CYWARN: Strategy and Technology Development for Cross-Platform Cyber Situational Awareness and Actor-Specific Cyber Threat Communication

Marc-André Kaufhold, Thea Riebe, Philipp Kühn, Markus Bayer, Christian Reuter
Science and Technology for Peace and Security (PEASEC)
Technical University of Darmstadt
Darmstadt, Germany
{kaufhold, riebe, kuehn, bayer, reuter}@peasec.tu-darmstadt.de

Jennifer Fromm, Ali Sercan Basyurt, Stefan Stieglitz
Digital Communication and Transformation (digicat)
University of Duisburg-Essen
Duisburg, Germany
{stefan.stieglitz, jennifer.fromm, ali-sercan.basyurt}@uni-due.de

Marc Stöttinger, Reinhard Möller
Hessen CyberCompetenceCenter (Hessen3C)
Hessian Ministry of the Interior and Sports
Wiesbaden, Germany
{marc.stoettinger, reinhard.moeller}@hmdis.hessen.de

Milad Mirbabaie
Management Information Systems
Paderborn University
Paderborn, Germany
milad.mirbabaie@uni-paderborn.de

Kaan Eyilmez, Christoph Fuchß
Virtimo AG
Berlin, Germany
{kaan.eyilmez, fuchß}@virtimo.de

ABSTRACT

Despite the merits of digitisation in private and professional spaces, critical infrastructures and societies are increasingly exposed to cyberattacks. Thus, Computer Emergency Response Teams (CERTs) are deployed in many countries and organisations to enhance the preventive and reactive capabilities against cyberattacks. However, their tasks are getting more complex by the increasing amount and varying quality of information disseminated into public channels. Adopting the perspectives of Crisis Informatics and safety-critical Human-Computer Interaction (HCI) and based on both a narrative literature review and group discussions, this paper first outlines the research agenda of the CYWARN project, which seeks to design strategies and technologies for cross-platform cyber situational awareness and actor-specific cyber threat communication. Second, it identifies and elaborates eight research challenges with regard to the monitoring, analysis and communication of cyber threats in CERTs, which serve as a starting point for in-depth research within the project.

CCS CONCEPTS

• Security and privacy → Human and societal aspects of security and privacy → **Usability in security and privacy**

Mensch und Computer 2021, Workshopband, Workshop on 8. Workshop Mensch-Maschine-Interaktion in sicherheitskritischen Systemen.

https://doi.org/10.18420/muc2021-mci-ws08-263

KEYWORDS

Computer Emergency Response Teams, Situational Awareness, Collaboration, Crisis Informatics, Human-Computer Interaction

ACM Reference format:

Marc-André Kaufhold, Jennifer Fromm, Thea Riebe, Milad Mirbabaie, Philipp Kühn, Ali Sercan Basyurt, Markus Bayer, Marc Stöttinger, Kaan Eyilmez, Reinhard Möller, Christoph Fuchß, Stefan Stieglitz and Christian Reuter. 2021. CYWARN: Strategy and Technology Development for Cross-Platform Cyber Situational Awareness and Actor-Specific Cyber Threat Communication. In *Mensch und Computer 2021 - Workshopband.* Bonn: Gesellschaft für Informatik e.V., https://doi.org/10.18420/muc2021-mci-ws08-263

1 Introduction

In a globalised world with a growing number of cyber threat situations, citizens and states are faced with a multitude of challenges [1]. This has been brought back to public attention not least by the WannaCry ransomware in 2017, which infected over 230,000 computers in over 150 countries, or the doxing of German politicians, journalists and celebrities in 2018/19. Such cyber-attacks pose an increasing threat to socio-cultural infrastructures, as they can cause a breakdown of important communication channels, the disclosure of personal data and the failure of critical infrastructures (CI). Technological developments in the context of digitalisation, such as the Internet of Things [2] or smart cities, enable ever greater connectivity in private and professional contexts. This effect is amplified by the current and global COVID-19 pandemic, whereby parts of business (e.g. home office) and public life

(e.g. digital teaching and social exchange) are becoming increasingly digitised, the complexity of the information space increases and new demands on the security of citizens arise [3].

Especially media and information infrastructures are threatened by cyber-attacks, as they are increasingly built on IT infrastructures, and the potential danger of cybercrime for citizens, authorities and companies is increasing [4]. Subsequently, the detection and analysis of and defence against such attacks are an important basis for civil security. This is particularly important against the background of a growing frequency and professionalism of cyber-attacks, the diversity of threats as well as an increasing interconnectedness of data infrastructures. This is where the Computer Emergency Response Teams (CERTs) come into play. They describe themselves as "the central contact point for preventive and reactive measures in the event of security-relevant incidents in computer systems" [5]. Amongst others, state-level CERTs provide cyber security reports for ministries, consult small- and medium-sized enterprises (SMEs), including critical infrastructure (CI) providers, with regard to security incidents or provide information on how to better protect against cyber threats for citizens. The German federal administration provides an interesting case as it facilitates the collaboration between independent cybersecurity organisations for the 16 states and the federal government. The states are represented by 13 CERTs within the public administrations or in state companies, whereas the federal CERT-Bund is integrated in the Federal Office for Information Security (BSI). The individual CERTs are part of the Administrative CERT Network (VCV) which provides an information exchange platform to institutionalise CERT partnerships.

By analysing the situation in cyberspace and issuing recommendations for action and warnings directed at different actors, such as citizens, authorities and CI operators, CERTs contribute significantly to raising awareness of cyber-attacks and threats. However, CERTs face major challenges in this context, which must be overcome by new strategies, methods and technologies. This paper sets up the research agenda of the CYWARN project and seeks to identify and elaborate these challenges, such as the gathering and analysis of a multitude of confusing information in complex cyber situations, inter-organisational collaboration with other CERTs and the BSI for effective incident management [6], actor-specific communication to affected stakeholders as well as the protection of sensitive data and compliance with data protection regulations [7]. First, it will present related work (Section 2) and the method (Section 3) of this paper. Second, it will present the research agenda of the CYWARN project including goals, the security scenario and planned innovations (Section 4). Thereafter, the paper discusses the identified research challenges (Section 5) and finishes with a short conclusion (Section 6).

2 Related Work

The organisation, collaboration and technology use of spatially and temporally distributed emergency response teams in general and specifically in the public sector is researched extensively within the domains of HCI and CSCW [8]–[10]. There has been substantial research on how technology design and use influences and supports response teams, their workflows and collaborative work [8], [11], [10]. In this sense, collaboration can be described as the development of a set of common practices to monitor individual behaviour and enable task coordination as well as flexible division of labour. Furthermore, technology provides a set of tools through which certain activities within the present setting become visible or publicly accessible. To allow effective crisis management, the practices are developed to be staff-independent so that adoption by newcomers without previous collaboration and without much explanation is possible [12].

