spaces, such as smart-home environments. The paper *ChatAnalysis Revisited: Can ChatGPT Undermine Privacy in Smart Homes with Data Analysis?* of Victor Jüttner, Arthur Fleig, and Erik Buchmann (Center for Scalable Data Analytics and Artificial Intelligence) investigates the capabilities of LLMs, specifically GPT-4 and GPT-4o, in analyzing smart-home sensor data to infer human activities, unusual activities, and daily routines. The authors use datasets from the CASAS project, which include data from connected devices such as motion sensors, door sensors, lamps, and thermometers. Extending prior work, they evaluate whether advances in model design, prompt engineering, and pre-trained knowledge enhance performance in these tasks and thus increase privacy risks. The findings reveal that GPT-4 infers daily activities and unusual activities with some accuracy but struggles with daily routines. With this experimental setup, GPT-4o underperforms its predecessor, even when supported by structured CO-STAR prompts and labeled data. Both models exhibit extensive background knowledge about typical daily routines, underscoring the potential for privacy violations in smart-home contexts.

6 Conclusions

This special issue highlights current research at the intersection of usable safety, security and privacy. The selected papers emphasize the importance of situational awareness, adaptive crisis communication, and the role of human-centered design in safety-critical decision-making. Additionally, they explore challenges in cybersecurity, digital identity management, and the impact of AI on data privacy. By addressing these topics, the contributions provide valuable insights into designing more resilient, user-friendly, and secure digital infrastructures. Future research should continue bridging the gap between usability, security, and technological advancements to enhance trust and effectiveness in critical applications.

Acknowledgments: This special issue was organised by the special interest group Usable Safety and Security, originally founded in 2015 under the name Human-Machine Interaction in Safety-Critical Systems, within the Human-Computer Interaction division of the German Informatics Society (GI). We would like to thank all the authors and reviewers who made this special issue possible.
Research funding: This research was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 (CROSSING) – 236615297 and SPP 2199 - Project number 521584557 (PervaSafe Computing), and by the German Federal Ministry of Education and Research (BMBF) and the Hessian Ministry of Science and Research, Arts and Culture (HMWK) within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