2.1 Organisation of State CERTs

Incident response in uncertain and tense situations has been studied in HCI with regard to natural and man-made disasters, focusing on the collaboration between different emergency services as well as with citizens [13]–[15]. In terms of cyber incident response, state-level CERTs have become important organisations to protect citizens, public administration and CI against cyberattacks and their potential real-world impact [16]. CERTs are found in public and private organisations, providing a variety of proactive and reactive services [17] to achieve their goal "to be a focal point for preventing, receiving and responding to computer security incidents" [5]. Existing work has been emphasising the necessity of collaboration between the different CERTs as well as with other security experts and volunteers [18], [19]. Comparing national security strategies, Boeke [20] has highlighted that due to the state's size, Estonian cyber security largely relies on the help of state-directed civilian volunteers and international cooperation. In the United Kingdom, studies have found that cybersecurity is the task of the private sector with less importance of state interference as a consequence of privatising communication infrastructure [21].

With regard to German state CERTs, research has focused on the implications of the federal structure for cyber security [22]. Legal experts have suggested a reform of the federal security architectures due to the increasing challenges of cyber security, effectively integrating the local and state level response into national security strategy [23]. In this context, studies also showed that a decentralised approach to security can also improve crisis response [24]. Distributed management as well as information and experience sharing has shown to positively impact effectiveness of cyber security [23]. Van der Kleij [25, pp. 6–7] identified additional factors influencing the performance of CERTs such as "coordination and sharing information with outside parties", "collaborative problem-solving capacity and shared incident awareness" and "organizational and incident learning". This is supported by Ahmad [26], who suggests double-loops for learning, meaning that the learning should not only be about individual incidents but also systematic response structures. Furthermore, the participation in cyber security defence competitions for simulation training is also desirable [27]. To create educational simulations for the training of municipal security experts for effective defence, Gedris et al. [28] derived design implications for cyber security scenarios that reflect the complex socio-technical context of public infrastructure.

2.2 Technology and Collaboration of CERTs

To fulfil their tasks and enhance cyber incident response, CERTs use a variety of different technologies, especially Cyber Threat Intelligence (CTI) platforms; moreover, to facilitate collective crisis management, they maintain cross-organisational collaboration with other CERTs and external stakeholders [29]. Incident monitoring has shown to become more complex due to increasing digitisation and services that CERTs have to provide. Often, procedures for incident reporting and management are not standardised, and sometimes there are legal and psychological constraints to reporting due to data protection and company policies [30]. Receiving and analysing threat incident information necessitated additional security infrastructure and access for CERTs, such as information on network traffic [31], deep packet inspection [32], and the use of machine learning to support incident detection [33]. Padayachee and Worku [34] highlight that collaboration among CERTs offers advantages, as they are more easily alerted to large-scale cyber security incidents and better capable to manage them adequately. Whereas many private and governmental actors still manage cyber security incidents individually, interconnected networks can be better protected against internationally operating criminal groups with a shift towards cross-organisational information exchange [35]. Khurana et al. [36] propose the prototype "Plantir" to facilitate effective multi-site cyber incident response including a collaborative workspace for discussions and data exchange. The authors highlight that trust between organisations is a central precondition for the sharing of incident data.

Despite the identified need for cross-organisational collaboration and information exchange between cyber security organisations like CERTs [25], cooperation between law enforcement agencies has remained at the focus of study [37], [38]. In the German CERT architecture, the communication between the federal- and the state-level CERTs as well as the private CERTs is considered as pivotal to achieve situational awareness on the scope and severity of incidents and decide on adequate measures [39], [40]. After the initial establishment of CERTs in Germany, Kossakowski [16] observed that additionally to scarce time resources, also insufficient trust relationships impaired cooperation. Thus, the work of security experts consists of "heterogenous bundles of practices" for the shared commitment towards cyber security [41]. Therefore, our research project takes the organisational structure and the use of technology into account.

3 Method

We conducted a narrative literature review and group discussions to develop the research agenda of the CYWARN project and identify research challenges for developing CERT-focused strategies and technologies for cross-platform cyber situational awareness and actor-specific cyber threat communication. First, narrative literature reviews aim to summarise prior knowledge, address a broad scope of questions or topics, usually deploy a selective search strategy and integrate both conceptual and empirical work [42]. We used Google Scholar to search for domain-specific (i.e. crisis informatics, cyber situational awareness and cyber threat communication) and method-specific (i.e. supervised machine learning, visual analytics and technology assessment) literature, focussing on method applications within the present domain.

Second, following the search process, we conducted multiple group discussions among the authors. These discussions did not follow a predefined structure but were designed to achieve a first sketch of the research idea and then iteratively integrate and revise our findings into the final research agenda (Section 4) and distinct research challenges (Section 5). Both results serve as a starting point for more comprehensive and rigor research within the three-year CYWARN project, including systematic literature reviews, qualitative and quantitative empirical research, design science research, usability and user experience research as well as technology assessment.

4 Results I: The Research Agenda

The aim of CYWARN is to develop strategies and technologies for CERTs to analyse and communicate the *cyber-situation*. This helps to improve the *early detection* of cyber threats (preparation) and the implementation of *countermeasures* (response) to protect media and information infrastructures by CERTs. The process is supported by a novel demonstrator and includes (I) the automated collection and integration of data from public and closed sources, (II) the intra- and inter-organisational data analysis with credibility assessment of content and sources using visual analytics and (III) the cross-channel communication of cyber threats to different stakeholders (e.g. citizens, authorities and CI operators) to enable them to best protect themselves. The social, practical and scientific relevance of the project is ensured by the work plan. It includes theory-oriented systematic literature studies, qualitative and quantitative empirical studies (WP1), participatory demonstrator and strategy developments (WP2, WP3), evaluations of acceptance and usability (WP4) and an assessment of the ethical, legal and social implications (WP5).

CYWARN aims to added value through strategies, methods and technologies for improved preparation and response to cyber threats. Crisis informatics has so far mainly focused on the use of social media by emergency services, especially fire departments and the police, in "physical" large-scale incidents and emergencies [14]. In contrast, CYWARN examines information sources in cyberspace more comprehensively in the sense of *Open-Source Intelligence (OSINT)* and, with CERTs, places a new actor at the centre of the research project that focuses on the "virtual" threat situation in cyberspace. In contrast to IT security, CYWARN does not intend to develop and investigate attack methods and means or protective measures. Instead, it aims to enhance civil security with regard to the protection of media and information infrastructures through socio-technical solutions and organisational strategies that improve the analysis of the cyber situation and the communication of cyber threats by CERTs. The project provides support for CERTs in their central activity of situation assessment, communication and coordination. The implementation of the suggested security measures is eventually carried out by IT security officers and IT service providers on the basis of CERT alerts.

4.1 Security Scenario

Even though concepts and technologies of information and IT security can improve the confidentiality, availability and integrity of socio-technical systems, absolute security in cyberspace cannot be guaranteed [43]. Therefore, threatened actors must be provided with warnings and recommendations for action to strengthen civil security in the sense of an early warning system but also in response to a cyber incident. The specific target group-oriented preparation of such notifications is a major challenge for CERTs, as the following security scenario illustrates.

First, detection and classification of security vulnerabilities and software: Based on the degree of distribution and the associated active support in security patch management by the responsible IT service provider, software is classified by CERTs as A-, B- or C-software. Microsoft Office, for example, is A-software because it is used in most private households as well as in companies and other organisations. It is also included in the standard scope of delivery of a workstation computer in state and local government, implemented by IT service providers and continuously supplied with software updates and security patches. An example of B-software would be software that is not needed by all users and is provided by the IT service provider upon request, i.e. it is not used in all public authorities. C-software, on the other hand, is only used by individual organisations and often has to be managed and provided with updates by the using organisation itself.

Second, monitoring and analysis of the cyber situation: A security vulnerability in A-software thus affects most users at first glance. Due to increasing digitisation, the number of hardware and software that CERTs have to keep an eye on in order to detect security vulnerabilities at an early stage is growing. This takes place mainly through manual monitoring of software manufacturers' websites as well as of posts on social media and technology blogs. Manually collecting and evaluating information from an increasing number of different information channels represents an immense effort, which is why the focus is primarily on identifying security vulnerabilities in A-software. In the absence of automated methods for the collection and evaluation of data sources, it is becoming increasingly difficult for CERTs to identify and communicate security vulnerabilities in B- and C-software in a timely manner. There is also the challenge of assessing the credibility of vulnerability reports unless they are published by the software or hardware manufacturer itself. Often, due to a multitude of citations on different sites on the internet, the original source of the report is difficult to find and even if it can be located, its competence and credibility is often difficult to assess. However, undetected security vulnerabilities can have serious consequences for infrastructures even in B- and C- software. Security vulnerabilities in less common software could, for example, be used to penetrate critical information infrastructures of the Ministry of the Environment or a CI operator. Taking the example of the Ministry of the Environment and its competent authority for chemical safety, the Darmstadt Regional Council, vacant security gaps that are already known to criminals or terrorists but have not yet been patched or shut down quickly enough could have consequences for the control of chemical safety at chemical plants. Such a situation would quickly expand from the cyber security realm, which integrates cybercrime as a law enforcement challenge, into the area of fire- and disaster-control.

Third, prioritised cross-actor communication of cyberthreats: In addition to the timely detection of vulnerabilities in B- and C-software, other significant challenges are both the appropriate assessment, including a preliminary evaluation of the criticality and urgency of vulnerabilities (e.g. taking into account the CVSS score, which is an open framework for communicating the characteristics and extent of software vulnerabilities) and the communication of vulnerabilities to those affected for effective and timely remediation. CERTs are faced with an increasing number of different stakeholders whose information interests must be taken into account depending on the situation. These include not only the state and local governments (and also subgroups of authorities with a prominent role in security situations, such as the police, the judiciary and MPs), CI operators and the IT service providers of the state and local governments but also politicians and citizens. In the event of a vulnerability in B- or C-software at the Ministry of the Environment, CERT staff would therefore not only have to instruct often less trained staff but also assess the damage and communicate it to other departments. They would not be able to take action at the Ministry of Environment themselves and would therefore have to rely on the proper implementation of measures by the information security officer and the IT service providers. If several serious vulnerabilities arise within a short period of time, additional concepts for the sequence of processing must be developed and prioritisation of reports to the actors must be carried out.

4.2 Planned Innovations

In CYWARN, strategic, methodological and technological solutions are created that seek to optimise the information collection and analysis processes of CERTs and make them future-proof. The protection of media and information infrastructures is supported by communication and processing procedures involving diverse actors. The CYWARN architecture will be based on five sub-goals, which are designed, implemented, evaluated and improved through iterative computer and social science research:

First, a **framework** that focuses on the systematic collection, analysis and evaluation of data from public sources (blogs, feeds, photo and video portals, sensors, social media, websites) in the sense of an open-source intelligence approach to create a cyber situation picture. Although the focus is on cyber threats and CERTs, a framework transferable to other domains is sought through the continuous involvement of associated partners. While previous research in crisis informatics has mainly focused on the analysis of social media in disaster situations, the novel framework of CYWARN includes additional public data sources and complements the scenario of security-critical incidents in cyberspace.

Second, **empirical insights** about the intra- and inter-organisational analysis and communication of cyber threats and security vulnerabilities in CERTs, also in cooperation with the CERT-Bund and the BSI, as well about expectations and current practices of authorities, citizens and CI operators with regard to the

communication of cyber threats. In CYWARN, these findings will be used to serve as the basis for the user-oriented development of novel strategies and technologies for CERTs to enhance civil security, to expand the current state of research through scientific publications and to communicate lessons learned to CERTs citizens, and other relevant stakeholders.

Third, long-term organisational **strategies** for CERTs, considering the advancing digitisation, connectivity and constant change of the technology landscape, for systematic intra- and inter-organisational analysis and early warning, especially in cooperation with the BSI and other CERTS, as well as for the communication of cyber threats to external actors, e.g. citizens, authorities and CI operators. This includes the selection and (further) development of exchange formats and of novel best practices and guidelines for inter-organisational cooperation and external communication, considering the demonstrators tested in CYWARN as well as event-based, organisational and social frameworks.

Fourth, CYWARN intends to design **methods** for credibility analysis and prioritisation of public content and sources (with regard to cyber threats and security vulnerabilities), which combine metadata-based indicators and explainable machine learning (white-box approach) as a novel approach. This facilitates the optimisation of the classification quality compared to existing black-box approaches, which are difficult to understand for end users, establishes transparency for algorithmic decisions and allows to investigate its influence on the users' acceptance of and trust in the algorithms and the entire CYWARN demonstrator.

Finally, a **demonstrator** for cross-media collection of public data sources (base module), real-time based and configurable visual analysis for early detection and prioritisation of cyber threats and vulnerabilities based on open and closed data sources (analysis module) and actor-specific communication of recommended actions, awareness raising measures, situation reports and alerts (communication module). Through a high degree of automation and the use of templates, the demonstrator enables CERTs to identify, analyse and communicate cyber threats and vulnerabilities more effectively and efficiently.

5 Results II: Identified Research Challenges

Based on the overall research agenda, we elaborated eight distinct research challenges combined with information on how CYWARN will attempt to overcome these challenges.

5.1 Using Crisis Informatics, Communication and Situational Awareness Research (C1)

Research over the past 20 years shows that prevention, management and recovery in disasters, crises and emergencies are increasingly dependent on ICT [43]. Crisis informatics, at the intersection between computer science and social sciences, has primarily investigated the use of social media with regard to disaster scenarios, usage patterns, roles or perceptions [44], [14]. The domain has explored the use of social media in the context of physical, natural (e.g. wildfires, earthquakes, landslides, floods or hurricanes) or anthropogenic crises (e.g. building collapses, bombings or shootings) [13], [14]. In addition to the potentials of citizen self-organisation and official crisis communication via social media [45], [46], emergency services are faced with the question of how user-generated information (e.g. eyewitness reports, photos, videos and status updates [47]) can contribute to an improvement of crisis communication and situational awareness [48], [40].