1. Kahle, M.; Kempf, M.; Martin, B.; Glaser, R. Classifying the 2021 “Ahrtal” Flood Event Using Hermeneutic Interpretation, Natural Language Processing, and Instrumental Data Analyses. *Environ. Res. Commun.* **2022**, *4* (5), 16.
2. Behnassi, M.; El Haiba, M. Implications of the Russia—Ukraine War for Global Food Security. *Nat. Hum. Behav.* **2022**, *6* (6), 754—755.
3. Murray, C. J. L. COVID-19 will Continue but the End of the Pandemic is Near. *Lancet* **2022**, *399* (10323), 417—419.
4. Steffen, W.; Richardson, K.; Rockström, J.; Cornell, S. E.; Fetzer, I.; Bennett, E. M.; Biggs, R.; Carpenter, S. R.; de Vries, W.; de Wit, C. A.; Folke, C.; Gerten, D.; Heinke, J.; Mace, G. M.; Persson, L. M.; Ramanathan, V.; Reyers, B.; Sörlin, S. Planetary Boundaries: Guiding Human Development on a Changing Planet. *Science* **2015**, *347* (6223), 1259855.
5. Naveed Noor, M.; Kumar Prankumar, S.; Alkhaldi, M.; Torres, I. Academic Voices on the Health and Humanitarian Crises in Gaza. *Med. Conflict Surviv.* **2025**, 1—17.
6. Imran, M.; Castillo, C.; Diaz, F.; Vieweg, S. Processing Social Media Messages in Mass Emergency: A Survey. *ACM Comput. Surv.* **2015**, *47* (4), 1—38.
7. Kaufhold, M.-A. *Information Refinement Technologies for Crisis Informatics: User Expectations and Design Principles for Social Media and Mobile Apps*; Springer Vieweg: Wiesbaden, Germany, 2021.
8. Heise, M.; Pietsch, M.; Steinke, F.; Bauer, M.; Yilmaz, B. Optimized UAV Placement for Resilient Crisis Communication and Power Grid Restoration. In *2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*; IEEE: Novi Sad, Serbia, 2022; pp. 1—5.
9. Kuntke, F.; Baumgärtner, L.; Reuter, C. Rural Communication in Outage Scenarios: Disruption-Tolerant Networking via LoRaWAN Setups. In *Proceedings of Information Systems for Crisis Response and Management (ISCRAM)*, 2023; pp. 1—13. https://idl.iscram.org/files/kuntke/2023/2581_Kuntke_etal2023.pdf.
10. Ki Kwok, P.; Yan, M.; Chan, B. K. P.; Lau, H. Y. K. Crisis Management Training Using Discrete-Event Simulation and Virtual Reality Techniques. *Comput. Ind. Eng.* **2019**, *135*, 711—7225.
11. Kwok, P. K.; Yan, M.; Qu, T.; Lau, H. Y. K. User Acceptance of Virtual Reality Technology for Practicing Digital Twin-Based Crisis Management. *Int. J. Comput. Integrated Manuf.* **2021**, *34* (7 8), 874—887.
12. Kaufhold, M.-A. Exploring the Evolving Landscape of Human-Centred Crisis Informatics: Current Challenges and Future Trends. *I-com — J. Interact. Media* **2024**, *23*, 155—163.
13. Schmid, S.; Guntrum, L.; Haesler, S.; Schultheiß, L.; Reuter, C. Digital Volunteers During the COVID-19 Pandemic: Care Work on Social Media for Socio-Technical Resilience. *Weizenbaum J. Digit. Soc.* 2023, *3* (1), 1—31.
14. Perng, S.-Y.; Büscher, M.; Wood, L.; Halvorsrud, R.; Stiso, M.; Ramirez, L.; Al-Akkad, A. Peripheral Response: Microblogging During the 22/7/2011 Norway Attacks. *Int. J. Inf. Syst. Crisis Response Manag.* **2013**, *5* (1), 41—57.
15. Reuter, C.; Ludwig, T.; Kaufhold, M.-A.; Spielhofer, T. Emergency Services Attitudes Towards Social Media: A Quantitative and Qualitative Survey Across Europe. *Int. J. Hum.-Comput. Stud.* **2016**, *95*, 96—111.
16. Karl, I.; Rother, K.; Nestler, S. Crisis-Related Apps: Assistance for Critical and Emergency Situations. *Int. J. Inf. Syst. Crisis Response Manag.* **2015**, *7* (2), 19—35.
17. Reuter, C.; Kaufhold, M.-A.; Biselli, T.; Pleil, H. Increasing Adoption Despite Perceived Limitations of Social Media in Emergencies: Representative Insights on German Citizens’ Perception and Trends from 2017 to 2021. *Int. J. Disaster Risk Reduct.* **2023**, *96*, 103880.
18. Kaufhold, M.-A.; Riebe, T.; Bayer, M.; Reuter, C. ‘We Do Not Have the Capacity to Monitor All Media’: A Design Case Study on Cyber Situational Awareness in Computer Emergency Response Teams. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI) (CHI ’24)*; Association for Computing Machinery: New York, NY, USA, 2024.
19. Van Der Kleij, R.; Kleinhuis, G.; Young, H. Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Front. Psychol.* **2017**, *8*, 2179.
20. Flegel, N.; Wessel, D.; Pöhler, J.; Laerhoven, K. V.; Mentler, T. Autonomy and Safety: A Quantitative Study with Control Room Operators on Affinity for Technology Interaction and Wish for Pervasive Computing Solutions. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA ‘23)*; Association for Computing Machinery: New York, NY, USA, 2023; p. 10.
21. Flegel, N.; Poehler, J.; Mentler, T.; Laerhoven, K. V. Whereables? Examining Personal Technology Adoption in Contemporary Control Rooms. *IEEE Pervasive Comput.* **2023**, *22* (2), 49—53.
22. Kaufhold, M.-A.; Rupp, N.; Reuter, C.; Habdank, M. Mitigating Information Overload in Social Media during Conflicts and Crises: Design and Evaluation of a Cross-Platform Alerting System. *Behav. Inf. Technol.* **2020**, *39* (3), 319—342.
23. Berndt, H.; Wessel, D. Immersion and Presence in Virtual Reality Training for Mass Casualty Incidents. In *Proceedings of the 15th ISCRAM Conference*, 2018. https://idl.iscram.org/files/henrikberndt/2018/2153_HenrikBerndt_etal2018.pdf.
24. Mentler, T.; Herczeg, M.; Jent, S.; Stoislow, M.; Kindsmüller, M. C.; Rumland, T. Routine Mobile Applications for Emergency Medical Services in Mass Casualty Incidents. *Biomed. Eng./Biomed. Tech.* **2012**, *57*, 784—787.
25. Bäumler, J.; Kaufhold, M.-A.; Voronin, G.; Reuter, C. Towards an Online Hate Speech Classification Scheme for German Law Enforcement and Reporting Centers: Insights from Research and Practice. In *Mensch und Computer 2024 — Workshopband*; Gesellschaft für Informatik e.V.: Karlsruhe, Germany, 2024.
26. Bäumler, J.; Riebe, T.; Kaufhold, M.-A.; Reuter, C. Harnessing Inter-Organizational Collaboration and Automation to Combat Online Hate Speech: A Qualitative Study with German Reporting Centers. In *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing*, 2025.

27. Nestler, S. Evaluation der Mensch-Computer-Interaktion in Krisenszenarien/Evaluating Human-Computer-Interaction in Crisis Scenarios. *I-com* **2014**, *13* (1), 53—62.
28. Rohde, M.; Brödner, P.; Stevens, G.; Betz, M.; Wulf, V. Grounded Design — A Praxeological IS Research Perspective. *J. Inform. Technol.* **2017**, *32* (2), 163—179.
29. Reuter, C. Einleitung in die sicherheitskritische Mensch-Computer-Interaktion. In *Sicherheitskritische Mensch-Computer-Interaktion*; Reuter, C., Ed.; Springer Vieweg: Wiesbaden, 2021.
30. Reuter, C. *Sicherheitskritische Mensch-Computer-Interaktion*; Springer Vieweg: Wiesbaden, 2021.
31. Reuter, C.; Lo Iacono, L.; Benlian, A. A Quarter Century of Usable Security and Privacy Research: Transparency, Tailorability, and the Road Ahead. *Behav. Inf. Technol.* **2022**, *41* (10), 2035—2048.
32. Alt, F.; von Zezschwitz, E. Emerging Trends in Usable Security and Privacy. *I-com* **2019**, *18* (3), 189—195.
33. Mentler, T.; Reuter, C.; Geisler, S. Introduction to This Special Issue on “Human-Machine Interaction and Cooperation in Safety-Critical Systems”. *I-com* **2016**, *15* (3), 219—226.