In CYWARN, crises are investigated that originate from cyberspace but have an impact on physical space (e.g. infestation of end devices, failure of critical communication or power infrastructures), thus bringing CERTs to the fore as a unit of hazard protection. This will involve basics of cyber situational awareness, including the elements of network awareness (assets and defence capability), threat awareness (attack methods and vulnerabilities), operational awareness and prediction of the future situation [49].

5.2 Open-Source Intelligence for the Collection of Cyber Information (C2)

For the technical establishment of the cyber situation picture, open and closed data sources must first be collected. While CERTs already have internal closed data sources, open data sources are usually evaluated manually. Nevertheless, for example, there are already initial approaches to extract cyber threats and security vulnerabilities from Twitter [50]. In crisis informatics, however, it has been noted that different social media are used for different purposes and therefore cross-source strategies and technologies are needed to support situational awareness [51]. Furthermore, information relevant to CERTs is often published outside social media. The CYWARN project therefore pursues the goal of enabling the search for and creative combination of publicly accessible information [52], i.e. from blogs, feeds and websites in addition to social media, in a semi-automated manner and integrating it into a cyber situation picture. For this purpose, official developer interfaces (application programming interfaces) should essentially be used, but if necessary, alternative access options (e.g. analysis of website code) are also to be developed, taking into account legal framework conditions [53].

5.3 Filtering and Prioritisation of Relevant Cyber Information (C3)

The analysis of social media in professional and private contexts as well as in large-scale disaster situations is already subject to the challenge that the large quantity of media and text information, also called big social data or big crisis data [54], [55], generated across platforms such as Facebook, Twitter and YouTube, can lead to information overload and can thus no longer be analysed by individuals or organisations [56], [57]. If social media are now supplemented by other public sources, this problem intensifies. In addition to legal, personal, organisational and strategic factors of information exploitation [47], [58], technical support solutions can contribute to reducing information overload [59], [60].

Research shows that technical support solutions can be used to reduce the amount of data by means of a thought-out usability, configurable filtering mechanisms, duplicate detection, classifiers to automatically hide irrelevant information, grouping of similar messages and information summaries [61], [62]. Artificial

intelligence approaches show that very accurate models for the automatic classification of relevant information can be developed efficiently by including text and metadata and using active learning, even though domain requirements must be taken into account in the learning process of the model [63]. In CYWARN, in addition to usability and configurable filter mechanisms, a model for classifying relevant information with regard to cyber threats and security gaps will be tailored in order to contribute to the strategic prioritisation of cyber information.

5.4 Indicator- and Learning-based Credibility Assessment of Cyber Information (C4)

After collection and filtering, the quality of information needs to be assessed. In existing research, information quality in social media has been operationalised as a multidimensional construct of credibility, relevance, completeness, comprehensibility and timeliness of information [64], [65]. While the relevance of information is already addressed in the context of data filtering, CERTs need to be supported in the credibility assessment of sources and content. Existing research shows that (journalistic) gatekeeping, algorithmic supervised machine learning solutions for the automatic assessment of credibility criteria, indicator-based visual assistance systems such as TrustyTweet or the improvement of media literacy can contribute to the assessment of information quality [66]–[69]. As previous machine learning approaches are predominantly implemented as a black box, the user does not gain insight into the decision criteria of the underlying model, which can limit the trust in the decision made and complicates the improvement of model quality [62]. In CYWARN, a novel approach is implemented combining an indicator-based approach with an explainable white-box learning approach [66].

5.5 Visual Analysis of the Cyber Situation (C5)

Not only the filtering and analysis of social media data but also the visualisation of the large amounts of unstructured data is difficult [57]. Visual analytics combines automatic analysis techniques with interactive visualisations to enable effective comprehension, inference and decision-making based on large and complex data sets. In interviews, emergency response teams also confirmed that they lack technologies, methods and expertise for collecting, filtering and visualising social media data [58]. In research, there already exist approaches to visualise crisis-related information by means of augmented reality in order to reduce the cognitive load of emergency managers when processing the information [70]. Furthermore, the first systems for visualising geodata and the emotionality of tweets have been developed in the research field of visual analytics [71]. However, it is still unclear how social media data and, in the broader sense of the application, open-source data can be used for the detection of cyber-attacks and how the data would have to be visually processed so that a clear cyber situation picture can be conveyed that supports decision-making processes. Here, CYWARN plans to contribute to a comprehensible visualisation by initially incorporating the state of the art of visual analytics research and then extending it via evaluation studies.

5.6 Cross-Actor Communication of Cyber Threats and Warnings (C6)

In crisis informatics, there are numerous case studies in which the dissemination of content on social media was examined before, during and after crisis situations. A large number of these case studies focus on Twitter communication during man-made crises, such as the terrorist attacks in Brussels [72], and during natural disasters, such as hurricane Harvey [73]. Influential actors in crisis communication have already been identified as well as typical content that is observable over the course of crises [74]. In this context, it has been shown that emotional messages in particular spread faster during crisis situations [75]. In addition, other factors such as the length of the message, the addition of URLs, images and videos as well as the number of followers of the authors play an important role in the effective dissemination of crisis-related information [76]. Furthermore, depending on sociodemographic factors (e.g. age, education, gender, income or region) citizens use different media, such as crisis apps, radio, social media, television or websites, to stay informed during crises [77], [78]. However, little attention has been paid to cyber threat communication yet. In particular, there is a lack of research on the effective and targeted dissemination of cyber alerts to specific actors, as most studies to date have focused on how to reach the largest possible user base on social media. CYWARN seeks to address this research gap.

5.7 Organisational and Strategic Integration of Cyber Threat Technology (C7)

Even if technological innovations, which are planned in CYWARN, promise added value for the analysis of the cyber situation, they must be in line with organisational, social and strategic factors of the CERTs. In this context, mere adaptation to existing strategies is usually not sufficient, since the introduction of technology gives rise to new strategic requirements and patterns of use that were not or cannot be anticipated in advance [79], which is why CYWARN pursues integrated strategy and technology development. To implement the proposed strategies (see Section 2.2), plans and guidelines need to be drafted that support the achievement of organisational goals [80]. These should take into account the phases of the crisis management cycle (preparation, response and follow-up), the use of different technologies (existing and new technologies designed by CYWARN), organisational framework conditions (metrics, resources, roles and responsibilities) and collaboration with stakeholders (e.g. externally with authorities and citizens, as well as inter-organisationally with other CERTs).

With regard to the interaction with citizens, previous national and international comparative studies illustrate that German citizens in particular expect emergency services to continuously monitor social media and respond promptly to enquiries [81]. In CYWARN, attitudes and expectations of citizens with regard to the analysis and communication of cyber threats by CERTs will also be surveyed in order to derive implications for the implementation of the strategies [82], [83].

5.8 Ethical-Social Implications and Technology Assessment (C8)

Assessing ethical and social implications at an early stage in order to minimise undesirable consequences and thus ensure the acceptance and success of a project is an increasingly important requirement in research and development of technical artefacts in safety-critical HCI [84], [85]. This includes not only methods for privacy impact analysis (PIA), which addresses legal requirements, but also in particular the design of room for manoeuvre for users in the sense of a "decision architecture", which should prevent tragic decisions [86, p. 75]. In order to comply with the recommendations of the German Data Ethics Commission, the collection, storage and access to data must be reviewed iteratively, as must the data processing methods used, such as machine learning algorithms and the interfaces for user interaction [87]. A range of methods has evolved to assess technology impacts early and iteratively during the design process: User-centred design approaches [88] and participatory co-design approaches [89], [90] have emerged from design research since the 1980s with the intent to anticipate users' practices and requirements, particularly by incorporating interdisciplinary user perspectives. This enables experimentation with scenarios and the facilitation of desirable technology use and socio-technical interaction [91, p. 5].

However, when designing crisis technologies, not only the interests of the direct users but also of indirect actors need to be taken into account. Value-Sensitive Design (VSD), a theory and method that systematically integrates the interests of direct and indirect participants (stakeholders) within the design process, is suitable for this purpose in order to incorporate values such as privacy and autonomy into technology design [92]. The method is particularly suitable for the iterative negotiation of conflicts between values, involving users, developers and designers [92], [93], [91]. VSD offers opportunities for these negotiations at different levels but is more commonly used in direct human-machine interaction, such as in medical technology development [94], [95]. In CYWARN, research is also being conducted into how ethical and social consequences of technology can be assessed at an early stage, particularly in the CERT context, and how, derived from this, contradictions in the requirements of direct and indirect stakeholders can be negotiated and balanced as far as possible. This includes their use practices of safety-critical information systems as well as the collection, analysis and visualisation of data from public and closed sources.

6 Conclusion

In this paper, we presented the goals, scenario and planned innovations of the CYWARN project and identified eight research challenges for developing strategies and technologies in order to enhance the cross-platform cyber situational awareness and actor-specific cyber threat communication of CERTs. Using the lens of HCI, these challenges discuss a meaningful integration of humans and technology, including human-centred usage patterns, roles and perceptions (C1), semi-automatic data collection (C2), configurable, usable and transparent analytics (C3, C4, C5), actor-specific communication (C6), organisational integration (C7) and social implications (C8). However, the conducted narrative literature review does not "involve a systematic and comprehensive search of all relevant literature" [42] and the group discussions followed an open structure, lacking explicit and reproducible methods. Thus, based on these initial challenges, the project has started conducting systematic literature reviews on cyber situational awareness and cyber threat communication, performing qualitative expert interviews with German CERT personnel [4] and conceptualising a representative citizen survey. The theoretical and empirical insights will he used to design, implement and evaluate supportive strategies and technologies. Finally, the project will explore the transfer of results to enterprise-level CERTs, IT security advisors and other related organisations.

ACKNOWLEDGMENTS

This work has been funded by the German Federal Ministry of Education and Research (BMBF) in the project CYWARN (13N15407-13N15410).

REFERENCES

[1] John S. II Davis, Benjamin Boudreaux, Jonathan William Welburn, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase. 2017. Stateless Attribution: Toward International Accountability in Cyberspace.

[2] Thomas Ludwig, Peter Tolmie, and Volkmar Pipek. 2019. From the Internet of Things to an Internet of Practices. In *Proceedings of 15th European Conference on Computer-Supported Cooperative Work - Exploratory Papers*, DOI: 10.18420/ecscw2017-10.

[3] Bo Xie et al. 2020. Global healtah crises are also information crises: A call to action. *Journal of the Association for Information Science and Technology*, 1–5. DOI: 10.1002/asi.24357.

[4] Thea Riebe, Marc-André Kaufhold, and Christian Reuter. 2021. The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study. *Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing*, CSCW, 1–26.

[5] Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. 2003. State of the Practice of Computer Security Incident Response Teams (CSIRTs)., Pittsburgh, PA, USA.

[6] Mag Edith Huber and Otto Hellwig. 2016. Wissensaustausch und Vertrauen unter Computer Emergency Response Teams – eine europäische Herausforderung. *Datenschutz und Datensicherheit - DuD*, 6, 162–166.

[7] Kurt Einzinger and Florian Skopik. 2017. Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken. *Datenschutz und Datensicherheit - DuD*, 41, 9, 572–576. DOI: 10.1007/s11623-017-0833-9.

[8] Camille Cobb et al. 2014. Designing for the Deluge: Understanding & Supporting the Distributed, Collaborative Work of Crisis Volunteers. In *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*, ACM, 888–899 DOI: 10.1145/2531602.2531712.

[9] David Mendonça, Theresa Jefferson, and John Harrald. 2007. Collaborative adhocracies and Mix-and-Match Technologic in emergency management. *Communications of the ACM*, 50, 3, 44–49. DOI: 10.1145/1226736.1226764.

[10] Christian Reuter, Thomas Ludwig, and Volkmar Pipek. 2014. Ad Hoc Participation in Situation Assessment: Supporting Mobile Collaboration in Emergencies. *ACM Transactions on Computer-Human Interaction (ToCHI)*, 21, 5, 1–26. DOI: 10.1145/2651365.

[11] Sophia B. Liu. 2014. Crisis Crowdsourcing Framework: Designing Strategic Configurations of Crowdsourcing for the Emergency Management Domain. *Computer Supported Cooperative Work (CSCW)*, 23, 4–6, 389–443. DOI: 10.1007/s10606-014-9204-3.

[12] Christian Heath and Paul Luff. 1992. Collaboration and control. Crisis management and multimedia technology in London Underground Line Control Rooms. *Computer Supported Cooperative Work (CSCW)*, 1, 1–2, 69–94. DOI: 10.1007/BF00752451.

[13] Alexandra Olteanu, Sarah Vieweg, and Carlos Castillo. 2015. What to Expect When the Unexpected Happens: Social Media Communications Across Crises. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, New York, USA, ACM, 994–1009 DOI: 10.1145/2675133.2675242.

[14] Christian Reuter and Marc-André Kaufhold. 2018. Fifteen Years of Social Media in Emergencies: A Retrospective Review and Future Directions for Crisis Informatics. *Journal of Contingencies and Crisis Management (JCCM)*, 26, 1, 41–57. DOI: 10.1111/1468-5973.12196.

[15] Robert Soden and Leysia Palen. 2018. Informating Crisis: Expanding Critical Perspectives in Crisis Informatics. In *Proceedings of the ACM on Human-Computer Interaction*, New York, NY, ACM DOI: https://doi.org/10.1145/3274431.

[16] Klaus-Peter Kossakowski. 2000. *Information technology incident response capabilities*. Hamburg.

[17] Johannes Wiik, Jose J. Gonzalez, and Klaus-Peter Kossakowski. 2006. Effectiveness of Proactive CSIRT Services. *FIRST Conference*, 2–11.

[18] Ramian Fathi, Dennis Thom, Steffen Koch, Thomas Ertl, and Frank Fiedrich. 2020. VOST: A case study in voluntary digital participation for collaborative emergency management. *Information Processing and Management*, 57, 4, 102174. DOI: 10.1016/j.ipm.2019.102174.

[19] Rebecca Slayton and Brian Clarke. 2020. Trusting infrastructure: The emergence of computer security incident response, 1989-2005. *Technology and Culture*, 61, 1, 173–206. DOI: 10.1353/tech.2020.0036.

[20] Sergei Boeke. 2018. National cyber crisis management: Different European approaches. *Governance*, 31, 3, 449–464. DOI: 10.1111/gove.12309.

[21] Jamie Collier. 2017. Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom. In *Ethics and Policies for Cyber Operations*, Mariarosaria Taddeo and Ludovica Glorioso (Eds.). Basel, Springer International Publishing, 187–212 DOI: 10.1007/978-3-319-45300-2_9.

[22] Stiftung Neue Verantwortung. 2019. Staatliche Cyber-Sicherheitsarchitektur Version 3. 4.

[23] André Duvillard and Melanie Friedli. 2018. Nationale Cyber-Strategie: Einbezug der lokalen Ebene in einem föderalen Staat. In *Cybersecurity Best Practices*, Springer Fachmedien Wiesbaden, 117–123 DOI: 10.1007/978-3-658-21655-9_10.

[24] Carmine Scavo, Richard C. Kearney, and Richard J. Kilroy. 2007. Challenges to Federalism: Homeland Security and Disaster Response. *The Journal of Federalism*, 38, 1, 81–110.

[25] Rick Van der Kleij, Geert Kleinhuis, and Heather Young. 2017. Computer security incident response team effectiveness: A needs assessment. *Frontiers in Psychology*, 8, DEC, 1–8. DOI: 10.3389/fpsyg.2017.02179.

[26] Atif Ahmad, Justin Hadgkiss, and A. B. Ruighaver. 2012. Incident response teams - Challenges in supporting the organisational security function. *Computers and Security*, 31, 5, 643–652. DOI: 10.1016/j.cose.2012.04.001.

[27] Claire La Fleur, Blaine Hoffman, C. Benjamin Gibson, and Norbou Buchler. 2021. Team performance in a series of regional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization. *Computers and Security*, 104102229. DOI: 10.1016/j.cose.2021.102229.

[28] Kira Gedris et al. 2021. Simulating Municipal Cybersecurity Incidents: Recommendations from Expert Interviews Kira. In *Proceedings of the 54th Hawaii International Conference on System Sciences 2021*, 2036–2045.

[29] Philipp Kuehn, Thea Riebe, Lynn Apelt, Max Jansen, and Christian Reuter. 2020. Sharing of Cyber Threat Intelligence between States. *S+F Sicherheit und Frieden / Peace and Security*, 38, 1, 22–28.

[30] Shahriar Badsha, Iman Vakilinia, and Shamik Sengupta. 2019. Privacy Preserving Cyber Threat Information Sharing and Learning for Cyber Defense. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 0708–0714 DOI: 10.1109/CCWC.2019.8666477.

[31] Paúl Valladares, Walter Fuertes, Freddy Tapia, Theofilos Toulkeridis, and Ernesto Pérez. 2017. Dimensional data model for early alerts of malicious activities in a CSIRT. In *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, Seattle, WA, USA DOI: 10.23919/SPECTS.2017.8046771.

[32] Gabriel Pimenta Rodrigues et al. 2017. Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection. *Applied Sciences*, 7, 10, 1082. DOI: 10.3390/app7101082.

[33] Marko Krstic, Milan Cabarkapa, and Aleksandar Jevremovic. 2019. Machine Learning Applications in Computer Emergency Response Team Operations. *27th Telecommunications Forum, TELFOR 2019*, 13–16. DOI: 10.1109/TELFOR48224.2019.8971040.

[34] Keshnee Padayachee and Elias Worku. 2018. Shared situational awareness in information security incident management. *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017*, 479–483. DOI: 10.23919/ICITST.2017.8356454.

[35] Florian Skopik, Giuseppe Settanni, and Roman Fiedler. 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*, 60154–176. DOI: 10.1016/j.cose.2016.04.003.

[36] Himanshu Khurana, Jim Basney, Mehedi Bakht, Mike Freemon, Von Welch, and Randy Butler. 2009. Palantir: a framework for collaborative incident response and investigation. In *Proceedings of the 8th Symposium on Identity and Trust on the Internet - IDtrust '09*, New York, New York, USA, ACM Press, 38 DOI: 10.1145/1527017.1527023.

[37] David Croasdell. 2019. The Role of Transnational Cooperation in Cybersecurity Law Enforcement. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 5598–5607.

[38] Marios Ioannou, Eliana Stavrou, and Maria Bada. 2019. Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, DOI: 10.1109/CyberSecPODS.2019.8885240.

[39] Otto Hellwig. 2015. Organisation, Rahmenbedingungen und Kommunikation bei CERTs. In *Sicherheit in Cyber-Netzwerken*, Edith Huber (Ed.). Wiesbaden, Springer VS, 559–574.

[40] Florian Skopik, Tímea Páhi, and Maria Leitner, Eds. 2018. *Cyber Situational Awareness in Public-Private-Partnerships*. Berlin, Germany, Springer Vieweg DOI: 10.1007/978-3-662-56084-6.

[41] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT security: Accountabilities, moralities, and oscillations in IT security practices. *Proceedings of the ACM on Human-Computer Interaction*, 2, CSCW, . DOI: 10.1145/3274361.

[42] Guy Paré, Marie Claude Trudel, Mirou Jaana, and Spyros Kitsiou. 2015. Synthesizing information systems knowledge: A typology of literature reviews. *Information and Management*, 52, 2, 183–199. DOI: 10.1016/j.im.2014.08.008.

[43] Christian Reuter. 2018. *Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement*. Wiesbaden, Springer Vieweg (Lehrbuch/Fachbuch) DOI: 10.1007/978-3-658-19523-6.

[44] Marc-André Kaufhold. 2021. *Information Refinement Technologies for Crisis Informatics: User Expectations and Design Principles for Social Media and Mobile Apps*. Wiesbaden, Springer Vieweg DOI: 10.1007/978-3-658-33341-6.

[45] Umar Ali Bukar, Marzanah A. Jabar, Fatimah Sidi, Rozi Nor Haizan Binti Nor, Salfarina Abdullah, and Mohamed Othman. 2020. Crisis Informatics in the Context of Social Media Crisis Communication: Theoretical Models, Taxonomy, and Open Issues. *IEEE Access*, 8185842–185869. DOI: 10.1109/access.2020.3030184.

[46] Milad Mirbabaie, Deborah Bunker, Stefan Stieglitz, Julian Marx, and Christian Ehnis. 2020. Social media in times of crisis: Learning from Hurricane Harvey for the coronavirus disease 2019 pandemic response. *Journal of Information Technology*, 35, 3, 195–213. DOI: 10.1177/0268396220929258.

[47] Christian Reuter, Thomas Ludwig, Marc-André Kaufhold, and Thomas Spielhofer. 2016. Emergency Services Attitudes towards Social Media: A Quantitative and Qualitative Survey across Europe. *International Journal on Human-Computer Studies (IJHCS)*, 9596–111. DOI: 10.1016/j.ijhcs.2016.03.005.

[48] M. R. Endsley. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37, 1, 32–64. DOI: 10.1518/001872095779049543.

[49] Alexander Kott, Cliff Wang, and Robert F. Erbacher. 2014. *Cyber Defense and Situational Awareness* 62. DOI: 10.1007/978-3-319-11391-3.

[50] Sudip Mittal, Prajit Kumar Das, Varish Mulwad, Anupam Joshi, and Tim Finin. 2016. CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities. In *Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2016*, 860–867 DOI: 10.1109/ASONAM.2016.7752338.

[51] Christian Reuter, Thomas Ludwig, Marc-André Kaufhold, and Volkmar Pipek. 2015. XHELP: Design of a Cross-Platform Social-Media Application to Support Volunteer Moderators in Disasters. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, Seoul, Korea, ACM Press, 4093–4102 DOI: 10.1145/2702123.2702171.

[52] Michael Glassman and Min Ju Kang. 2012. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, 28, 2, 673–682. DOI: 10.1016/j.chb.2011.11.014.

[53] Christian Reuter and Simon Scholl. 2014. Technical Limitations for Designing Applications for Social Media. In *Mensch & Computer: Workshopband*, M. Koch, A. Butz, and J. Schlichter (Eds.). München, Germany, Germany, Oldenbourg-Verlag, 131–140.

[54] Carlos Castillo. 2016. *Big Crisis Data: Social Media in Disasters and Time-Critical Situations*. New York, NY, USA, Cambridge University Press.

[55] Ekaterina Olshannikova, Thomas Olsson, Jukka Huhtamäki, and Hannu Kärkkäinen. 2017. Conceptualizing Big Social Data. *Journal of Big Data*, 4, 1, 1–19. DOI: 10.1186/s40537-017-0063-x.

[56] Linda Plotnick and Starr Roxanne Hiltz. 2016. Barriers to Use of Social Media by Emergency Managers. *Journal of Homeland Security and Emergency Management*, 13, 2, 247–277. DOI: 10.1515/jhsem-2015-0068.

[57] Stefan Stieglitz, Milad Mirbabaie, Björn Ross, and Christoph Neuberger. 2018. Social media analytics – Challenges in topic discovery, data collection, and data preparation. *International Journal of Information Management*, 39156–168. DOI: 10.1016/j.ijinfomgt.2017.12.002.

[58] Stefan Stieglitz, Milad Mirbabaie, J. Fromm, and S. Melzer. 2018. The Adoption of Social Media Analytics for Crisis Management - Challenges and Opportunities. In *Proceedings of the 26th European Conference on Information Systems (ECIS)*, Portsmouth, UK.

[59] Markus Bayer, Marc-André Kaufhold, and Christian Reuter. 2021. Information Overload in Crisis Management: Bilingual Evaluation of Embedding Models for Clustering Social Media Posts in Emergencies. In *Proceedings of the European Conference on Information Systems (ECIS)*, .

[60] Linda Plotnick and Starr Roxanne Hiltz. 2018. Software Innovations to Support the Use of Social Media by Emergency Managers. *International Journal of Human-Computer Interaction*, 34, 4, 367–381. DOI: 10.1080/10447318.2018.1427825.

[61] Firoj Alam, Ferda Ofli, and Muhammad Imran. 2020. Descriptive and visual summaries of disaster events using artificial intelligence techniques: case studies of Hurricanes Harvey, Irma, and Maria. *Behaviour & Information Technology (BIT)*, 39, 3, 288–318. DOI: 10.1080/0144929X.2019.1610908.

[62] Marc-André Kaufhold, Nicola Rupp, Christian Reuter, and Matthias Habdank. 2020. Mitigating Information Overload in Social Media during Conflicts and Crises: Design and Evaluation of a Cross-Platform Alerting System. *Behaviour & Information Technology (BIT)*, 39, 3, 319–342. DOI: 10.1080/0144929X.2019.1620334.

[63] Marc-André Kaufhold, Markus Bayer, and Christian Reuter. 2020. Rapid relevance classification of social media posts in disasters and emergencies: A system and evaluation featuring active, incremental and online learning. *Information Processing and Management*, 57, 1, 1–32. DOI: 10.1016/j.ipm.2019.102132.

[64] Philipp Kuehn, Markus Bayer, Marc Wendelborn, and Christian Reuter. 2021. OVANA: An Approach to Analyze and Improve the Information Quality of Vulnerability Databases. In *Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES)*, ACM, 11 DOI: 10.1145/3465481.3465744.

[65] Matthias Moi, Therese Habig, Annika Schubert, Michaela Brune, Fabian Witter, and Maximilian Kiel. 2017. EmerGent Deliverable 4.5: Information Quality Criteria and Indicators., Paderborn.

[66] Katrin Hartwig and Christian Reuter. 2019. TrustyTweet: An Indicator-based Browser-Plugin to Assist Users in Dealing with Fake News on Twitter. In *Proceedings of the International Conference on Wirtschaftsinformatik (WI)*, Siegen.

[67] Marc-André Kaufhold and Christian Reuter. 2019. Cultural Violence and Peace in Social Media. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, Christian Reuter (Ed.). Wiesbaden, Germany, Springer Vieweg, 361–381 DOI: 10.1007/978-3-658-25652-4_17.

[68] Thea Riebe, Katja Pätsch, Marc-André Kaufhold, and Christian Reuter. 2018. From Conspiracies to Insults: A Case Study of Radicalisation in Social Media Discourse. In *Mensch und Computer 2018: Workshopband*, Raimund Dachselt and Gerhard Weber (Eds.). Dresden, Germany, Gesellschaft für Informatik e.V., 595–603.

[69] Marco Viviani and Gabriella Pasi. 2017. Credibility in social media: opinions, news, and health information—a survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7, 5, e1209--n/a. DOI: 10.1002/widm.1209.

[70] Milad Mirbabaie and Jennifer Fromm. 2019. Reducing the Cognitive Load of Decision-Makers in Emergency Management through Augmented Reality. In *European Conference on Information Systems (ECIS)*, Stockholm & Uppsala, Sweden, 1–11.

[71] Guofeng Cao, Shaowen Wang, Myunghwa Hwang, Anand Padmanabhan, Zhenhua Zhang, and Kiumars Soltani. 2015. A Scalable Framework for Spatiotemporal Analysis of Location-based Social Media Data. *Computers, Environment and Urban Systems*, 5170–82. DOI: 10.1016/j.compenvurbsys.2015.01.002.

[72] Milad Mirbabaie and Elisa Zapatka. 2017. Sensemaking in Social Media Crisis Communication – A Case Study on the Brussels Bombings in 2016. In *Twenty-Fifth European Conference on Information Systems (ECIS)*, Guimarães, Portugal, 2169–2186.

[73] Julian Marx, Milad Mirbabaie, and Christian Ehnis. 2018. Sense-Giving Strategies of Media Organisations in Social Media Disaster Communication: Findings from Hurricane Harvey. In *Proceedings of the 29th Australasian Conference on Information Systems (ACIS)*, Sydney, Australia, 1–12.

[74] Andreas Weiler, Michael Grossniklaus, and Marc Scholl. 2016. Situation Monitoring of Urban Areas Using Social Media Data Streams. *Information Systems*, 57129–141. DOI: 10.1016/j.is.2015.09.004.

[75] Stefan Stieglitz and Linh Dang-Xuan. 2013. Emotions and Information Diffusion in Social Media — Sentiment of Microblogs and Sharing Behavior. *Journal of Management Information Systems*, 29, 4, 217–248. DOI: 10.2753/MIS0742-1222290408.

[76] Stefan Stieglitz, Milad Mirbabaie, Lara Schwenner, Julian Marx, Janina Lehr, and Felix Brünker. 2017. Sensemaking and Communication Roles in Social Media Crisis Communication. In *Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI)*, St. Gallen, Switzerland.

[77] Marc-André Kaufhold et al. 2019. Potentiale von IKT beim Ausfall kritischer Infrastrukturen: Erwartungen, Informationsgewinnung und Mediennutzung der Zivilbevölkerung in Deutschland. In *Proceedings of the International Conference on Wirtschaftsinformatik*, Siegen, Germany, AIS Electronic Library (AISeL).

[78] Christian Reuter, Thomas Ludwig, Marc-André Kaufhold, and Julian Hupertz. 2017. Social Media Resilience during Infrastructure Breakdowns using Mobile Ad-Hoc Networks. In *Advances and New Trends in Environmental Informatics - Proceedings of the 30th EnviroInfo Conference*, V. Wohlgemuth, Frank Fuchs-Kittowski, and Jochen Wittmann (Eds.). Berlin, Germany, Germany, Springer, 75–88 DOI: 10.1007/978-3-319-44711-7_7.

[79] Volker Wulf, Markus Rohde, Volkmar Pipek, and Gunnar Stevens. 2011. Engaging with Practices: Design Case Studies as a Research Framework in CSCW. In *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*, Hangzhou, China, ACM Press, 505–512.

[80] Marc-André Kaufhold, Alexis Gizikis, Christian Reuter, Matthias Habdank, and Margarita Grinko. 2019. Avoiding Chaotic Use of Social Media before, during, and after Emergencies: Design and Evaluation of Citizens' Guidelines. *Journal of Contingencies and Crisis Management (JCCM)*, 27, 3, 198–213. DOI: 10.1111/1468-5973.12249.

[81] Christian Reuter, Marc André Kaufhold, Stefka Schmid, Thomas Spielhofer, and Anna Sophie Hahne. 2019. The impact of risk cultures: Citizens' perception of social media use in emergencies across Europe. *Technological Forecasting and Social Change (TFSC)*, 148, 119724, . DOI: 10.1016/j.techfore.2019.119724.

[82] Marc-André Kaufhold, Nicola Rupp, Christian Reuter, Christoph Amelunxen, and Massimo Cristaldi. 2018. 112.social: Design and Evaluation of a Mobile Crisis App for Bidirectional Communication between Emergency Services and Citizens. In *European Conference on Information Systems (ECIS)*, Portsmouth, UK, AIS Electronic Library (AISeL).

[83] Clayton Wukich. 2015. Social media use in emergency management. *Journal of Emergency Management*, 13, 4, 281–294. DOI: 10.5055/jem.2015.0242.

[84] Thea Riebe and Christian Reuter. 2019. Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In *Information Technology for Peace and Security*, DOI: 10.1007/978-3-658-25652-4_8.

[85] Thea Riebe, Stefka Schmid, and Christian Reuter. 2020. Measuring Spillover Effects from Defense to Civilian Sectors – A Quantitative Approach Using LinkedIn. *Defence and Peace Economics*, 00, 00, 1–13. DOI: 10.1080/10242694.2020.1755787.

[86] Jeroen van den Hoven. 2010. The use of normative theories in computer ethics. In *The Cambrdige Handbook of Information and Computer Ethics*, Luciano Floridi (Ed.). Cambridge, 60–76 DOI: 10.3172/JIE.21.2.17.

[87] Datenethikkommission. 2019. Gutachten der Datenethikkommission., Berlin.

[88] Turkka Keinonen. 2008. User-centered design and fundamental need. In *NordiCHI '08: Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*, 211–219.

[89] Alexander Boden, Michael Liegl, and Monika Büscher. 2018. Ethische, rechtliche und soziale Implikationen (ELSI). *Sicherheitskritische Mensch-Computer-Interaktion*, 163–182. DOI: 10.1007/978-3-658-19523-6_9.

[90] B. Törpel, A. Voss, M. Hartswood, and R. Procter. 2009. Participatory Design: Issues and Approaches in Dynamic Constellations of Use, Design, and Research. In *Configuring User-Designer Relations. Computer Supported Cooperative Work.*, M. Büscher, R. Slack, M. Rouncefield, R. Procter, M. Hartswood, and A. Voss (Eds.). London, Springer.

[91] Michael Liegl, Alexander Boden, Monika Büscher, Rachel Oliphant, and Xaroula Kerasidou. 2016. Designing for ethical innovation: A case study on ELSI co-design in emergency. *International Journal of Human Computer Studies*, 9580–95. DOI: 10.1016/j.ijhcs.2016.04.003.

[92] Batya Friedman, Peter H. Kahn Jr., and A. Borning. 2006. Value Sensitive Design and information systems. *Human-computer interaction and management information systems: Foundations*, 1–27. DOI: 10.1145/242485.242493.

[93] Batya Friedman, Lisa P. Nathan, and Daisy Yoo. 2017. Multi-lifespan information system design in support of transitional justice: Evolving situated design principles for the Long(er) Term. *Interacting with Computers*, 29, 1, 80–96. DOI: 10.1093/iwc/iwv045.

[94] Oliver Heger, Bjoern Niehaves, and Henrik Kampling. 2018. The value declaration: a method for integrating human values into design-oriented research projects. *Ethics and Information Technology*, 2375–78. DOI: 10.1007/s10676-018-9464-6.

[95] Marius Mueller and Oliver Heger. 2018. Health at any cost? Investigating ethical dimensions and potential conflicts of an ambulatory therapeutic assistance system through value sensitive design. In *International Conference on Information Systems 2018, ICIS 2018*, 1–17.